DIN EN 18031-1

ICS 33.060.20; 35.030 Einsprüche bis 2024-07-03

Entwurf

Gemeinsame Sicherheitsanforderungen für Funkanlagen – Teil 1: Funkanlagen mit Internetanschluss; Deutsche und Englische Fassung prEN 18031-1:2023

Common security requirements for radio equipment –
Part 1: Internet connected radio equipment;
German and English version prEN 18031-1:2023

Exigences de sécurité communes applicables aux équipements radioélectriques connectés à l'internet;
Version allemande et anglaise prEN 18031-1:2023

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2024-05-03 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil das beabsichtigte Dokument 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 Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 253 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

www.din.de
www.dinmedia.de
3540883

Nationales Vorwort

Das Dokument prEN 18031-1:2023 wurde vom Technischen Komitee CEN/CENELEC/JTC 13/WG 8 „WG 8 Arbeitsgruppe RED Normungsantrag“ erarbeitet, dessen Sekretariat von NEN (Niederlande) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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

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

– Entwurf –

August 2023

prEN 18031-1

Gemeinsame Sicherheitsanforderungen für Funkanlagen – Teil 1: Funkanlagen mit Internetanschluss

Common security requirements for radio equipment – Part 1: Internet connected radio equipment

Exigences de sécurité communes applicables aux équipements radioélectriques connectés à l'internet

E DIN EN 18031-1:2024-06
prEN 18031-1:2023 (D)

Inhalt

Bilder

Tabellen

Europäisches Vorwort

Dieses Dokument (prEN 18031-1:2023) wurde vom Technischen Komitee CEN/CENELEC/JTC 13/WG 8 „WG 8 Arbeitsgruppe RED Normungsantrag“ erarbeitet, dessen Sekretariat von NEN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wurde im Rahmen eines Normungsauftrages erarbeitet, den die Europäische Kommission und die Europäische Freihandelsassoziation CEN/CENELEC erteilt haben, und unterstützt grundlegende Anforderungen der EU-Richtlinie(n)/Verordnung(en).

Zum Zusammenhang mit EU-Richtlinie(n)/Verordnung(en) siehe informativen Anhang ZA, der Bestandteil dieses Dokuments ist.

Einleitung

Es ist wichtig anzumerken, dass bewährte Verfahrensweisen zur Verteidigung in der Tiefe erforderlich sind, um eine umfassende Cybersicherheit von Funkanlagen zu erreichen. Insbesondere ist keine Einzelmaßnahme ausreichend, um die vorgegebenen Ziele zu erreichen; tatsächlich ist üblicherweise eine Reihe von Mechanismen und Maßnahmen erforderlich, um nur eine Sicherheitszielsetzung zu erreichen. Die Leitlinien in diesem Dokument enthalten Listen von Beispielen. Diese Listen sind so zu verstehen, dass sie nur Hinweise auf Möglichkeiten geben; es gibt andere Möglichkeiten, die nicht aufgeführt sind, und selbst die Anwendung der angegebenen Beispiele ist nicht ausreichend, wenn die gewählten Mechanismen und Maßnahmen nicht in koordinierter Weise implementiert werden.

1 Anwendungsbereich

Dieses Dokument legt gemeinsame Sicherheitsanforderungen für mit dem Internet verbundene Funkanlagen fest. Dieses Dokument enthält technische Spezifikationen für Funkanlagen; dies betrifft elektrische oder elektronische Produkte, die fähig sind, über das Internet zu kommunizieren, unabhängig davon, ob diese Produkte direkt oder über irgendwelche anderen Geräte kommunizieren.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

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

— IEC Electropedia: verfügbar unter https://www.electropedia.org/

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

3.1
Zugangssteuerungsmechanismus
Funktionalität von *Geräten*, um den Zugang zu spezifischen Ressourcen des *Geräts* zu gewähren, einzuschränken oder zu verweigern

Anmerkung 1 zum Begriff: Der Zugang zu spezifischen Geräteressourcen kann sich unter anderem auf Folgendes beziehen:

— das Lesen spezifischer Daten; oder

— das Schreiben spezifischer Daten in den dauerhaften Speicher des Geräts; oder

— die Durchführung einer bestimmten Gerätefunktionalität, beispielsweise einer Audioaufzeichnung.

3.2
Authentisierung
Sicherstellung, dass eine *Entität* das ist, was sie angibt zu sein

3.3
Authentisierungsmechanismus
Funktionalität von *Geräten*, um zu verifizieren, dass eine *Entität* das ist, was sie angibt zu sein

Anmerkung 1 zum Begriff: Eine Entität kann unter anderem angeben:

— eine spezifische Person, ein Eigentümer eines Benutzerkontos, ein spezifisches Gerät oder ein spezifischer Dienst zu sein; oder

— ein Mitglied einer spezifischen Gruppe zu sein, beispielsweise einer zum Zugang zu einer bestimmten Geräteressource autorisierten Gruppe; oder

— durch eine andere Entität für den Zugang zu einer bestimmten Geräteressource autorisiert zu sein.

Anmerkung 2 zum Begriff: Üblicherweise beruht die Verifizierung auf der Untersuchung von Nachweisen eines oder mehrerer Elemente aus den folgenden Kategorien:

— Wissen; und

— Besitz; und

— Inhärenz.

3.4
Authentifikator
Mittel, das zur Validierung der Angabe einer *Entität* verwendet wird

BEISPIEL Ein Passwort oder ein Token können als Authentifikator verwendet werden.

3.5
bewährte Verfahrensweisen
Maßnahmen, für die nachgewiesen wurde, dass sie eine angemessene Sicherheit für den entsprechenden Anwendungsfall bieten

3.6
Brute-Force-Angriff
auf Versuch und Irrtum beruhendes Verfahren, um den richtigen *Authentifikator* zu erraten

3.7
Kommunikationsmechanismus
Funktionalität von *Geräten*, die die Kommunikation über eine *Schnittstelle* des Geräts ermöglicht

3.8
vertrauliche Sicherheitsparameter
geheime sicherheitsrelevante Informationen, deren Änderung oder Offenlegung die Sicherheit eines Werts kompromittieren können

3.9
Denial of Service (DoS)
Verhinderung oder Unterbrechung des autorisierten Zugangs zu einer Geräteressource oder Verlangsamung des Betriebs und der Funktionen von Geräten

[QUELLE: IEC 62443-1-1:2019, 3.2.42 — modifiziert]

3.10
Entität
Benutzer, Gerät oder Dienst

3.11
Gerät
Funkanlage
elektrisches oder elektronisches Erzeugnis, das zum Zweck der Funkkommunikation und/oder der Funkortung bestimmungsgemäß Funkwellen ausstrahlt und/oder empfängt, oder elektrisches oder elektronisches Erzeugnis, das Zubehör, etwa eine Antenne, benötigt, damit es zum Zweck der Funkkommunikation und/oder der Funkortung bestimmungsgemäß Funkwellen ausstrahlen und/oder empfangen kann

[QUELLE: Richtlinie 2014/53/EU, Artikel 2.1(1)]

3.12
externe Schnittstelle
Schnittstelle am *Gerät*, die von außerhalb des *Geräts* zugänglich ist

3.13
Werksvoreinstellung
definierter Zustand, in dem die Konfigurationseinstellungen und die Konfiguration des Geräts auf Anfangswerte eingestellt sind, die üblicherweise beim Verlassen der herstellenden Fabrik eingestellt werden

Anmerkung 1 zum Begriff: Eine Werksvoreinstellung kann Sicherheitsaktualisierungen einschließen, die nach der Markteinführung des Geräts installiert wurden.

3.14
Initialisierung
Prozess, bei dem die Netzwerkverbindung des *Geräts* für den Betrieb konfiguriert wird

Anmerkung 1 zum Begriff: Die Initialisierung kann die Möglichkeit bieten, Authentisierungsmerkmale für einen Benutzer oder für den Netzwerkzugang zu konfigurieren.

3.15
Schnittstelle
gemeinsame Begrenzung, über die *Entitäten* Informationen austauschen

3.16
Legacy
Gerät, Software-/Hardware-Komponente, Kryptographie oder Kommunikationsprotokoll, das/die nicht ohne Eindämmungsmaßnahmen vor aktuellen Cybersicherheitsbedrohungen geschützt werden kann

3.17
Maschinenschnittstelle
externe Schnittstelle zwischen der *Anlage* und einem Dienst oder einem Gerät

3.18
Netzwerkeinrichtung
Einrichtung, über die Daten zwischen verschiedenen Netzwerken ausgetauscht werden

3.19
Netzwerkwert
Netzwerkfunktion oder *Netzwerkfunktionskonfiguration,* die auf *Geräten* gespeichert ist, oder *sensitiver Sicherheitsparameter,* die auf dem *Gerät* gespeichert ist, um den Zugang zu Netzwerkressourcen zu ermöglichen

3.20
Netzwerkfunktion
Gerätefunktionalität für den Zugang zu Netzwerkressourcen

3.21
Konfiguration von Netzwerkfunktionen
Daten, die das Verhalten der *Netzwerkfunktionen* eines *Geräts* bestimmen

3.22
Netzwerkschnittstelle
externe Schnittstelle, die es ermöglicht, dass *Geräte* Zugang zu einem Netzwerk haben oder bereitstellen

Anmerkung 1 zum Begriff: Beispiele für Netzwerkschnittstellen sind LAN-Anschlüsse (drahtgebunden) oder drahtlose Netzwerkschnittstellen, die die Kommunikation über WLAN oder Bluetooth ermöglichen, z. B. mithilfe einer 2,4-GHz-Antenne.

3.23
Betriebszustand
Zustand, in dem *Geräte* ordnungsgemäß entsprechend ihrer bestimmungsgemäßen Verwendung und in ihrer für die Nutzung vorgesehenen Betriebsumgebung arbeiten

3.24
optionale Dienste
Dienste, die zur Ersteinrichtung des *Geräts* nicht erforderlich sind und die kein Teil der Grundfunktionalität sind, die jedoch für die bestimmungsgemäße Verwendung des *Geräts* relevant und Teil der Werksvoreinstellung sind

BEISPIEL Ein SSH-Dienst ist für die Grundfunktionalität des Geräts nicht erforderlich, aber er kann verwendet werden, um einen Fernzugriff auf das Gerät zuzulassen.

3.25
Passwort
Zeichenfolge (Buchstaben, Zahlen oder andere Symbole), die zur Authentisierung einer *Entität* verwendet werden

Anmerkung 1 zum Begriff: Persönliche Identifikationsnummern (PINs) gelten ebenfalls als eine Art Passwort.

3.26
öffentliche Sicherheitsparameter
sicherheitsbezogene Information, deren Änderung die Sicherheit eines Werts kompromittieren kann

3.27
resilient
fähig, ungünstige Bedingungen, Belastungen, Angriffe oder Kompromittierungen von Systemen, die Cyber-Ressourcen nutzen oder durch diese ermöglicht werden, vorherzusehen, ihnen zu widerstehen, sie zu beheben und sich ihnen anzupassen

[QUELLE: NIST Glossary: https://csrc.nist.gov/glossary/term/cyber_resiliency]

3.28
Risiko
Kombination der Wahrscheinlichkeit eines Schadenseintritts und seines Schadensausmaßes

[QUELLE: ISO/IEC Guide 51:2014]

3.29
Sicherheitswert
Sicherheitsfunktionalität des *Geräts*, die die Integrität des *Geräts* direkt beeinflussen kann, oder *sicherheitsrelevante Konfiguration*, die vom *Gerät* genutzt wird, oder *sensibler Sicherheitsparameter* für die Integrität des *Geräts,* der vom *Gerät* genutzt wird

3.30
sicherheitsrelevante Konfiguration
Daten, die das Verhalten der Sicherheitsfunktionalität von *Geräten* beeinflussen

3.31
sensible Sicherheitsparameter
vertraulicher Sicherheitsparameter für einen Wert oder *öffentlicher Sicherheitsparameter* für einen Wert

3.32
Sicherheitsaktualisierung
Software-Aktualisierung, die Sicherheitsschwachstellen durch Code-Patches oder andere Eindämmungsmaßnahmen behandelt

3.33
Speichermechanismus
Funktionalität von *Geräten*, die die Speicherung von Informationen ermöglicht

3.34
Aktualisierungsmechanismus
Funktionalität von *Geräten*, die die Änderung der *Geräte*software ermöglicht

3.35
Benutzungsschnittstelle
externe Schnittstelle zwischen dem *Gerät* und einem Benutzer

3.36
Schwachstelle
Schwäche oder Design- oder Implementationsfehler, die/der zu einem unerwarteten unerwünschten Ereignis führen kann, das die Sicherheit der beteiligten *Geräte*, des Netzwerks, der Anwendung oder des Protokolls gefährdet

[QUELLE: (ITSEC) (Definition durch ENISA, „Computersystem“ wurde durch „Gerät“ ersetzt)]

4 Anwendung dieser Norm

Diese Norm nutzt das Konzept von Mechanismen, die den Anwender dieser Norm anleiten, wann bestimmte Sicherheitsmaßnahmen anzuwenden sind. Mechanismen behandeln deren Anwendbarkeit und Angemessenheit anhand eines Satzes von Anforderungen, einschließlich Beurteilungskriterien. Die Entscheidung über das Bestehen oder Nichtbestehen wird für jede angegebene Einheit getroffen; wenn beispielsweise die Anwendbarkeit einer Anforderung auf externe Schnittstellen geprüft wird, wird die Entscheidung, ob die Anforderung und alle weiteren Anforderungen erfüllt werden müssen, unabhängig für jede externe Schnittstelle getroffen.

Die Mechanismen und deren Anwendung werden mithilfe der folgenden Struktur dokumentiert:

Tabelle 1 —

Abschnitt Nr.	Titel	Beschreibung, wie die Norm anzuwenden ist
5.x	XXX Mechanismus	Mechanismus für jede spezifische Einheit (z. B. externe Schnittstelle oder Sicherheitswert)
5.x.1	XXX-1 Anwendbarkeit der Mechanismen	Anwendbarkeit des Mechanismus
5.x.1.1	Anforderung	Für jede spezifische Einheit ist zu bestimmen und zu beurteilen, ob der Mechanismus erforderlich ist. ANMERKUNG Die Anwendbarkeit und Angemessenheit des Mechanismus kann in einer Anforderung zusammengefasst werden.
5.x.1.2	Begründung	
5.x.1.3	Leitlinie	
5.x.1.4	Beurteilungskriterien	
5.x.1.4.1	Beurteilungsziel	
5.x.1.4.2	Erforderliche Informationen	
5.x.1.4.3	Konzeptuelle Beurteilung	
5.x.1.4.4	Beurteilung der funktionalen Vollständigkeit	
5.x.1.4.5	Beurteilung der funktionalen Suffizienz	
5.x.2	XXX-2 Angemessene Mechanismen	Angemessenheit des Mechanismus

Tabelle 1 (*fortgesetzt*)

Abschnitt Nr.	Titel	Beschreibung, wie die Norm anzuwenden ist
5.x.2.1	Anforderung	Für jede spezifische Einheit, für die der Mechanismus wie in XXX-1 festgelegt erforderlich ist, ist zu bestimmen und zu beurteilen, ob der Mechanismus in ausreichendem Umfang implementiert wurde. ANMERKUNG Für die Angemessenheit eines Mechanismus können mehrere Unterabschnitte vorhanden sein, die sich auf spezifische Eigenschaften beziehen.
5.x.2.2	Begründung	
5.x.2.3	Leitlinie	
5.x.2.4	Beurteilungskriterien	
5.x.2.4.1	Beurteilungsziel	
5.x.2.4.2	Erforderliche Informationen	
5.x.2.4.3	Konzeptuelle Beurteilung	
5.x.2.4.4	Beurteilung der funktionalen Vollständigkeit	
5.x.2.4.5	Beurteilung der funktionalen Suffizienz	
5.x.y	XXX-Nr. Unterstützende Anforderungen	Anwendbarkeit und Angemessenheit von unterstützenden Anforderungen für den Mechanismus
5.x.y.1	Anforderung	Für jede spezifische Einheit, für die der durch XXX-1 festgelegte Mechanismus erforderlich ist, ist zu bestimmen und zu beurteilen, ob die unterstützende Anforderung implementiert werden muss (es können spezifische Bedingungen gelten, beispielsweise wenn das Gerät ein Spielzeug ist), und falls sie implementiert werden muss, ob die Implementation ausreichend ist.
5.x.y.2	Begründung	
5.x.y.3	Leitlinie	
5.x.y.4	Beurteilungskriterien	
5.x.y.4.1	Beurteilungsziel	
5.x.y.4.2	Erforderliche Informationen	
5.x.y.4.3	Konzeptuelle Beurteilung	
5.x.y.4.4	Beurteilung der funktionalen Vollständigkeit	
5.x.y.4.5	Beurteilung der funktionalen Suffizienz	

Die Beurteilungen werden durchgeführt, indem die dokumentierten Beurteilungsfälle untersucht werden; es sind möglicherweise nicht alle Beurteilungsfälle für jeden Mechanismus verfügbar:

— Konzeptuelle Beurteilung

Es ist zu untersuchen, ob die verfügbare Dokumentation und Begründung die erforderlichen Nachweise in angemessener Weise bereitstellt (beispielsweise die Begründung, warum ein Mechanismus für eine bestimmte Netzwerkschnittstelle nicht anwendbar ist).

— Beurteilung der funktionalen Vollständigkeit

Es ist zu untersuchen und zu prüfen, ob die verfügbare Dokumentation vollständig ist (beispielsweise durch den Einsatz von Netzwerk-Scannern, um zu verifizieren, ob alle externen Schnittstellen ordnungsgemäß identifiziert, dokumentiert und beurteilt wurden).

— Beurteilung der funktionalen Suffizienz

Es ist zu untersuchen und zu prüfen, ob die Implementation angemessen ist (beispielsweise ist mithilfe von Fuzzing-Tools zu prüfen, ob eine Netzwerkschnittstelle Angriffen mit fehlerhaften Daten gegenüber resilient ist).

Jede Beurteilung ist weiter in die folgenden Unterabschnitte gegliedert, bei denen ein Entscheidungsbaum zur Steuerung der Beurteilung genutzt werden kann:

— Zweck der Beurteilung;

— Voraussetzungen;

— Beurteilungseinheiten;

— Entscheidungszuweisung.

Unter den erforderlichen Informationen sind Informationen aufgeführt, die durch die technische Dokumentation bereitgestellt werden müssen. Die Norm fordert nicht, dass jedes erforderliche Informationselement als getrenntes Dokument zur Verfügung gestellt werden muss.

5 Anforderungen

5.1 [ACM] Zugangssteuerungsmechanismus (en: Access Control Mechanism)

5.1.1 [ACM-1] Anwendbarkeit von Zugangssteuerungsmechanismen

5.1.1.1 Anforderung

Das Gerät muss Zugangssteuerungsmechanismen einsetzen, um den Zugang von Entitäten zu Sicherheitswerten und Netzwerkwerten zu verwalten, außer bei Sicherheits- oder Netzwerkwerten, für die gilt:

— die vollständige öffentliche Zugänglichkeit entspricht der „vernünftigerweise vorhersehbaren und bestimmungsgemäßen Verwendung des Geräts“; oder

— die „für die Nutzung vorgesehene und bestimmungsgemäße Betriebsumgebung“ stellt sicher, dass der Zugang auf autorisierte Entitäten beschränkt wird.

5.1.1.2 Begründung

Sicherheits- und Netzwerkwerte sind nicht autorisierten Zugangsversuchen ausgesetzt. Zugangssteuerungsmechanismen beschränken die Möglichkeit, dass nicht autorisierte Entitäten auf diese Werte zugreifen.

5.1.1.3 Leitlinie

Die Anforderung fordert keine Zugangssteuerungsmechanismen für Werte, die nicht durch sie abgedeckt sind (z. B. für den Ausgabeknopf einer Kaffeemaschine). Darüber hinaus fordert sie keine Zugangssteuerungsmechanismen für Werte, die grundsätzlich abgedeckt sind, die aber bei der vernünftigerweise vorhersehbaren und bestimmungsgemäßen Verwendung allgemein für die Öffentlichkeit zugänglich sind oder bei denen die für die Nutzung vorgesehene und bestimmungsgemäße Betriebsumgebung sicherstellt, dass nur ein autorisierter Zugang möglich ist.

Es ist zu beachten, dass Funkschnittstellen zugänglich sein können, selbst wenn sich das Gerät in einer vertrauenswürdigen Umgebung befindet; beispielsweise sind drahtlose Netzwerke oft von außerhalb der Wohnung des Benutzers zugänglich.

Beispielsweise können je nach den technischen Eigenschaften, der vorgesehenen und bestimmungsgemäßen Verwendung und der für die Nutzung des Geräts vorgesehenen und bestimmungsgemäßen Betriebsumgebung unter Umständen keine Zugangssteuerungsmechanismen für maßgebliche Werte erforderlich sein, wenn:

— alle Entitäten mit Zugang zum Gerät (das Gerät wird bestimmungsgemäß in einem Bereich mit physischer Zugangskontrolle betrieben) für den Zugang zu diesen Werten autorisiert sind (z. B. die WPS-Taste an einem Home-Router);

— die Gerätefunktionalität nur Informationen (über Werte) bereitstellt, die öffentlich zugänglich sein sollen (z. B. Ausstrahlung von Bluetooth Advertising Beacons).

Zugangssteuerungsmechanismen benötigen Eigenschaften, mit denen die Zugangsrechte verknüpft werden können. Dies können unter anderem die folgenden Eigenschaften sein:

— verifizierte Angaben von Entitäten (beispielsweise Eigentümer eines Benutzerkontos, Mitglied einer spezifischen Gruppe oder durch eine andere Entität autorisiert zu sein);

— bestimmte Zustände des Geräts oder der Geräteumgebung (so kann beispielsweise ein elektronischer Pilotenkoffer während des Betriebs in der Luft andere Zugangsrechte für einen lokalen Benutzer haben, als wenn er am Boden aufbewahrt wird);

— die Schnittstelle, über die ein Zugang erfolgt (beispielsweise kann ein lokaler Zugang, bei dem offensichtlich eine physische Zugangskontrolle eingerichtet ist, andere Zugangsrechte haben als ein Fernzugriff);

— unterschiedliche Kombinationen dieser oder anderer Eigenschaften.

5.1.1.4 Beurteilungskriterien

5.1.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung ACM-1.

5.1.1.4.2 Erforderliche Informationen

[E.Doc.DT.ACM-1] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 1 für jeden Sicherheits- und Netzwerkwert.

[E.Just.DT.ACM-1] Begründung für den Pfad durch den Entscheidungsbaum in Bild 1 für jeden Sicherheits- und Netzwerkwert.

[E.Doc.SecurityAsset] Dokumentation für jeden Sicherheitswert.

[E.Doc.NetworkAsset] Dokumentation für jeden Netzwerkwert.

[E.Doc.ACM] Dokumentation aller Zugangssteuerungsmechanismen, die den Zugang von Entitäten zu jedem in [E.Doc.SecurityAsset] dokumentierten Sicherheitswert und jedem in[E.Doc.NetworkAsset] dokumentierten Netzwerkwert verwalten.

5.1.1.4.3 Konzeptuelle Beurteilung

5.1.1.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob Zugangssteuerungsmechanismen implementiert wurden, wo sie erforderlich sind.

5.1.1.4.3.2 Voraussetzungen

Keine.

5.1.1.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each security and network asset;
if (Is the full public accessibility of the asset the\n"equipment's
   reasonably foreseeable and\nintended use?) then (Yes)
   #application :NOT APPLICABLE\nIntended use is fully\npublic;
   detach;
else (No)
   if (Does the "foreseeable and intended\noperational environment of use"
   ensure\nthat accessibility to the asset is limited\nto authorized
   entities? ) then (Yes)
      #application :NOT APPLICABLE\nIntended environment\nprotects the
   asset;
      detach;
   else (No)
         if (<b>access control mechanism property:</b>\nAre there access
   control mechanisms that\nmanage entities access to the security\nand
   network asset? ) then (Yes)
            #lightgreen :PASS\nAccess control\nmechanism needed\nand
   present;
            detach;
         else (No)
            #pink :FAIL\nAccess control\nmechanism needed\nbut not present;
            detach;
         endif
      endif
endif
@enduml
```

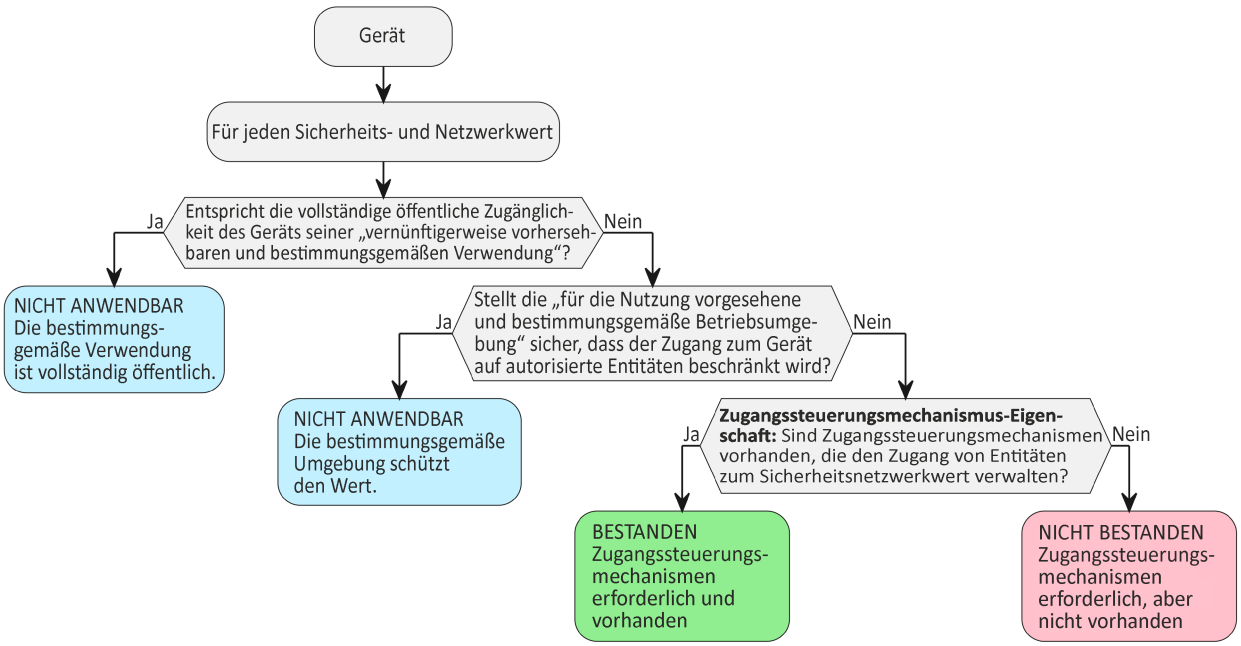

Bild 1 — Entscheidungsbaum für Anforderung ACM-1

Für jeden in [E.Doc.SecurityAsset] dokumentierten Sicherheitswert und jeden in [E.Doc.NetworkAsset] dokumentierten Netzwerkwert ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.ACM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.ACM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.ACM-1] dokumentierte Begründung zu untersuchen.

5.1.1.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.1.1.4.4 Beurteilung der funktionalen Vollständigkeit

5.1.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation der Sicherheits- und Netzwerkwerte vollständig ist.

5.1.1.4.4.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.1.1.4.4.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob Sicherheitswerte existieren, die nicht in [E.Doc.SecurityAsset] dokumentiert sind, und ob Netzwerkwerte existieren, die nicht in [E.Doc.NetworkAsset] dokumentiert sind.

5.1.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen Sicherheitswerte in [E.Doc.SecurityAsset] dokumentiert sind und alle gefundenen Netzwerkwerte in [E.Doc.NetworkAsset] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Sicherheitswert gefunden wird, der nicht in [E.Doc.SecurityAsset] dokumentiert ist, oder wenn ein Netzwerkwert gefunden wird, der nicht in [E.Doc.NetworkAsset] dokumentiert ist.

5.1.1.4.5 Beurteilung der funktionalen Suffizienz

5.1.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob Zugangssteuerungsmechanismen implementiert wurden, wo sie erforderlich sind.

5.1.1.4.5.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.1.1.4.5.3 Beurteilungseinheiten

Für jeden in [E.Doc.SecurityAsset] dokumentierten Sicherheitswert und jeden in [E.Doc.NetworkAsset] dokumentierten Netzwerkwert ist funktional das Vorhandensein von Zugangssteuerungsmechanismen entsprechend [E.Doc.ACM] zu bestätigen.

5.1.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass Zugangssteuerungsmechanismen nicht wie beschrieben implementiert wurden.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass Zugangssteuerungsmechanismen nicht wie beschrieben implementiert wurden.

5.1.2 [ACM-2] Angemessene Zugangssteuerungsmechanismen

5.1.2.1 Anforderung

Bei allen Sicherheits- und Netzwerkwerten, die durch Zugangssteuerungsmechanismen verwaltet werden, müssen die Zugangssteuerungsmechanismen sicherstellen, dass nur autorisierte Entitäten Zugang zu den verwalteten Sicherheits- und Netzwerkwerten haben.

5.1.2.2 Begründung

Sicherheits- und Netzwerkwerte können nicht autorisierten Zugangsversuchen ausgesetzt sein. Angemessene Zugangssteuerungsmechanismen stellen sicher, dass diese Werte vor nicht autorisierten Zugriffen geschützt sind.

5.1.2.3 Leitlinie

Diese Anforderung soll sicherstellen, dass die Zugangssteuerungsmechanismen, die zum Schutz der maßgeblichen Werte verwendet werden, so ausgewählt und konfiguriert wurden, dass nicht autorisierte Zugänge verhindert werden. Aufgrund vielfältiger Zugangsverfahren und Kontrollmechanismen für Werte (beispielsweise durch Anzeige auf einem Wearable-Bildschirm), Anwendungsfälle für Geräte und Betriebsumgebungen ist es schwierig, ein allgemeines Modell für Entitäten und die damit verbundenen Zugangsrechte festzulegen.

Ob ein Zugangssteuerungsmechanismus einen nicht autorisierten Zugang verweigern kann, hängt immer davon ab, welche externen Annahmen erfüllt werden müssen. Beispielsweise, ob das Teilen von Passwörtern oder der nicht autorisierte physische Zugang unzulässig ist.

Abhängig von den technischen Geräteeigenschaften und der für die Nutzung vorgesehenen und bestimmungsgemäßen Betriebsumgebung nutzen Zugangssteuerungsmechanismen angemessene Eigenschaften, mit denen die Zugangsrechte verknüpft sind, und stellen sicher, dass diese Zugangsrechte in geeigneter Weise vergeben werden.

Wenn Zugangssteuerungsmechanismen auf Authentisierungsmechanismen beruhen (siehe beispielsweise AUM),

— kann eine autorisierte Entität, z. B. eine spezifische Person, der Besitzer eines Benutzerkontos, eines Geräts oder Dienstes, nach der Authentisierung auf den Wert zugreifen, um beispielsweise die Sicherheitskonfiguration zu ändern,

— kann ein Mitglied einer spezifischen autorisierten Gruppe nach der Authentisierung auf ein Gerät zugreifen oder

— kann eine Entität, die durch eine andere Entität dafür autorisiert wurde, auf einen spezifischen Wert zugreifen.

Bei der Festlegung von Zugangssteuerungsmechanismen für Geräte sind die folgenden Aspekte wichtig:

— das Risiko, das mit dem Zugang einer Entität zu einem Wert verbunden ist;

— die Art des Zugangs zu einem Wert, den die Gerätefunktionalität zulässt;

— die Schnittstelle, über die auf den Wert zugegriffen wird; und

— der Einfluss durch die Zugangssteuerung, die von der für die Nutzung vernünftigerweise vorhersehbaren und bestimmungsgemäßen Umgebung bereitgestellt wird.

Bei der Festlegung der Zugangsrechte von Entitäten zu Werten (autorisierten Entitäten für einen bestimmten Zugang zu Werten) sind die folgenden Aspekte wichtig:

— das Risiko, das mit dem Zugang einer Entität zu einem Wert verbunden ist;

— das „Need-to-know-Prinzip“: ist es erforderlich, dass die Entität Informationen zu einem Wert erhält;

— das „Need-to-use-Prinzip“: hat eine Entität einen eindeutigen Bedarf, eine Funktionalität eines Werts zu nutzen;

— das „Least-Privilege-Prinzip“: alles ist verboten, außer es ist erlaubt;

— die eindeutig angegebene Funktionalität des Geräts, beispielsweise bezüglich der Zugänglichkeit von Werten oder der Interoperabilität mit Komponenten einer vorhandenen Infrastruktur.

5.1.2.4 Beurteilungskriterien

5.1.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung ACM-2.

5.1.2.4.2 Erforderliche Informationen

[E.Doc.DT.ACM-2] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 2 für jeden Sicherheits- und Netzwerkwert, der durch Zugangssteuerungsmechanismen verwaltet wird.

[E.Just.DT.ACM-2] Begründung für den Pfad durch den Entscheidungsbaum in Bild 2 für jeden Sicherheits- und Netzwerkwert, der durch Zugangssteuerungsmechanismen verwaltet wird.

ANMERKUNG Eine Begründung beinhaltet eine Beschreibung der Entitäten, ihre Zugangsrechte zum entsprechenden Wert und das Verfahren, wie durch Zugangssteuerungsmechanismen sichergestellt wird, dass nur autorisierter Zugang zum entsprechenden Wert gewährt wird.

[E.Doc.SecurityAsset] Dokumentation für jeden Sicherheitswert.

[E.Doc.NetworkAsset] Dokumentation für jeden Netzwerkwert.

[E.Doc.ACM] Dokumentation aller Zugangssteuerungsmechanismen, die den Zugang von Entitäten zu jedem in [E.Doc.SecurityAsset] dokumentierten Sicherheitswert und jedem in[E.Doc.NetworkAsset] dokumentierten Netzwerkwert verwalten.

5.1.2.4.3 Konzeptuelle Beurteilung

5.1.2.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Zugangssteuerungsmechanismen die erforderlichen Eigenschaften haben.

5.1.2.4.3.2 Voraussetzungen

Keine.

5.1.2.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each security and network asset that\nis managed by access control
   mechanisms;
    if (<b>access control mechanism property:</b>\nDo the access control
   mechanisms ensure\nthat only authorized entities have access\nto the
   managed security and network asset? ) then (Yes)
      #lightgreen :PASS\nAccess control mechanisms\nare appropriate;
      detach;
    else (No)
      #pink :FAIL\nAccess control mechanisms\nare not appropriate;
      detach;
    endif
@enduml
```

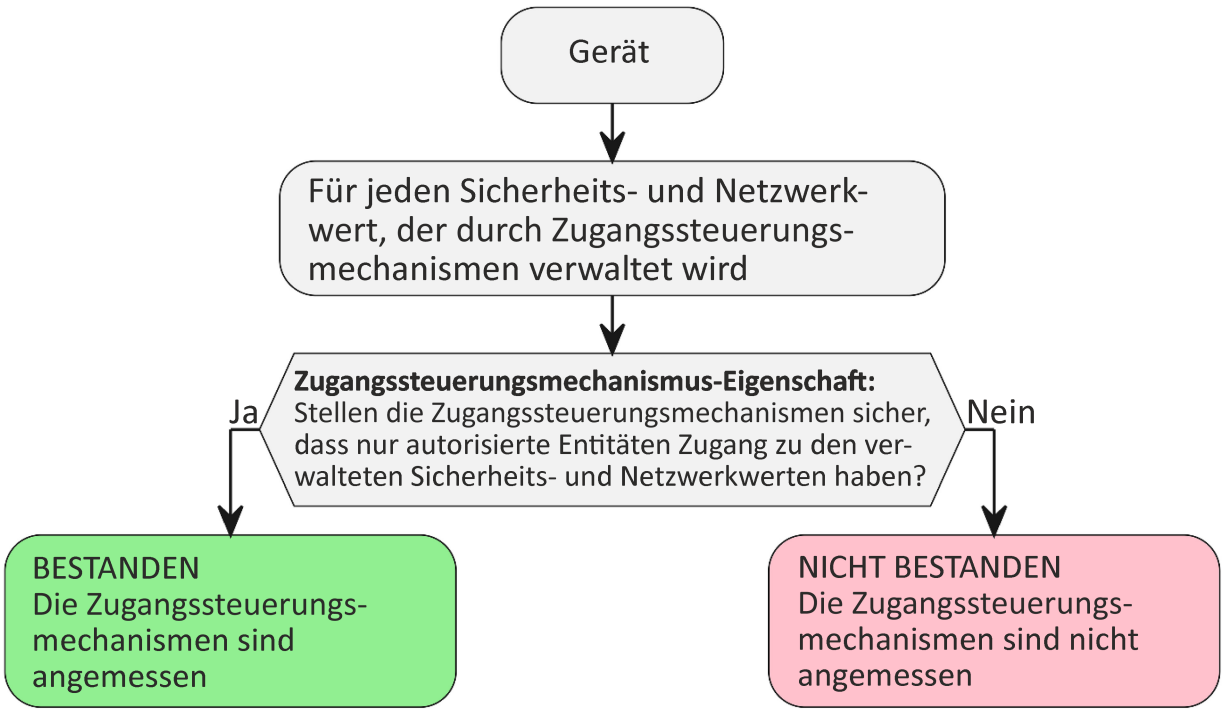

Bild 1 — Entscheidungsbaum für Anforderung ACM-2

Für jeden in [E.Doc.SecurityAsset] dokumentierten Sicherheitswert und jeden in [E.Doc.NetworkAsset] dokumentierten Netzwerkwert, der durch Zugangssteuerungsmechanismen entsprechend [E.Doc.ACM] verwaltet wird, ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.ACM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.ACM-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.ACM-2] dokumentierte Begründung zu untersuchen.

5.1.2.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „BESTANDEN“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.1.2.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.1.2.4.5 Beurteilung der funktionalen Suffizienz

5.1.2.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Zugangssteuerungsmechanismen die erforderlichen Eigenschaften haben.

5.1.2.4.5.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.1.2.4.5.3 Beurteilungseinheiten

Für jeden in [E.Doc.SecurityAsset] dokumentierten Sicherheitswert und jeden in [E.Doc.NetworkAsset] dokumentierten Netzwerkwert, der durch Zugangssteuerungsmechanismen entsprechend [E.Doc.ACM] verwaltet wird, sind die Eigenschaften der Zugangssteuerungsmechanismen in der in [E.Doc.DT.ACM-2] angegebenen Begründung funktional zu bestätigen.

5.1.2.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Eigenschaften der Zugangssteuerungsmechanismen nicht wie beschrieben sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Eigenschaften der Zugangssteuerungsmechanismen nicht wie beschrieben sind.

5.2 [AUM] Authentisierungsmechanismus (en: Authentication Mechanism)

Im Kontext der Anforderungen in diesem Abschnitt bedeutet die Formulierung „Zugang ermöglichen“, dass eine Schnittstelle implementiert wurde, die die Nutzung spezifischer, zum Gerät gehöriger Werte ermöglicht.

5.2.1 [AUM-1] Anwendbarkeit von Authentisierungsmechanismen für externe Schnittstellen

5.2.1.1 [AUM-1-1] Anforderung Netzwerkschnittstelle

Das Gerät muss bei jeder vom Netzwerk aus zugänglichen Schnittstelle, deren bestimmungsgemäße Verwendung die Bereitstellung des Zugangs zu Netzwerkwerten oder Sicherheitswerten des Geräts ist, mindestens einen Authentisierungsmechanismus nutzen, außer

— an der Schnittstelle ist keine Authentisierung zulässig, damit die bestimmungsgemäße Funktion der Schnittstelle erfüllt werden kann oder

— das Gerät kann nur in einem vertrauenswürdigen Netzwerk betrieben werden, das logisch oder physisch von nicht vertrauenswürdigen Netzwerken getrennt ist.

5.2.1.2 [AUM-1-2] Anforderung Benutzungsschnittstelle

Das Gerät muss bei jeder vom Netzwerk aus zugänglichen Schnittstelle, deren bestimmungsgemäße Verwendung die Bereitstellung von Zugang zu Netzwerkwerten oder Sicherheitswerten des Geräts ist, mindestens einen Authentisierungsmechanismus nutzen, außer die für die Nutzung vorgesehene Betriebsumgebung schafft Vertrauen in die Korrektheit der Angaben der Entitäten.

5.2.1.3 Begründung

Das Gerät muss einen Authentisierungsmechanismus in Verbindung mit einem Zugangssteuerungsmechanismus bereitstellen, um erfolgreiche Angriffe auf die Gerätewerte und den Missbrauch der Netzwerkressource zu verhindern. Der Authentisierungsmechanismus verifiziert, dass die Entität das ist, was sie angibt zu sein.

5.2.1.4 Leitlinie

Im Kontext dieses Abschnitts stellen die behandelten Schnittstellen Pfade zu den von der Anforderung abgedeckten Werten zur Verfügung. Authentisierungsmechanismen verifizieren die Gültigkeit der Angaben der Entität an einem Punkt des Pfads (z. B. in der Anwendung oder im Netzwerk). Die Verwaltung der zugehörigen Zugangsrechte für Entitäten ist Teil des Zugangssteuerungsmechanismus.

Es gibt verschiedene Arten von Entitäten, die mit dem Gerät interagieren können, z. B.:

— eine spezifische Person, der Eigentümer eines Benutzerkontos, ein Gerät oder ein Dienst; oder

— ein Mitglied einer spezifischen Gruppe, beispielsweise einer zum Zugang zu einer bestimmten Geräteressource autorisierten Gruppe; oder

— eine Entität, die durch eine andere Entität für den Zugang zu einer spezifischen Geräteressource autorisiert wurde.

Üblicherweise beruht die Verifizierung einer Entität auf der Untersuchung von Nachweisen eines oder mehrerer Elemente der folgenden Kategorien:

— Kenntnis (etwas, das man weiß); und

— Besitz (etwas, das man hat); und

— Inhärenz (etwas, das man ist).

Zur Authentisierung einer Entität kann das Vertrauensverhältnis zu einem Netzwerk genutzt werden (z. B. wenn die Entität über ein gemeinsames Geheimnis verfügt, wie beispielsweise WLAN-Anmeldedaten).

Eine Authentisierung ist unter Umständen nicht für alle externen Schnittstellen erforderlich; Beispiele sind Schnittstellen, die Protokolle zur Verfügung stellen, die bestimmungsgemäß ohne Authentisierung zugänglich sind, wie unter anderem DHCP- und ICMP-Meldungen.

5.2.1.5 Beurteilungskriterium Netzwerkschnittstelle

5.2.1.5.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-1-1.

5.2.1.5.2 Erforderliche Informationen

[E.Doc.DT.AUM-1-1] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 3 für jeden Sicherheits- und Netzwerkwert.

[E.Just.DT.AUM-1-1] Begründung für den Pfad durch den Entscheidungsbaum in Bild 3 für jeden Sicherheits- und Netzwerkwert.

[E.Doc.NetworkInterfaces.AUM-1-1] Beschreibung jeder Schnittstelle, die vom Netzwerk aus zugänglich ist, einschließlich der Beschreibung folgender Punkte:

— bestimmungsgemäße Nutzung der Schnittstelle;

— Beschreibung der Funktionalität der Schnittstelle.

(Falls angegeben) [E.Doc.SecurityAsset.AUM-1-1] Dokumentation jedes Sicherheitswerts, der über die in [E.Doc.NetworkInterfaces.AUM-1-1] dokumentierten Netzwerkschnittstellen zugänglich ist.

(Falls angegeben) [E.Doc.NetworkAsset.AUM-1-1] Dokumentation jedes Netzwerkwerts, der über die in [E.Doc.NetworkInterfaces.AUM-1-1] dokumentierten Schnittstellen zugänglich ist.

[E.Doc.AUM-1-1] Dokumentation der implementierten Authentisierungsmechanismen für alle in [E.Doc.NetworkInterfaces.AUM-1-1] dokumentierten Netzwerkschnittstellen.

[E.Doc.OperationalEnvironment] Beschreibung der für die Nutzung des Geräts vorgesehenen Betriebsumgebung.

5.2.1.5.3 Konzeptuelle Beurteilung

5.2.1.5.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob ein Authentisierungsmechanismus implementiert ist, wenn er zum Schutz von Netzwerkwerten oder Sicherheitswerten erforderlich ist.

5.2.1.5.3.2 Voraussetzungen

Keine.

5.2.1.5.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each network interface;
if (<b>Intended interface use</b>:\nDoes the interface provide \naccess to
   network assets \nor security assets? ) then (Yes )
```

```
  if (<b>Intended environment</b>:\nIs the equipment logically \nor
   physically separated \nfrom untrusted networks?) then (Yes )
  #application :NOT APPLICABLE \nUsed in a \nprotected \nenvironment;
  detach
  else (No)
          if (<b>Interface property</b>:\nDoes the interface require\n the
   absence of authentication \nin order to fullfill its indended use? ) then
   (Yes )
           #application :NOT APPLICABLE \nAbsence of \nauthentication
   \nrequired;
           detach
    else (No)
      if (<b>Interface property</b>:\nDoes the interface use an
   \nauthentication mechanism? ) then (Yes )
        #lightgreen :PASS;
        detach
      else (No)
        #pink :FAIL \nApplicable but not met;
        detach
      endif
    endif
  endif
else (No)
  #application :NOT APPLICABLE \nOut of scope;
  detach
endif
@enduml
```

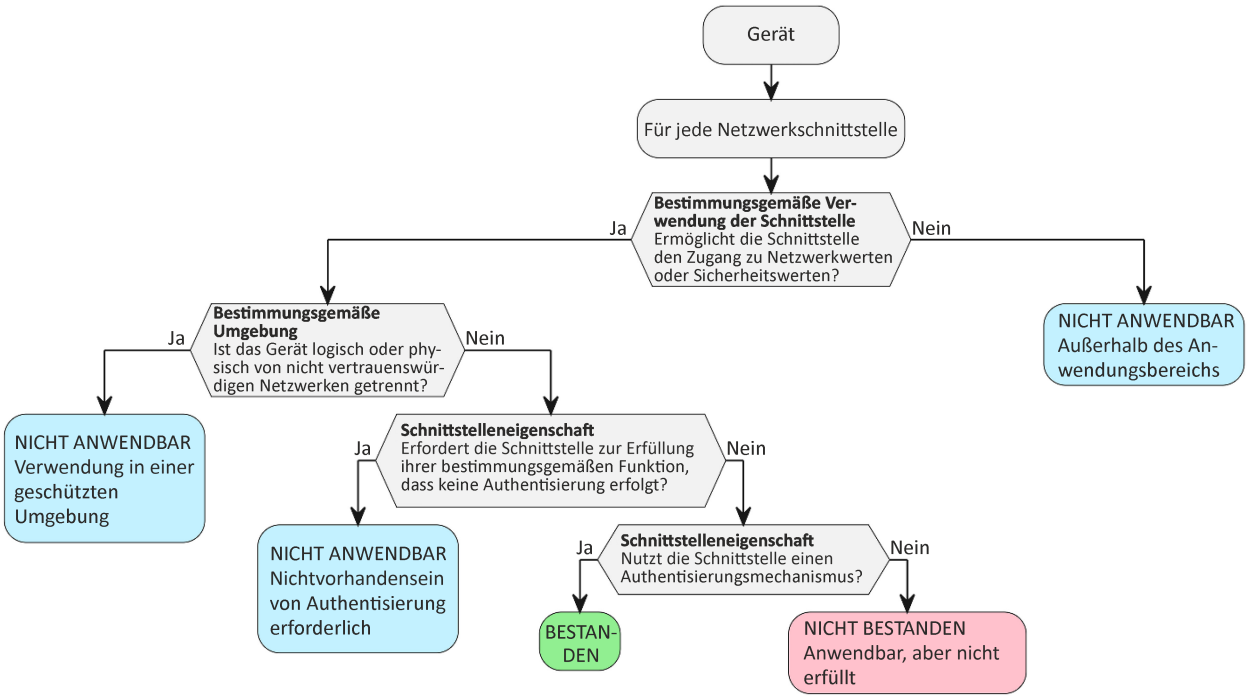

Bild 2 — Entscheidungsbaum für Anforderung AUM-1-1

Für jede in [E.Doc.NetworkInterfaces.AUM-1-1] dokumentierte Netzwerkschnittstelle, für den Zugang zu den in [E.Doc.SecurityAsset.AUM-1-1] dokumentierten Sicherheitswerten und/oder den in [E.Doc.NetworkAsset.AUM-1-1] dokumentierten Netzwerkwerten, für die in [E.Doc.OperationalEnvironment] dokumentierte,

für die Nutzung vorgesehene Betriebsumgebung und die in [E.Doc.AUM-1-1] dokumentierten Authentisierungsmechanismen ist zu prüfen, ob der in [E.Doc.DT.AUM-1-1] dokumentierte Pfad durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.AUM-1-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-1-1] dokumentierte Begründung zu untersuchen.

5.2.1.5.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.2.1.5.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.2.1.5.5 Beurteilung der funktionalen Suffizienz

Keine.

5.2.1.6 Beurteilungskriterium Benutzungsschnittstelle

5.2.1.6.1.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-1-2.

5.2.1.6.2 Erforderliche Informationen

[E.Doc.DT.AUM-1-2] Beschreibung des gewählten Pfads durch den in Bild 4 dargestellten Entscheidungsbaum für jeden Sicherheits- und Netzwerkwert.

[E.Just.DT.AUM-1-2] Begründung des gewählten Pfads durch den in Bild 4 dargestellten Entscheidungsbaum für jeden Sicherheits- und Netzwerkwert.

[E.Doc.UserInterfaces.AUM-1-2] Beschreibung jeder Schnittstelle, die vom Netzwerk aus zugänglich ist, einschließlich Beschreibung folgender Punkte:

— bestimmungsgemäße Nutzung der Schnittstelle;

— Beschreibung der Funktionalität der Schnittstelle.

(Falls angegeben) [E.Doc.SecurityAsset.AUM-1-2] Dokumentation jedes Sicherheitswerts, der über die in [E.Doc.NetworkInterfaces.AUM-1-2] dokumentierten Benutzungsschnittstellen zugänglich ist.

(Falls angegeben) [E.Doc.NetworkAsset.AUM-1-2] Dokumentation jedes Netzwerkwerts, der über die in [E.Doc.NetworkInterfaces.AUM-1-2] dokumentierten Benutzungsschnittstellen zugänglich ist.

[E.Doc.AUM-1-2] Dokumentation der implementierten Authentisierungsmechanismen für alle in [E.Doc.User-Interfaces.AUM-1-2] dokumentierten Benutzungsschnittstellen.

[E.Doc.OperationalEnvironment] Beschreibung der für die Nutzung des Geräts vorgesehenen Betriebsumgebung.

5.2.1.6.3 Konzeptuelle Beurteilung

5.2.1.6.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob Authentisierungsmechanismen implementiert sind, wenn sie zum Schutz von Netzwerkwerten oder Sicherheitswerten erforderlich sind.

5.2.1.6.3.2 Voraussetzungen

Keine.

5.2.1.6.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each user interface;
if (<b>Intended interface usage</b>:\nDoes the interface provide \naccess to
   network assets \nand/or security assets? ) then (Yes )
  if (<b>Intended environment</b>:\nDoes the intended operational
   \nenvironment of use provides \nconfidence in the correctness \nof an
   entity's claim? ) then (Yes )
  #application :NOT APPLICABLE \nUsed in a secure \noperational
   \nenvironment;
  detach
    else (No)
      if (<b>Interface property</b>:\nDoes the human \ninterface use an
   \nauthentication \nmechanism? ) then (Yes )
        #lightgreen :PASS;
        detach
      else (No)
        #pink :FAIL \nApplicable but not met;
        detach
      endif
  endif
else (No)
  #application :NOT APPLICABLE \nOut of scope;
  detach
endif
@enduml
```

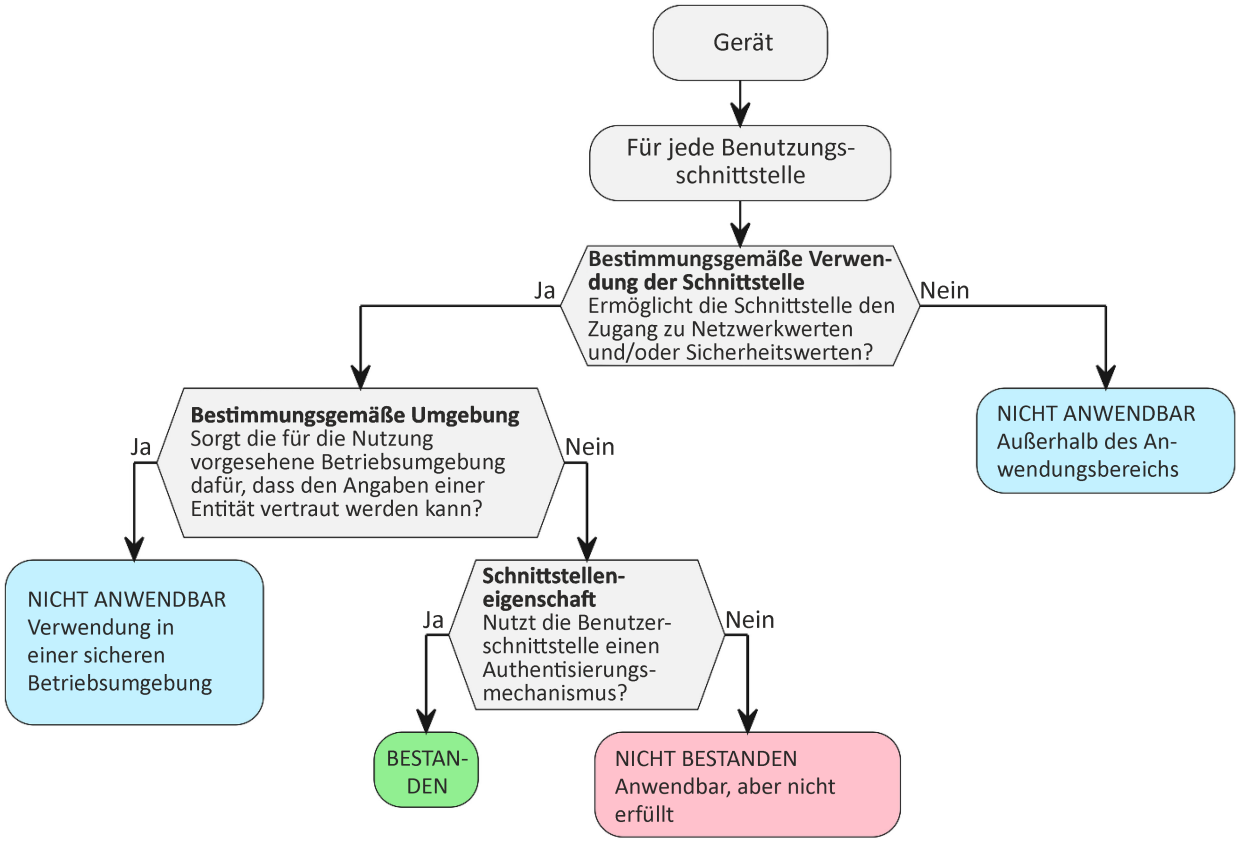

Bild 3 — Entscheidungsbaum für Anforderung AUM-1-2

Für jede in [E.Doc.UserInterfaces.AUM-1-2] dokumentierte Benutzungsschnittstelle, für den Zugang zu den in [E.Doc.SecurityAsset.AUM-1-2] dokumentierten Sicherheitswerten und/oder den in [E.Doc.NetworkAsset.AUM-1-2] dokumentierten Netzwerkwerten, für die in [E.Doc.OperationalEnvironment] dokumentierte, für die Nutzung vorgesehene Betriebsumgebung und die in [E.Doc.AUM-1-2] dokumentierten Authentisierungsmechanismen ist zu prüfen, ob der in [E.Doc.DT.AUM-2-1] dokumentierte Pfad durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.AUM-1-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-1-2] dokumentierte Begründung zu untersuchen.

5.2.1.6.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.2.1.6.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.2.1.6.5 Beurteilung der funktionalen Suffizienz

Keine.

5.2.2 [AUM-2] Angemessene Authentisierungsmechanismen für externe Schnittstellen

5.2.2.1 Anforderung

Für jeden Zugang zu Sicherheits- und/oder Netzwerkwerten, für den aufgrund von AUM-1-1 (Netzwerkschnittstelle) oder AUM-1-2 (Benutzungsschnittstelle) ein Authentisierungsmechanismus erforderlich ist, muss die Angabe der Entität verifiziert werden, indem mindestens ein Element aus den Kategorien Wissen, Besitz und Inhärenz durch mindestens einen Authentisierungsmechanismus geprüft wird (Ein-Faktor-Authentisierung).

5.2.2.2 Begründung

Die Ein-Faktor-Authentisierung eignet sich zum Schutz der Netzwerkressourcen eines Geräts gegen Missbrauch, z. B. im Verlauf eines DoS-Angriffs. Darüber hinaus müssen personenbezogene Daten auf dem Gerät mindestens durch Ein-Faktor-Authentisierung geschützt werden, insbesondere gegen Manipulation und Diebstahl.

Wenn die Hauptnutzung des Geräts spezifisch die Verarbeitung sensibler Daten ist, ist ein höherer Schutz erforderlich, da die Offenlegung schwerwiegende Auswirkungen haben könnte. In diesem Fall ist mindestens eine Zwei-Faktor-Authentisierung erforderlich. Bei Geräten, deren allgemeiner Zweck die Verarbeitung von Daten ist, die nur möglicherweise sensible personenbezogene Daten umfassen könnten, wie beispielsweise Desktop-PCs, Smartphones, Kameras oder Drucker, muss nur ein Schutz der personenbezogenen Daten vorgesehen werden. Allgemein ist es beim Design von Geräten zur Speicherung personenbezogener Daten vernünftig, die Bereitstellung einer Multifaktor-Authentisierung in Betracht zu ziehen.

5.2.2.3 Leitlinie

Beispiele für die Verifizierung der Angaben einer Entität durch Prüfung von Nachweisen eines Elements aus den Kategorien Wissen, Besitz und Inhärenz:

— PIN-Code, genutzt für die Benutzungsschnittstelle;

— 1-Faktor-Authentisierung (z. B. durch Passwort) für jede, an einer Schnittstelle eingehende Verbindung.

Vertrauensverhältnis zu einem Netzwerk (z. B. aufgrund eines gemeinsamen Geheimnisses), das bei der Verbindungsaufnahme etabliert wurde.

Beispiele für die Verifizierung der Angaben einer Entität durch Untersuchung der Nachweise von mindestens zwei verschiedenen Elementen aus den Kategorien Wissen, Besitz und Inhärenz:

— Passwort + OTP;

— PIN + Smartcard;

— Passwort + Token.

Ein wichtiger Aspekt bei der Implementation angemessener Authentisierungsmechanismen ist die Berücksichtigung möglicher Einschränkungen von menschlichen Benutzern mit Behinderungen.

Aktuell gelten lange Passwörter wie „Weihnachtsmarkt2023@Bonn“ als besser als kurze Passwörter wie „P@ssw0rd!“.

Weitere Leitlinien zu bewährten Verfahrensweisen für Passwörter sind in der NIST Sonderveröffentlichung 800-63B [8], in EN ISO/IEC 27002:2022 [3], EN ISO/IEC 24760 [4], EN IEC 62443-4-2 [2] und in ETSI EN 303 645 [5] zu finden.

5.2.2.4 Beurteilungskriterien

5.2.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-2.

5.2.2.4.2 Erforderliche Informationen

[E.Doc.DT.AUM-2] Beschreibung des gewählten Pfads durch den in Bild 5 dargestellten Entscheidungsbaum für jeden Authentisierungsmechanismus, der Sicherheits- und/oder Netzwerkwerte betrifft.

[E.Just.DT.AUM-2] Begründung des gewählten Pfads durch den in Bild 5 dargestellten Entscheidungsbaum für jeden Authentisierungsmechanismus, der Sicherheits- und/oder Netzwerkwerte schützt.

[E.Doc.SecurityAsset.AUM-2] Dokumentation jedes Sicherheitswerts, der über Netzwerkschnittstellen und/oder Benutzungsschnittstellen zugänglich ist.

[E.Doc.NetworkAsset.AUM-2] Dokumentation jedes Netzwerkwerts, der über Netzwerkschnittstellen und/oder Benutzungsschnittstellen zugänglich ist.

[E.Doc.AUM] Beschreibung aller Authentisierungsmechanismen für jeden Pfad für den Zugriff auf in [E.Doc.SecurityAsset.AUM-2] dokumentierte Sicherheitswerte und/oder in [E.Doc.NetworkAsset.AUM-2] dokumentierte Netzwerkwerte, einschließlich aller Netzwerkschnittstellen und/oder Benutzungsschnittstellen.

5.2.2.4.3 Konzeptuelle Beurteilung

5.2.2.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle Authentisierungsmechanismen für Sicherheits- und/oder Netzwerkwerte in jedem Pfad die erforderlichen Eigenschaften haben.

5.2.2.4.3.2 Voraussetzungen

Keine.

5.2.2.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  : For each access to security and/or network assets;
    if (<b>authentication mechanism property:</b>\nDoes at least one
   authentication mechanism on the path use \nat least one factor
   authentication to verify an entities' claim?) then (Yes)
      #lightgreen :PASS\nAuthentication mechanisms\nare appropriate;
      detach;
    else (No)
      #pink :FAIL\nAuthentication mechanisms\nare not appropriate;
      detach;
```

```
    endif
@enduml
```

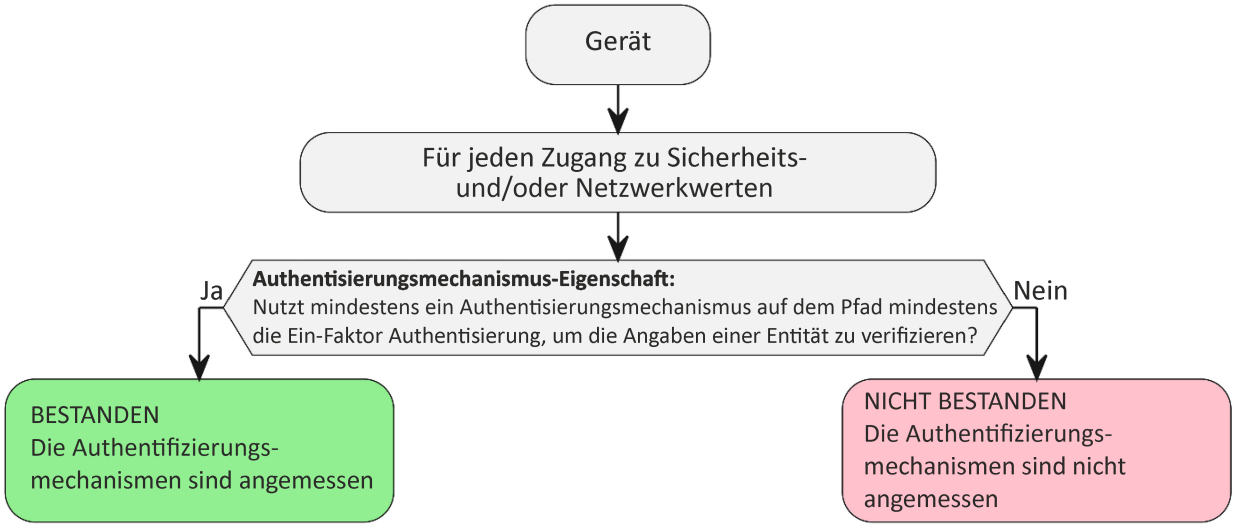

Bild 4 — Entscheidungsbaum für Anforderung AUM-2

Für jeden in [E.Doc.AUM] dokumentierten Authentisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.AUM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.ACM-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Doc.DT.AUM-2] dokumentierte Begründung zu untersuchen.

5.2.2.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „BESTANDEN“ enden; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— kein Authentisierungsmechanismus für den Schutz von Sicherheits- und/oder Netzwerkwerten erforderlich ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.2.2.4.4 Beurteilung der funktionalen Vollständigkeit

5.2.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation der Authentisierungsmechanismen vollständig ist.

5.2.2.4.4.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.2.2.4.4.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob Authentisierungsmechanismen existieren, die nicht in [E.Doc.AUM] aufgeführt sind.

5.2.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen Authentisierungsmechanismen in [E.Doc.AUM] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein gefundener Authentisierungsmechanismus nicht in [E.Doc.AUM] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.2.2.4.5 Beurteilung der funktionalen Suffizienz

5.2.2.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob mindestens eine Authentisierung in jedem Pfad zu Netzwerk- und/oder Sicherheitswerten die erforderlichen Eigenschaften hat.

5.2.2.4.5.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.2.2.4.5.3 Beurteilungseinheiten

Für jeden in [E.Doc.AUM] dokumentierten Authentisierungsmechanismus ist der Betrieb des Authentisierungsmechanismus wie in [E.Doc.AUM] dokumentiert funktional zu bestätigen.

5.2.2.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Authentisierungsmechanismen von [E.Doc.AUM] abweichen.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Authentisierungsmechanismen von [E.Doc.AUM] abweichen.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.2.3 [AUM-3] Authentifikator-Validierung

5.2.3.1 Anforderung

Jeder Authentisierungsmechanismus, der AUM-1 unterliegt, muss abhängig von den in der verwendeten Betriebsumgebung verfügbaren Informationen, alle relevanten Eigenschaften der verwendeten Authentifikatoren validieren.

5.2.3.2 Begründung

Auch wenn das Gerät einen Authentisierungsmechanismus bereitstellt, besteht das Risiko, dass ein Angreifer eine typische Design-Schwachstelle zu dessen Überwindung nutzt. Ein üblicher Angriff gegen solche Mechanismen beruht auf der Nutzung gefälschter oder teilweise gefälschter Authentifikatoren. Daher sind beim Sicherheitsdesign von Mechanismen Techniken erforderlich, um gefälschten Authentifikatoren, beispielsweise manipulierten PKI-Zertifikaten, zu widerstehen.

5.2.3.3 Leitlinie

Der Authentifikator und seine Attribute können sich je nach Authentisierungsmechanismus unterscheiden. Für die Validierung des Authentifikators sollten bewährte Verfahrensweisen angewendet werden; diese sind üblicherweise in einer Norm für das entsprechende Authentisierungsprotokoll beschrieben. Dies ist erforderlich, um die Verwendung von gefälschten Authentifikatoren zu erkennen und zu verhindern. Wenn ein Gerät beispielsweise nur einen Textvergleich des gemeinsamen Namens eines PKI-Zertifikats durchführt, ohne zusätzlich die vollständigen Zertifikatinformationen zu validieren, würde ein entsprechend gefälschter Authentifikator akzeptiert. In diesem Beispiel wären die maßgeblichen Eigenschaften die Signaturen und öffentlichen Schlüssel der Vertrauenskette, und in vielen Fällen auch die Validität des Zertifikats. Der Satz maßgeblicher Eigenschaften kann sich abhängig davon unterscheiden, ob das Gerät tatsächlich mit dem Internet verbunden ist oder nicht. Beispielsweise hat ein nicht verbundenes Gerät möglicherweise keinen Zugang zu einer zuverlässigen Zeitquelle oder zu Sperrinformationen für Zertifikate.

Ein weiteres Beispiel ist die nur teilweise Validierung von Passwörtern. Dies würde die Passwortstärke schwächen und so Brute-Force-Angriffe auf den entsprechenden Authentisierungsmechanismus erleichtern.

5.2.3.4 Beurteilungskriterien

5.2.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-3.

5.2.3.4.2 Erforderliche Informationen

[E.Doc.DT.AUM-3] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 6 für jeden Authentisierungsmechanismus.

[E.Just.DT.AUM-3] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 6 für jeden Authentisierungsmechanismus.

[E.Doc.AUM] Beschreibung aller Authentisierungsmechanismen für jeden Pfad zum Zugriff auf Sicherheits- und Netzwerkwerte, einschließlich Benutzungsschnittstelle und Netzwerkschnittstellen.

[E.Doc.AuthVal] Beschreibung, wie die Validierung des Authentifikators bei allen Authentisierungsmechanismen durchgeführt wird, unter Berücksichtigung der verfügbaren Informationen über den Authentifikator in der genutzten Betriebsumgebung.

5.2.3.4.3 Konzeptuelle Beurteilung

5.2.3.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Authentisierungsmechanismen auf jedem Pfad zu den Sicherheits- und/oder Netzwerkwerten die erforderlichen Eigenschaften haben.

5.2.3.4.3.2 Voraussetzungen

Keine.

5.2.3.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each path to security and network assets;
```

```
    if (<b>authentication mechanism property</b>:\nDoes the authentication
   mechanism validate all relevant properties \nconsidering the available
   information about the authenticator in \nthe operational environments of
   use?) then (Yes)
      #lightgreen :PASS\nAuthenticator validation \nis appropriate;
      detach;
    else (No)
      #pink :FAIL\nAuthenticator validation \nis inappropriate;
      detach;
    endif
@enduml
```

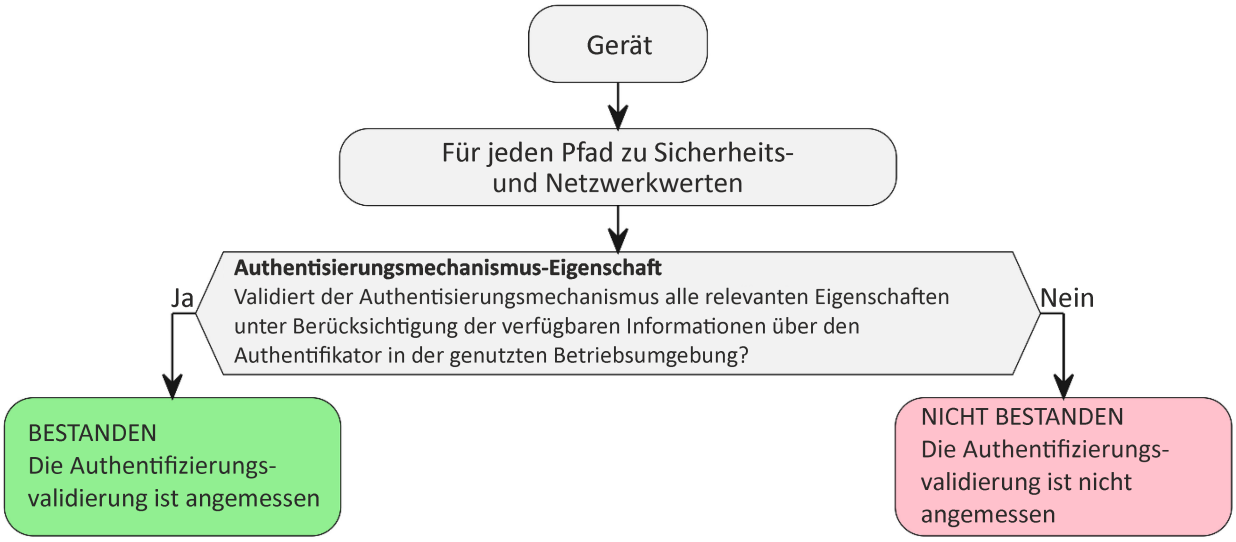

Bild 5 — Entscheidungsbaum für Anforderung AUM-3

Für jeden in [E.Doc.AUM] dokumentierten Authentisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.AUM-3] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.ACM-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Doc.DT.AUM-3] dokumentierte Begründung zu untersuchen.

5.2.3.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „BESTANDEN“ enden; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— kein Authentisierungsmechanismus für den Schutz von Netzwerk- und/oder Sicherheitswerten erforderlich ist (siehe 5.2.1).

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.2.3.4.4 Beurteilung der funktionalen Vollständigkeit

5.2.3.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation der Authentisierungsmechanismen vollständig ist.

5.2.3.4.4.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.2.3.4.4.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob Authentisierungsmechanismen existieren, die nicht in [E.Doc.AUM] aufgeführt sind.

5.2.3.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen Authentisierungsmechanismen in [E.Doc.AUM] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein gefundener Authentisierungsmechanismus nicht in [E.Doc.AUM] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.2.3.4.5 Beurteilung der funktionalen Suffizienz

5.2.3.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob alle Authentisierungsmechanismen auf jedem Pfad zu Netzwerk- und/oder Sicherheitswerten die erforderlichen Eigenschaften haben.

5.2.3.4.5.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.2.3.4.5.3 Beurteilungseinheiten

Für jeden in [E.Doc.AUM] dokumentierten Authentisierungsmechanismus ist die Funktionsweise der Validierung von Authentifikatoren, wie in [E.Doc.AuthVal] dokumentiert, funktional zu bestätigen.

5.2.3.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Validierung des Authentifikators von [E.Doc.AuthVal] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Validierung des Authentifikators von [E.Doc.AuthVal] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.2.4 [AUM-4] Änderung von Authentifikatoren

5.2.4.1 Anforderung

Jeder Authentisierungsmechanismus, der AUM-1 unterliegt, muss die Änderung des Authentifikators zulassen, außer widersprechende Sicherheitsziele erlauben keine Änderung.

5.2.4.2 Begründung

Nicht änderbare Authentifikatoren stellen ein Risiko für den sicheren Betrieb des Geräts dar, z. B. indem sie die Anfälligkeit für Brute-Force- und Abhörangriffe erhöhen. Daher ist als Gegenmaßnahme eine Unterstützung zur Änderung der Authentifikatoren auf dem Gerät erforderlich.

5.2.4.3 Leitlinie

Eine autorisierte Einheit muss eine Möglichkeit zur Änderung des Authentifikators haben. Das Verfahren kann sich je nach Authentisierungsmechanismus unterscheiden.

— Das Gerät stellt der autorisierten Entität, z. B. dem Benutzer, eine Funktionalität zur Änderung des Authentifikators auf dem Gerät zur Verfügung.

— Der Authentifikator, z. B. der Token, wird vom Hersteller erneuert oder ausgetauscht, und das Gerät akzeptiert den geänderten Authentifikator, weil die Vertrauenskette nach wie vor gültig ist.

— Der Authentifikator wird mithilfe eines sicheren Aktualisierungsmechanismus aktualisiert.

Bei Maschinenschnittstellen kann beispielsweise eine erneute Kopplung erforderlich sein. Bei Benutzungsschnittstellen, bei denen beispielsweise ein Fingerabdruck, ein Passwort oder ein anderer Token genutzt wird, erleichtert die Einbindung der Funktionalität in den üblichen Arbeitsablauf eine einfache Implementation.

Es kann Ausnahmen geben, bei denen ein Authentifikator statisch ist, beispielsweise eine Vertrauensgrundlage, bei der die Vertraulichkeit des entsprechenden kryptographischen Schlüssels durch den Hersteller sichergestellt wird. In solchen Fällen stellt der Hersteller üblicherweise Tokens für autorisierte Entitäten zur Verfügung, die alle mit der gleichen Vertrauensgrundlage verbunden sind.

Es kann Ausnahmen geben, bei denen das Gesamtrisiko für die Geräte durch die Änderung eines Authentifikators, z. B. aufgrund der Komplexität, höher ist als das mit der Nutzung statischer Authentifikatoren verbundene Risiko. In einem solchen Fall sollten „bewährte Verfahrensweisen für Sicherheits-Design-Grundsätze“ befolgt werden, um das mit dem statischen Authentifikator verbundene Risiko möglichst gering zu halten, z. B. indem keine globalen Authentifikatoren verwendet werden.

Je nach der beabsichtigten Nutzung des Geräts kann es erforderlich sein, die Gerätefunktionalität durch eine Rückstellungsmöglichkeit sicherzustellen, indem z. B. keine Passwortaktualisierung während der Autofahrt erzwungen wird.

5.2.4.4 Beurteilungskriterien

5.2.4.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-4.

5.2.4.4.2 Erforderliche Informationen

[E.Doc.DT.AUM-4] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 7 für jede Authentifikator-Änderungsfunktionalität.

[E.Just.DT.AUM-4] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 7 für jede Authentifikator-Änderungsfunktionalität.

[E.Doc.AUM] Beschreibung aller Authentisierungsmechanismen für jeden Pfad zum Zugriff auf Sicherheits- und Netzwerkwerte, einschließlich Benutzungsschnittstelle und Netzwerkschnittstellen.

[E.Doc.AuthChange] Beschreibung, wie die Änderung des Authentifikators bei allen Authentisierungsmechanismen durchgeführt wird, unter Berücksichtigung des Sicherheitskonzepts des Geräts.

5.2.4.4.3 Konzeptuelle Beurteilung

5.2.4.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Authentisierungsmechanismen auf jedem Pfad zu den Sicherheits- und/oder Netzwerkwerten die erforderlichen Eigenschaften haben.

5.2.4.4.3.2 Voraussetzungen

Keine.

5.2.4.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each path to security and/or network assets;
    if (<b>Equipment security concept:</b>\nDoes the change of the
   authenticatior \nconflict security goals?) then (Yes)
    #application:NOT APPLICABLE\nStatic for security reasons;
    detach;
    else(No)
    if (<b>Authentication mechanism property:</b>\nDoes the authentication
   mechanism allow \nthe change of the authenticator?) then (Yes)
      #lightgreen :PASS\nAuthenticator changeable;
      detach;
    else (No)
      #pink :FAIL\nAuthenticator not changeable;
      detach;
    endif
@enduml
```

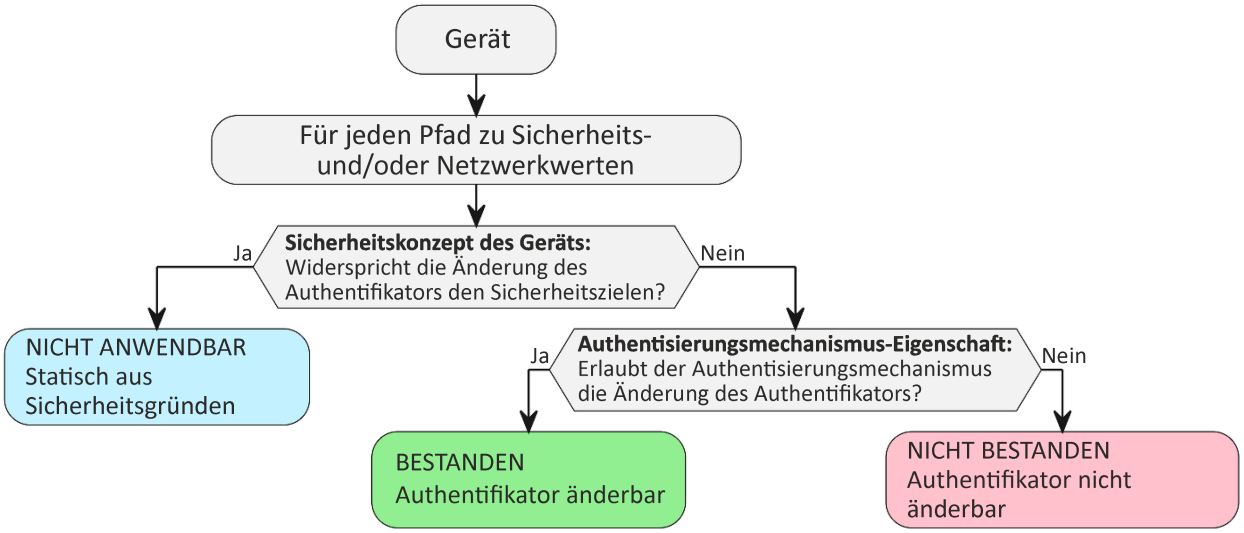

Bild 6 — Entscheidungsbaum für Anforderung AUM-4

Für jede in [E.Doc.AUM] dokumentierte Authentifikator-Änderungsfunktionalität ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.AUM-4] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.AUM-4] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Doc.DT.AUM-4] dokumentierte Begründung zu untersuchen.

5.2.4.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „BESTANDEN“ enden; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— kein Authentisierungsmechanismus für den Schutz von Netzwerk- und/oder Sicherheitswerten erforderlich ist (siehe 5.2.1).

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.2.4.4.4 Beurteilung der funktionalen Vollständigkeit

5.2.4.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation der Authentisierungsmechanismen vollständig ist.

5.2.4.4.4.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.2.4.4.4.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob Authentisierungsmechanismen existieren, die nicht in [E.Doc.AUM] aufgeführt sind.

5.2.4.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen Authentisierungsmechanismen in [E.Doc.AUM] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein gefundener Authentisierungsmechanismus nicht in [E.Doc.AUM] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.2.4.4.5 Beurteilung der funktionalen Suffizienz

5.2.4.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob alle Authentisierungsmechanismen auf jedem Pfad zu Netzwerk- und/oder Sicherheitswerten die erforderlichen Eigenschaften haben.

5.2.4.4.5.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.2.4.4.5.3 Beurteilungseinheiten

Für jeden in [E.Doc.AUM] dokumentierten Authentisierungsmechanismus ist die Änderung des Authentifikators wie in [E.Doc.AuthChange] dokumentiert funktional zu bestätigen.

5.2.4.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Änderung des Authentifikators von [E.Doc.AuthChange] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Änderung des Authentifikators von [E.Doc.AuthChange] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.2.5 [AUM-5] Verhinderung von statischen und Vorgabewerten

5.2.5.1 Anforderung

Wenn ein Authentisierungsmechanismus, der AUM-1-2 unterliegt, Passwörter verwendet, müssen diese:

— im Fall einer Werksvoreinstellung faktisch eindeutig für jedes Gerät sein; oder

— die Einstellung durch den Benutzer muss bei der ersten Benutzung erzwungen werden, wenn das Gerät logisch oder physisch von nicht vertrauenswürdigen Netzen getrennt ist; und

— in jedem Fall sind bezüglich der Stärke bewährte Verfahrensweisen einzuhalten.

ANMERKUNG Zu den Passwörtern zählen auch PIN-Codes.

5.2.5.2 Begründung

Universelle Passwörter stellen einen der am meisten ausgenutzten Angriffsvektoren bei Geräten dar. Es existiert ein breites Spektrum an Schadsoftware, die solche Passwörter zur automatischen Kompromittierung von Geräten nutzt. Daher ist die Verwendung individueller Passwörter bei der ersten Benutzung von Geräten wesentlich.

5.2.5.3 Leitlinie

Es gibt unterschiedliche Techniken, um universelle Passwörter zu vermeiden; Beispiele sind:

— Das vom Werk voreingestellte Passwort des Geräts ist auf einen Aufkleber unten am Gerätegehäuse aufgedruckt. Das Passwort wird durch einen Hardware-Zufallsgenerator oder eine andere kryptographisch sichere Implementation eines Pseudo-Zufallszahlengenerators (CSPRNG) erzeugt.

— Das Gerät fordert den Benutzer auf, bei der ersten Benutzung ein Passwort zu erstellen.

Leitlinien zu bewährten Verfahrensweisen für Passwörter sind in der NIST Sonderveröffentlichung 800-63B [8], in EN ISO/IEC 27002:2022 [3], EN ISO/IEC 24760 [4], in EN IEC 62443-4-2 [2] und in ETSI EN 303 645 [5] zu finden.

Eindeutig bedeutet, dass das Passwort nicht systematisch wiederverwendet wird oder für ein anderes Gerät des gleichen Produkttyps abgeleitet werden kann, und dass es nicht einfach von den Eigenschaften des Geräts (z. B. dem Herstellernamen, dem Modellnamen oder der Media Access Control-(MAC-)Adresse) abgeleitet werden kann. Ein gängiger Zufallsgenerator kann verwendet werden, um faktisch eindeutige Passwörter zu erzeugen.

Bei der Erzwingung einer Passwortänderung sind auch Sicherheitsaspekte relevant. Beispielsweise darf keine Erzwingung einer Passwortänderung während der Autofahrt erfolgen.

5.2.5.4 Beurteilungskriterien

5.2.5.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-5.

5.2.5.4.2 Erforderliche Informationen

[E.Doc.DT.AUM-5] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 8 für jeden Authentisierungsmechanismus.

[E.Just.DT.AUM-5] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 8 für jeden Authentisierungsmechanismus.

[E.Doc.AUM] Beschreibung aller Authentisierungsmechanismen für jeden Pfad zum Zugriff auf Sicherheits- und Netzwerkwerte, einschließlich Benutzungsschnittstelle und Netzwerkschnittstellen.

[E.Doc.PwdProperty] Beschreibung, wie für alle Authentisierungsmechanismen, die Passwörter nutzen, die faktische Eindeutigkeit des Passworts implementiert ist oder wie die Änderung des Passworts bei der ersten Benutzung erzwungen wird. Die Dokumentation enthält auch den Parameter der einzuhaltenden Passwortstärke.

5.2.5.4.3 Konzeptuelle Beurteilung

5.2.5.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Authentisierungsmechanismen auf jedem Pfad zu den Sicherheits- und/oder Netzwerkwerten die erforderlichen Eigenschaften haben.

5.2.5.4.3.2 Voraussetzungen

Keine.

5.2.5.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
    if (<b>Equipment property:</b>\nAre passwords used?) then (Yes)
     :For each path to security and network assets;
     if (<b>Password property:</b>\nIs the password practically \nunique per
   equipment \nin factory default) then (Yes)
      #lightgreen :PASS\nPassword is \npractically unique;
      detach;
     else(No)
      if(<b>Operational environment:</b>\nEquipment is logically \nor
   physically separated \nfrom untrusted networks?) then (No)
       #pink :FAIL\nInappropriate \nenvoirnment;
       detach;
      else(Yes)
       if(<b>AuthMech property:</b>\nIs setting a new \npassword enforced
   \non first use?) then (Yes)
```

```
        #lightgreen :PASS\nSetting of a \nnew password is \nenforced on
    first use;
        detach;
       else(No)
        #pink :FAIL\nSetting of a \nnew password is \nenforced on first use;
        detach;
       endif
      endif
     endif
     detach;
    else(No)
    #application:NOT APPLICABLE\nNo passwords used;
    detach;
    endif
@enduml
```

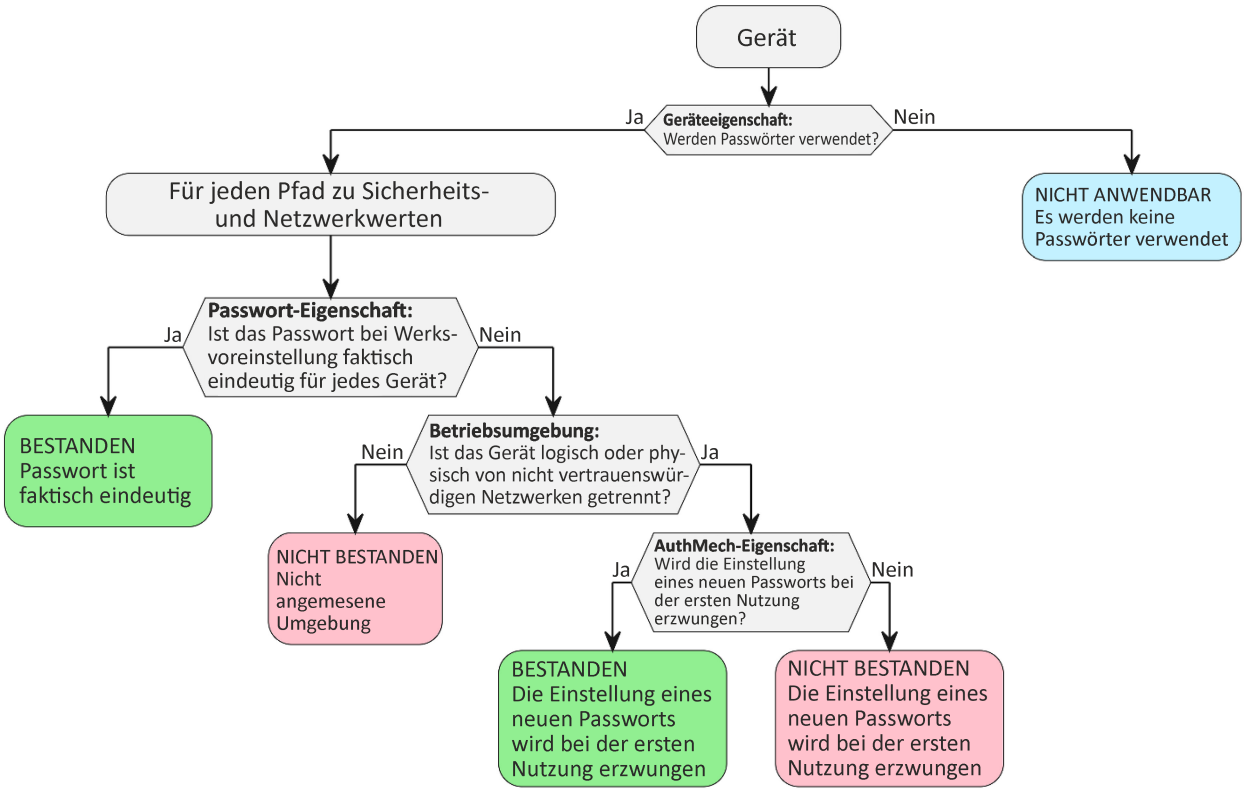

Bild 7 — Entscheidungsbaum für Anforderung AUM-5

Für jeden in [E.Doc.AUM] dokumentierten Authentisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.AUM-5] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.ACM-5] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-5] dokumentierte Begründung zu untersuchen.

5.2.5.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „BESTANDEN“ enden; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— kein Authentisierungsmechanismus für den Schutz von Netzwerk- und/oder Sicherheitswerten erforderlich ist (siehe AUM-1).

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.2.5.4.4 Beurteilung der funktionalen Vollständigkeit

5.2.5.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation der Authentisierungsmechanismen vollständig ist.

5.2.5.4.4.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.2.5.4.4.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob Authentisierungsmechanismen existieren, die nicht in [E.Doc.AUM] aufgeführt sind.

5.2.5.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen Authentisierungsmechanismen in [E.Doc.AUM] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein gefundener Authentisierungsmechanismus nicht in [E.Doc.AUM] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.2.5.4.5 Beurteilung der funktionalen Suffizienz

5.2.5.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob alle Authentisierungsmechanismen auf jedem Pfad zu Netzwerk- und/oder Sicherheitswerten die erforderlichen Eigenschaften haben.

5.2.5.4.5.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.2.5.4.5.3 Beurteilungseinheiten

Für jeden in [E.Doc.AUM] dokumentierten Authentisierungsmechanismus, der Passwörter nutzt, sind die in [E.Doc.PwdProperty] dokumentierten Passworteigenschaften und die damit verbundenen Funktionalitäten funktional zu bestätigen.

5.2.5.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Validierung des Authentifikators von [E.Doc.PwdProperty] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Validierung des Authentifikators von [E.Doc.PwdProperty] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.2.6 [AUM-6] Schutz vor Brute-Force-Angriffen

5.2.6.1 Anforderung

Das Gerät muss Brute-Force-Angriffen auf die Authentisierungsmechanismen gegenüber resilient sein, die AUM-1 unterliegen.

5.2.6.2 Begründung

Ein Angreifer kann versuchen, Massenauthentisierungsversuche zu nutzen, um einen Authentisierungsmechanismus zu überwinden oder um die Geräteverfügbarkeit zu beeinträchtigen. Daher sind Techniken erforderlich, um einen solchen Angriff einzudämmen.

5.2.6.3 Leitlinie

Es gibt eine Reihe von Techniken, die darauf abzielen, erfolgreiche Brute-Force-Angriffe praktisch unmöglich zu machen.

Zu den Techniken, die die Wahrscheinlichkeit eines erfolgreichen Brute-Force-Angriffs verringern, gehören beispielsweise:

— Zeitverzögerungen zwischen aufeinanderfolgenden fehlgeschlagenen Authentisierungsversuchen;

— eine begrenzte Anzahl fehlgeschlagener Authentisierungsversuche, gefolgt von einer Sperrzeit, während der keine Anmeldung zulässig ist;

— Multifaktor-Authentisierung;

— eine angemessene Entropie für Authentisierungswerte auf der Grundlage bewährter Verfahrensweisen für Kryptographie;

ANMERKUNG Eine angemessene Entropie wird bestimmt durch die Länge und den Inhalt des Werts unter Berücksichtigung des möglichen Zeichensatzes und der Anzahl an Versuchen, bevor die Brute-Force-Abwehr aktiviert wird.

— abhängig von den implementierten Techniken sind Risiken in Bezug auf das „Aufbrauchen von Ressourcen“ und „Denial-of-Service“ zu berücksichtigen.

Auch ist die Abwehr von wiederholten Versuchen zum Erlangen einer rechtswidrigen Authentisierung und die Abwehr des Blockierens von legitimen Zugriffen durch das Auslösen vorgeschalteter Abwehrmechanismen zu berücksichtigen.

Siehe NIST 800-63 Reihe [7].

5.2.6.4 Beurteilungskriterien

5.2.6.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung AUM-6.

5.2.6.4.2 Erforderliche Informationen

[E.Doc.DT.AUM-6] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 9 für jeden Authentisierungsmechanismus.

[E.Just.DT.AUM-6] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 9 für jeden Authentisierungsmechanismus.

[E.Doc.AUM] Beschreibung aller Authentisierungsmechanismen für jeden Pfad zum Zugriff auf Sicherheits- und Netzwerkwerte, einschließlich Benutzungsschnittstelle und Netzwerkschnittstellen.

[E.Doc.BFProtection] Beschreibung, wie bei allen Authentisierungsmechanismen die Resilienz gegen Brute-Force-Angriffe sichergestellt wird.

5.2.6.4.3 Konzeptuelle Beurteilung

5.2.6.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Authentisierungsmechanismen auf jedem Pfad zu den Sicherheits- und/oder Netzwerkwerten die erforderlichen Eigenschaften haben.

5.2.6.4.3.2 Voraussetzungen

Keine.

5.2.6.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each path to security and/or network assets;
    if (<b>Authentication mechanism property:</b>\nIs the authentication
   mechanism \nresilient against brute force attacks?) then (Yes)
      #lightgreen :PASS\nIs resilient ;
      detach;
    else (No)
      #pink :FAIL\nIs not resilient;
      detach;
    endif
@enduml
```

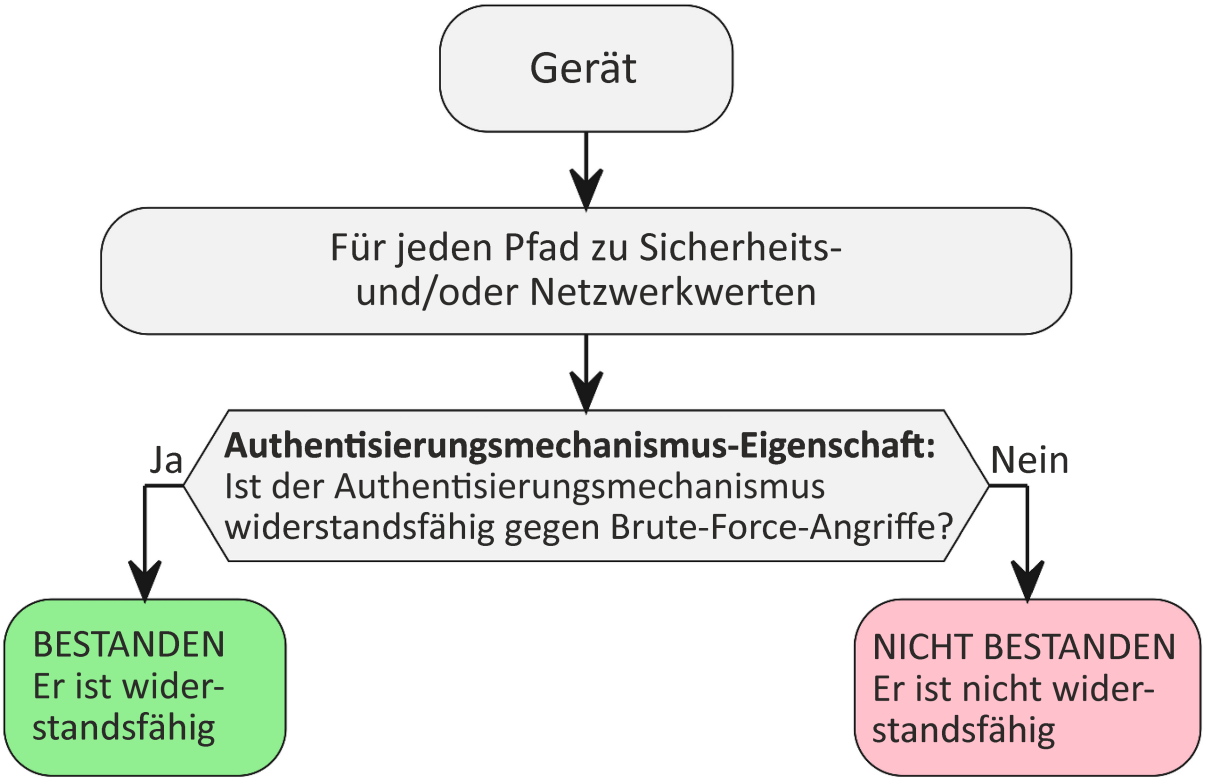

Bild 8 — Entscheidungsbaum für Anforderung AUM-6

Für jeden in [E.Doc.AUM] dokumentierten Authentisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.AUM-6] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.AUM-6] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.AUM-6] dokumentierte Begründung zu untersuchen.

5.2.6.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „BESTANDEN“ enden; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— kein Authentisierungsmechanismus für den Schutz von Netzwerk- und/oder Sicherheitswerten erforderlich ist (siehe 5.2.1).

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.2.6.4.4 Beurteilung der funktionalen Vollständigkeit

5.2.6.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation der Authentisierungsmechanismen vollständig ist.

5.2.6.4.4.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.2.6.4.4.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob Authentisierungsmechanismen existieren, die nicht in [E.Doc.AUM] aufgeführt sind.

5.2.6.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen Authentisierungsmechanismen in [E.Doc.AUM] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein gefundener Authentisierungsmechanismus nicht in [E.Doc.AUM] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.2.6.4.5 Beurteilung der funktionalen Suffizienz

5.2.6.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob alle Authentisierungsmechanismen auf jedem Pfad zu Netzwerk- und/oder Sicherheitswerten die erforderlichen Eigenschaften haben.

5.2.6.4.5.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.2.6.4.5.3 Beurteilungseinheiten

Für jeden in [E.Doc.AUM] dokumentierten Authentisierungsmechanismus ist die Resilienz gegen Brute-Force-Angriffe (vergleiche 5.2.6.3) [E.Doc.BFProtection] funktional zu bestätigen.

5.2.6.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Anzeichen vorliegt, dass der Schutz vor Brute-Force-Angriffen von [E.Doc.BFProtection] abweicht.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass der Schutz vor Brute-Force-Angriffen von [E.Doc.BFProtection] abweicht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.3 [SUM] Sicherer Aktualisierungmechanismus (en: Secure Update Mechanism)

5.3.1 [SUM-1] Anwendbarkeit von Aktualisierungsmechanismen

5.3.1.1 Anforderung

Das Gerät muss über mindestens einen Aktualisierungsmechanismus für die Aktualisierung jedes Softwareteils verfügen, der die Sicherheits- und/oder Netzwerkwerte betrifft, außer:

— Auswirkungen auf die funktionale Sicherheit erlauben keine Aktualisierungsfähigkeit; oder

— die Software ist aus Sicherheitsgründen unveränderlich; oder

— es existieren alternative Maßnahmen, die die Sicherheitswerte und/oder Netzwerkwerte während des gesamten Lebenszyklus des Geräts schützen.

Wenn die oben genannten Ausnahmen für die gesamte Software des Geräts gelten, ist kein Aktualisierungsmechanismus erforderlich.

5.3.1.2 Begründung

Die Fähigkeit zur Bereitstellung und Implementierung von Software-Aktualisierungen über einen Aktualisierungsmechanismus ist grundlegend wichtig für eine gute Gerätewartung und um Sicherheitsschwachstellen einzudämmen, die bei Ausnutzung zur Kompromittierung des Geräts verwendet werden und damit dem Netzwerk oder dessen Funktion schaden könnten, oder die durch den Missbrauch von Netzwerkressourcen zu einer nicht annehmbaren Verschlechterung von Diensten führen könnten.

Allerdings können manche Softwareteile aus Sicherheitsgründen unveränderlich und somit nicht aktualisierbar sein, oder Auswirkungen auf die funktionale Sicherheit erlauben keine Aktualisierbarkeit. Schwachstellen können auch durch andere Maßnahmen eingedämmt werden, beispielsweise durch den Austausch von anfälligen Geräten während des gesamten Lebenszyklus oder durch die sichere Eindämmung mittels anderer Geräte, die den Schutz der Werte sicherstellen.

5.3.1.3 Leitlinie

Es kann mehr als ein Aktualisierungsmechanismus für verschiedene Teile der Gerätesoftware vorhanden sein.

Es ist möglich, dass nicht die gesamte Software des Geräts aktualisierbar ist. Dies kann Software betreffen, die sich aus Sicherheitsgründen oder zur Erfüllung funktionaler Sicherheitsanforderungen im schreibgeschützten Speicher befindet.

In manchen Fällen sind alternative Maßnahmen zur Verhinderung von Schäden durch potentielle, öffentlich bekannte ausnutzbare Schwachstellen in Teilen der Gerätesoftware vorhanden, oder eine ausnutzbare Software-Schwachstelle gefährdet die Integrität des Geräts oder die zu schützenden Werte möglicherweise nicht. Zum Beispiel:

— Geräte, für die eine Austauschstrategie vorhanden ist, z. B. Geräte mit begrenzten Ressourcen (beispielsweise Sensoren, die viele Jahre batteriebetrieben laufen müssen); oder

— Geräte oder Software-Bestandteile, die bei der vorgesehenen Verwendung des Geräts sicher isoliert werden können und voraussichtlich werden; oder

— Software-Bestandteile, die mit eingeschränkten Privilegien laufen und die geschützten Werte nicht gefährden; oder

— Software(-Bestandteile), bei denen die bestimmungsgemäße Verwendung des Geräts und die vorgesehene Betriebsumgebung die Ausnutzung von Schwachstellen eindämmt.

Falls möglich, entspricht es bewährten Verfahren, einen Software-Aktualisierungsmechanismus zu implementieren, der eine Trennung zwischen sicherheitsbezogenen Software-Aktualisierungen und Anwendungssoftware-Aktualisierungen ermöglicht.

5.3.1.4 Beurteilungskriterien

5.3.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SUM-1.

5.3.1.4.2 Erforderliche Informationen

[E.Doc.DT.SUM-1] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 10 für jeden Teil der Software.

[E.Just.DT.SUM-1] Begründung für den gewählten Pfad durch den Entscheidungsbaum in Bild 10 für jeden Teil der Software.

[E.Doc.PartOfSoftw] Dokumentation für jeden Teil der Gerätesoftware.

ANMERKUNG Das vorliegende Dokument legt nicht die Granularität fest, mit der die Gerätesoftware untergliedert wird. Eine in Bezug auf den Dokumentationsaufwand geeignete Untergliederung berücksichtigt die Abdeckung der Softwareteile durch bestimmte Aktualisierungsmechanismen.

Wenn das Gerät über einen Aktualisierungsmechanismus für die Teile seiner Software verfügt, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind: [E.Doc.SUM] Vollständige Dokumentation des Aktualisierungsmechanismus für die Aktualisierung der Teile der Gerätesoftware, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind.

5.3.1.4.3 Konzeptuelle Beurteilung

5.3.1.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die Bestimmung, ob ein Aktualisierungsmechanismus implementiert wurde, falls er erforderlich ist.

5.3.1.4.3.2 Voraussetzungen

Das Gerät muss sich im Betriebszustand befinden.

5.3.1.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each part of the equipment's software;
if (<b>software part property:</b>\nDoes the part of the software affect
   security and/or network assets? ) then (Yes)
    if (Do functional safety implications prohibit updatability?) then (Yes)
        #application :NOT APPLICABLE\nFunctional safety implications;
        detach;
    else (No)
       if (Is the software is immutable for security reasons?) then (Yes)
           #application :NOT APPLICABLE\nImmutable for security;
           detach;
       else (No)
          if (Do alternative measures exist that protect security\nassets
   and/or network assets during the entire lifecycle?) then (Yes)
              #application :NOT APPLICABLE\nAlternative measures;
              detach;
          else (No)
      if (<b>software part property:</b>\nDoes the equipment provide at
   least\none update mechanism for updating\nthe part of the software? )
   then (No)
        #pink :FAIL\nSoftware is not updatable;
        detach;
```

```
      else (Yes)
        #lightgreen :PASS\nSoftware is updatable;
        detach;
      endif
          endif
       endif
    endif
else
     #application :NOT APPLICABLE\nSoftware does not \naffect asset;
     detach;
endif
@enduml
```

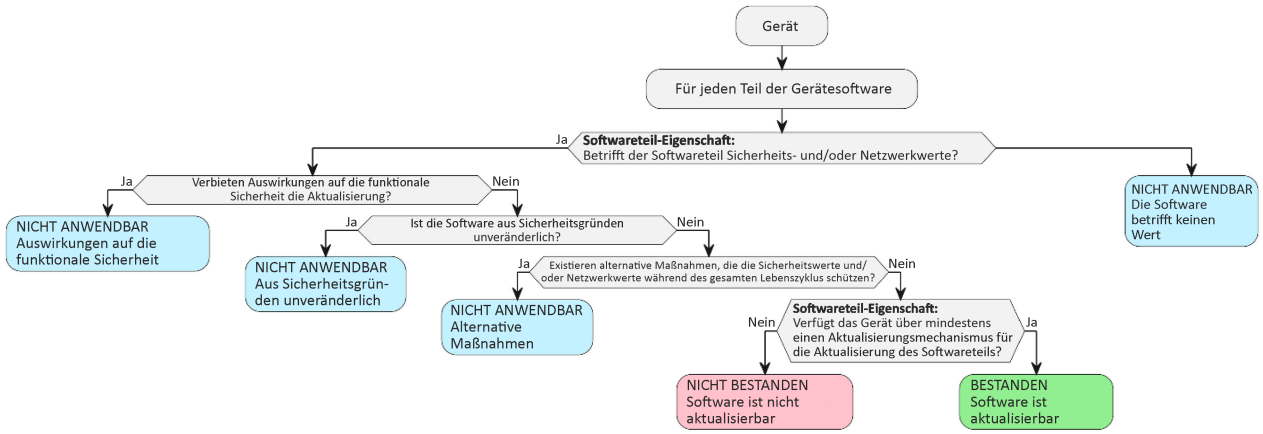

Bild 9 — Entscheidungsbaum für Anforderung SUM-1

Für jeden Teil der in [E.Doc.PartOfSoftw] dokumentierten Software ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.SUM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.SUM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SUM-1] dokumentierte Begründung zu untersuchen.

5.3.1.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle dokumentierten Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle dokumentierten Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle dokumentierten Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.3.1.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.3.1.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.3.2 [SUM-2] Sichere Aktualisierungen

5.3.2.1 Anforderung

Jeder Aktualisierungsmechanismus, der die Aktualisierung von Software ermöglicht, von der Sicherheits- und/oder Netzwerkwerte betroffen sind, darf nur Software installieren, deren Integrität und Authentizität zum Zeitpunkt der Installation gültig ist.

5.3.2.2 Begründung

Ein sicherer Software-Aktualisierungsmechanismus stellt sicher, dass die Software zur Kontrolle des Geräts nicht durch den Aktualisierungsmechanismus manipuliert wird.

5.3.2.3 Leitlinie

Ein häufiger Ansatz zur Bestätigung, dass eine Aktualisierung kryptographisch gültig ist, ist die Prüfung der Integrität und Authentizität anhand eines Vertrauensankers. Dies kann auf dem Gerät geschehen oder durch ein anderes vertrauenswürdiges Gerät, das die Verifizierung durchführt. Im letzteren Fall wird die verifizierte Aktualisierung üblicherweise über einen sicheren Kanal an das Gerät gesendet.

ANMERKUNG „Sichere Kanäle“ erhalten üblicherweise die Sicherheitseigenschaften der übertragenen Informationen und können auch beinhalten, dass autorisierte und authentifizierte Personen die validierte Software-Aktualisierung lokal bereitstellen (Beispiel für technische oder organisatorische Maßnahmen).

Der Hersteller darf ein sicheres Verfahren zur Installation alternativer, nicht vom Hersteller selbst bereitgestellter Software anbieten; beispielsweise kann es einem Benutzer erlaubt sein, auf einem Home-Router eine alternative Software zu installieren.

Es entspricht bewährten Verfahrensweisen für Sicherheit, den Downgrade von Software auf eine ältere Version zu verhindern.

5.3.2.4 Beurteilungskriterien

5.3.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SUM-2.

5.3.2.4.2 Erforderliche Informationen

[E.Doc.DT.SUM-2] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 11 für jeden Aktualisierungsmechanismus für Softwareteile, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind.

[E.Just.DT.SUM-2] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 11 für jeden Aktualisierungsmechanismus für Softwareteile, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind.

Wenn das Gerät über einen Aktualisierungsmechanismus für die Teile seiner Software verfügt, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind: [E.Doc.SUM] Dokumentation aller Aktualisierungsmechanismen für die Aktualisierung der Teile der Gerätesoftware, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind.

Wenn das Gerät über einen Aktualisierungsmechanismus für die Teile seiner Software verfügt, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind: [E.Doc.SUM.AuthIntVal] Eine Beschreibung der Verfahren, die vor der Installation die Gültigkeit der Software-Integrität und -Authentizität für alle Aktualisierungsmechanismen für Softwareteile sicherstellen, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind.

5.3.2.4.3 Konzeptuelle Beurteilung

5.3.2.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob Mechanismen zur Aktualisierung von Softwareteilen, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind, die erforderlichen Eigenschaften haben.

5.3.2.4.3.2 Voraussetzungen

Keine.

5.3.2.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each update mechanism for\nparts of the software affecting\nsecurity
   and/or network assets;
    if (<b>update mechanism property:</b>\nDoes the update mechanism\nonly
   install software whose\nintegrity and authenticity\nis validated? ) then
   (Yes)
      #lightgreen :PASS\nUpdate secure;
      detach;
    else (No)
       #pink :FAIL\nUpdate not secure;
       detach;
    endif
@enduml
```

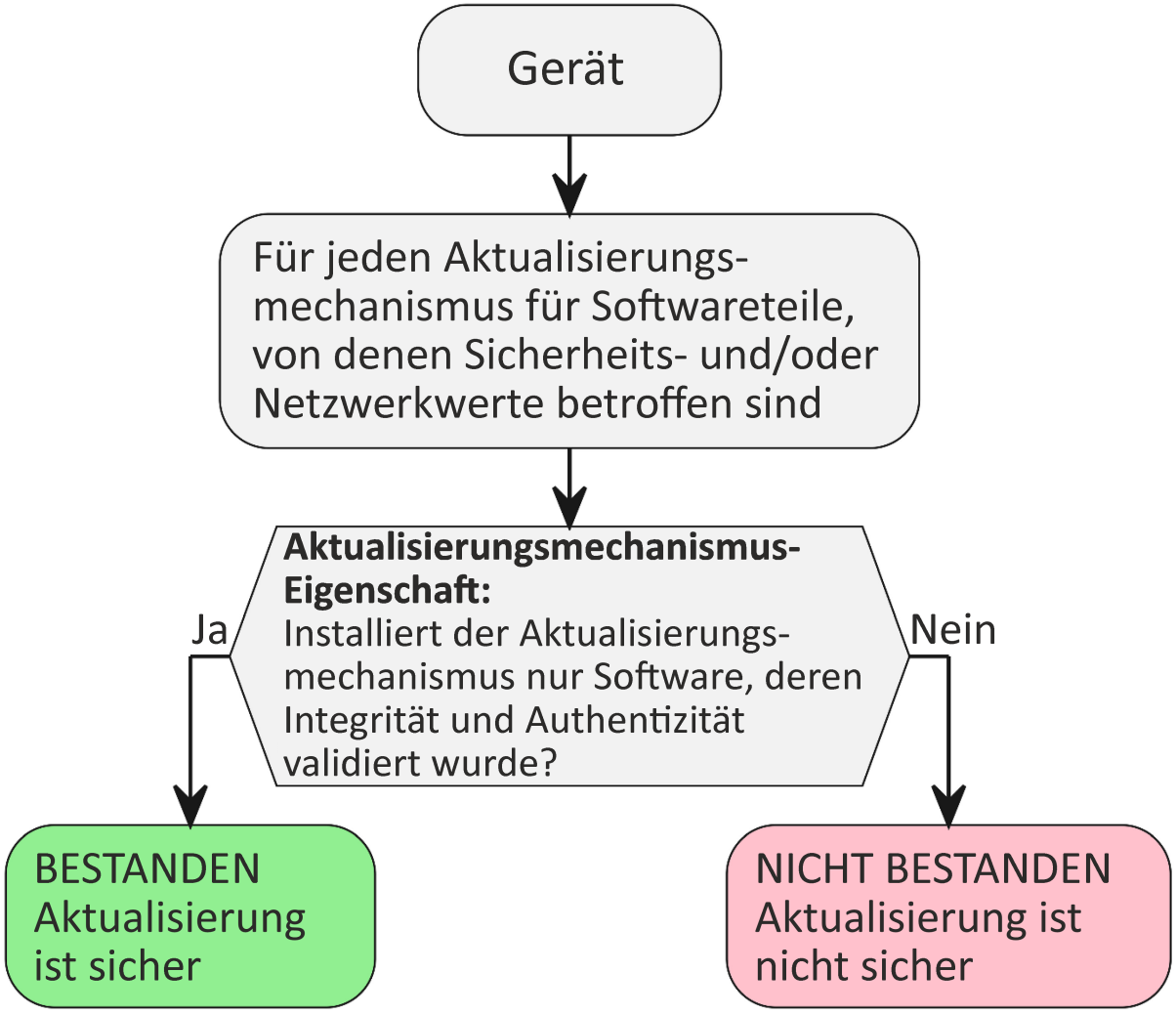

Bild 10 — Entscheidungsbaum für Anforderung SUM-2

Für jeden in [E.Doc.SUM] dokumentierten Aktualisierungsmechanismus ist zu prüfen, ob der Pfad durch den in [E.Just.DT.SUM-2] dokumentierten Entscheidungsbaum mit „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.SUM-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SUM-2] dokumentierte Begründung zu untersuchen.

5.3.2.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „BESTANDEN“ enden; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— kein Mechanismus für die Aktualisierung der Teile der Gerätesoftware erforderlich ist, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.3.2.4.4 Beurteilung der funktionalen Vollständigkeit

5.3.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation des Aktualisierungsmechanismus für Teile der Software, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind, vollständig ist.

5.3.2.4.4.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.3.2.4.4.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob es Aktualisierungsmechanismen für Teile der Software gibt, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind, die nicht in [E.Doc.SUM] dokumentiert sind.

5.3.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn alle gefundenen Aktualisierungsmechanismen in [E.Doc.SUM] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein gefundener Aktualisierungsmechanismus nicht in [E.Doc.SUM] dokumentiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.3.2.4.5 Beurteilung der funktionalen Suffizienz

5.3.2.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Aktualisierungsmechanismen für Softwareteile, von denen Sicherheits- und/oder Netzwerkwerte betroffen sind, die erforderlichen Eigenschaften haben.

5.3.2.4.5.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.3.2.4.5.3 Beurteilungseinheiten

Für jeden in [E.Doc.SUM] dokumentierten Aktualisierungsmechanismus sind die Verfahren zur Sicherstellung der Validität der Software-Integrität und -Authentizität vor der Installation funktional zu bestätigen, die in [E.Doc.SUM.AuthIntVal] dokumentiert sind und in der Begründung [E.Just.DT.SUM-2] verwendet werden.

5.3.2.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Verfahren zur Sicherstellung der Validität der Software-Integrität und -Authentizität vor der Installation nicht der Dokumentation entsprechen.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass ein Verfahren zur Sicherstellung der Validität der Software-Integrität und -Authentizität vor der Installation nicht der Dokumentation entspricht.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.3.3 [SUM-3] Automatisierte Aktualisierungen

5.3.3.1 Anforderung

Wenn das Gerät eine Netzwerkschnittstelle hat, die die Übertragung von Software-Aktualisierungen ermöglicht, muss wenigstens ein Aktualisierungsmechanismus für jeden aktualisierbaren Softwareteil , von dem Sicherheits- und/oder Netzwerkwerte betroffen sind, die Software-Aktualisierung folgendermaßen unterstützen:

— ohne menschlichen Eingriff am Gerät; oder

— durch Zeitsteuerung oder Auslösung der Installation einer Aktualisierung mit menschlicher Zustimmung;

es sei denn, Auswirkungen auf die funktionale Sicherheit erlauben keine automatisierte Aktualisierung dieses Softwareteils.

5.3.3.2 Begründung

Falls eine öffentlich ausnutzbare Schwachstelle des Geräts vorhanden ist, durch die Sicherheits- und Netzwerkwerte kompromittiert werden können, kann durch einen automatisierten Aktualisierungsmechanismus sichergestellt werden, dass eine verfügbare, diese Schwachstelle betreffende Sicherheitsaktualisierung automatisch installiert wird und so die Ausnutzung der Schwachstelle verhindert.

5.3.3.3 Leitlinie

In bestimmten Fällen können automatische Aktualisierungen zu Schäden führen (z. B. bei sicherheitskritischen Geräten). Ein Verfahren, um solche Schäden zu verhindern, ist die nicht automatisierte Bereitstellung von Aktualisierungen.

In spezifischen Fällen, in denen sicherheits- oder zeitkritische Aspekte betroffen sind, können vor dem Anstoßen der Aktualisierung unter Umständen einige Vorsichtsmaßnahmen und/oder Verifizierungen vor Ort erforderlich sein, und diese kann daher nicht automatisiert durchgeführt werden, um den Betrieb der Anwendung nicht zu beeinträchtigen.

Es wird empfohlen, neue Software vor der Aktivierung an einem freien Speicherplatz zu installieren.

ANMERKUNG 1 „Aktivierung“ der Software bedeutet, dass die Software zur Standardversion gemacht wird, die auf dem Gerät ausgeführt wird.

Falls die Installation der neuen Software fehlschlägt, d. h. die Validierung des/der Software-Images nicht erfolgreich ist, kann ein Rollback-Verfahren angewendet werden, um die vorherige Software wieder zu aktivieren.

Eine aus Benutzersicht einfache Aktualisierbarkeit unterstützt die Verteilung von Sicherheitsaktualisierungen.

ANMERKUNG 2 „Einfach aus Benutzersicht“ kann Folgendes einschließen:

— eine einfache Konfiguration von Mitteilungen bezüglich des sicheren Aktualisierungsmechanismus;

— eine einfache Konfiguration des Aktualisierungsmechanismus; und

— die einfache Zustimmung zu vollständig automatisierten Aktualisierungen

Wenn vollständig automatisierte Aktualisierungsmechanismen möglich sind, unterstützt das Einholen der Zustimmung des Benutzers bei der Inbetriebnahme des Geräts die Verteilung von Sicherheitsaktualisierungen.

Die Prüfung der Verfügbarkeit neuer Sicherheitsaktualisierungen nach der Initialisierung und in regelmäßigen Abständen kann die Verteilung von Sicherheitsaktualisierungen unterstützen.

5.3.3.4 Beurteilungskriterien

5.3.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SUM-3.

5.3.3.4.2 Erforderliche Informationen

[E.Doc.PartOfUpdableSoftw] Dokumentation aller aktualisierbaren, Sicherheits- und/oder Netzwerkwerte betreffenden Teile der Gerätesoftware.

[E.Doc.DT.SUM-3] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 12 für alle aktualisierbaren, Sicherheits- und/oder Netzwerkwerte betreffenden Teile der Software.

[E.Just.DT.SUM-3] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 12 für alle aktualisierbaren, Sicherheits- und/oder Netzwerkwerte betreffenden Teile der Software.

[E.Doc.SUM-3] Dokumentation des Automatisierungsverfahrens für Mechanismen zur Aktualisierung von Sicherheits- und/oder Netzwerkwerte betreffenden Teilen der Gerätesoftware.

5.3.3.4.3 Konzeptuelle Beurteilung

5.3.3.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die Bestimmung, ob alle aktualisierbaren Teile der Sicherheits- und/oder Netzwerkwerte betreffenden Teile der Software wie erforderlich automatisiert aktualisierbar sind.

5.3.3.4.3.2 Voraussetzungen

Keine.

5.3.3.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  if (<b>Equipment property:</b>\nDoes the equipment have a network
   interface \nthat allows transferring an update?) then (Yes)
    :For each updatable part of the software \naffecting security and/or
   network assets;
      if (<b>Functional safety implications:</b>\nAre there functional
   safety implications, that do not allow the \nautomation of updating this
   part of the software?) then (Yes)
            #application :NOT APPLICABLE\nFunctional safety implications
   \nprohibit automation;
            detach;
      else (No)
        switch (<b>update mechanism property:</b>\nIs there at least one
   update mechanism for the software \nthat is capable of updating the part
   of software:\n - without human intervention at the equipment;or\n - via
   scheduling or triggering the installation of an update under user
   approval? )
        case ( \n Yes,\n without intervention)
          #lightgreen :PASS\nUpdateable without intervention;
          detach;
        case ( \n  Yes,\n  via notification promt)
```

```
          #lightgreen :PASS\nUpdateable via notification;
          detach;
        case ( \n No)
          #pink :FAIL\nNot updateable as required;
          detach;
      endswitch
    endif
  else (No)
    #application :NOT APPLICABLE\nTechnical capabilities for \nautomated
   updates not present;
    detach;
  endif
@enduml
```

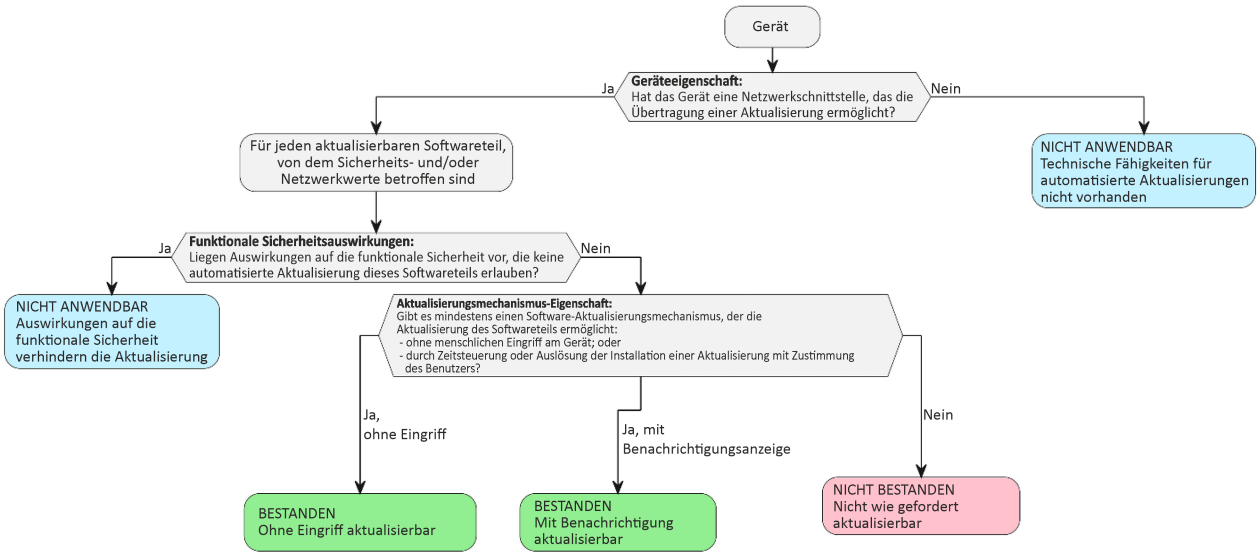

Bild 11 — Entscheidungsbaum für Anforderung SUM-3

Für jeden aktualisierbaren Teil der in [E.Doc.PartOfUpdableSoftw] dokumentierten Software, von der Sicherheits- und/oder Netzwerkwerte betroffen sind und die wie in [E.Doc.SUM-3] dokumentiert (optional) automatisch aktualisierbar ist, ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.SUM-3] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.SUM-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SUM-3] dokumentierte Begründung zu untersuchen.

5.3.3.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.3.3.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.3.3.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.4 [SSM] Sicherer Speichermechanismus (en: Secure Storage Mechanism)

5.4.1 [SSM-1] Anwendbarkeit von sicheren Speichermechanismen

5.4.1.1 Anforderung

Das Gerät muss sichere Speichermechanismen nutzen, um die dauerhaft auf dem Gerät gespeicherten Sicherheitswerte und Netzwerkwerte zu schützen, außer

— die Sicherheitswerte und Netzwerkwerte im Speicher werden durch die für die Nutzung vorgesehene Betriebsumgebung geschützt, die einen physischen oder logischen Schutz bereitstellt.

5.4.1.2 Begründung

Sichere Speichermechanismen schützen Werte gegen unbefugten Zugriff. Wenn Sicherheitswerte oder Netzwerkwerte nicht angemessen gesichert werden, kann ein Angreifer auf die Werte zugreifen, sie manipulieren oder löschen und das Gerät kompromittieren, was zu einem Missbrauch von Netzwerkressourcen führen könnte.

5.4.1.3 Leitlinie

Die Werte können beispielsweise folgendermaßen geschützt werden:

— durch kryptographische Maßnahmen wie Verschlüsselung, um die Vertraulichkeit sicherzustellen;

— durch kryptographische Maßnahmen wie digitale Signaturen, um die Integrität und Authentizität sicherzustellen;

— durch Zugangssteuerung mithilfe von Authentisierung oder Autorisierung;

— durch Hardware-Schutzmaßnahmen;

— durch physische Schutzmaßnahmen.

Zu den physischen Schutzmaßnahmen können unter anderem verschlossene Gehäuse mit Unversehrtheitssiegel zählen.

Der angemessene Schutzmechanismus hängt vom Risiko in Verbindung mit den zu speichernden Werten ab; dieses kann abhängen von:

— der Kritikalität der Werte;

— der Anzahl der Werte;

— der Zeitspanne, während der die Werte gespeichert werden müssen;

— der für die Nutzung vorgesehenen Betriebsumgebung.

5.4.1.4 Beurteilungskriterien

5.4.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SSM-1.

5.4.1.4.2 Erforderliche Informationen

[E.Doc.DT.SSM-1] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 13.

[E.Just.DT.SSM-1] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 13.

[E.Doc.SecurityAsset] Vollständige Dokumentation der auf dem Gerät gespeicherten Sicherheitswerte.

[E.Doc.NetworkAsset] Vollständige Dokumentation der auf dem Gerät gespeicherten Netzwerkwerte.

[E.Doc.SSM] Dokumentation der sicheren Speichermechanismen, die den Satz der zur Speicherung von Sicherheitswerten, wie in [E.Doc.SecurityAsset] dokumentiert, und von Netzwerkwerten, wie in [E.Doc.NetworkAsset] dokumentiert, verwendeten Mechanismen beschreibt.

5.4.1.4.3 Konzeptuelle Beurteilung

5.4.1.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob sichere Speichermechanismen implementiert sind, wenn dies zum Schutz der auf dem Gerät gespeicherten Sicherheitswerte und Netzwerkwerte erforderlich ist.

5.4.1.4.3.2 Voraussetzungen

Keine.

5.4.1.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:Equipment;
if (Are network assets or security\nassets stored on the equipment? ) then (
   Yes )
  :For each network asset and security \nasset stored on the equipment;
  if ( Is the asset secured while\n stored on the equipment? ) then ( Yes )
  #lightgreen :PASS\nAsset is protected;
  detach
  else (No)
        if (Is the asset stored on an equipment\nprotected by intended
   operational environment of use \nproviding physical or logical
   protection? ) then ( Yes )
        #application :NOT APPLICABLE\nAsset protected\nby the intended
   environment of use;
        detach
      else ( No )
        #pink :FAIL\nAsset not protected;
        detach
      endif
```

```
  endif
else (No)
  #application :NOT APPLICABLE\nNo assets stored;
  detach
endif
@enduml
```

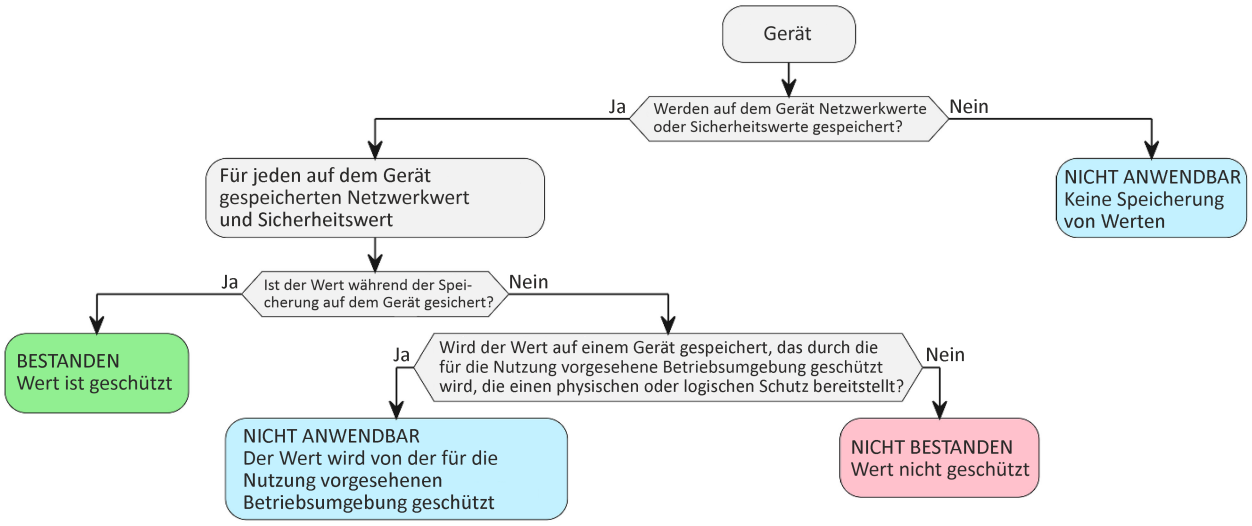

Bild 12 — Entscheidungsbaum für Anforderung SSM-1

Für jeden in [E.Doc.SecurityAsset] dokumentierten Sicherheitswert und für jeden in [E.Doc.NetworkAsset] dokumentierten Netzwerkwert ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.SSM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.SSM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SSM-1] dokumentierte Begründung zu untersuchen.

5.4.1.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.4.1.4.4 Beurteilung der funktionalen Vollständigkeit

5.4.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation vollständig ist.

5.4.1.4.4.2 Voraussetzungen

— Das Gerät muss sich im üblichen Betriebszustand befinden.

5.4.1.4.4.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob Sicherheitswerte auf dem Gerät gespeichert sind, die nicht in [E.Doc.SecurityAssets] aufgeführt sind.

Es ist funktional zu beurteilen, ob Netzwerkwerte auf dem Gerät gespeichert sind, die nicht in [E.Doc.NetworkAsset] aufgeführt sind.

Es ist funktional zu beurteilen, ob sichere Speichermechanismen zur Speicherung von Sicherheitswerten oder Netzwerkwerten verwendet werden, die nicht in [E.Doc.SSM] aufgeführt sind.

5.4.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Sicherheitswerte in [E.Doc.SecurityAsset] dokumentiert sind; und

— alle Netzwerkwerte in [E.Doc.NetworkAsset] dokumentiert sind; und

— kein Nachweis vorliegt, dass sichere Speichermechanismen zur Speicherung von Sicherheitswerten oder Netzwerkwerten verwendet werden, die nicht in [E.Doc.SSM] aufgeführt sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.4.1.4.5 Beurteilung der funktionalen Suffizienz

5.4.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob sichere Speichermechanismen implementiert wurden, wo sie erforderlich sind.

5.4.1.4.5.2 Voraussetzungen

— Das Gerät muss sich im üblichen Betriebszustand befinden.

5.4.1.4.5.3 Beurteilungseinheiten

Es ist funktional zu bestätigen, dass sichere Speichermechanismen wie in [E.Doc.SSM] dokumentiert implementiert sind.

5.4.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die sicheren Speichermechanismen nicht wie dokumentiert vorhanden sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Anzeichen vorliegt, dass die sicheren Speichermechanismen nicht wie dokumentiert vorhanden sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.4.2 [SSM-2] Angemessener Integritätsschutz für sichere Speichermechanismen

5.4.2.1 Anforderung

Jeder sichere Speichermechanismus, der SSM-1 unterliegt, muss die Integrität von dauerhaft gespeicherten Sicherheitswerten und Netzwerkwerten schützen.

5.4.2.2 Begründung

Sicherheitswerte und Netzwerkwerte müssen während der Speicherung gegen Manipulation geschützt werden. Wenn die Integrität der gespeicherten Werte nicht angemessen gesichert wird, kann ein Angreifer diese Werte manipulieren, was zur Gefährdung von Netzwerkressourcen führen könnte.

Die Integrität gilt sowohl für die verschlüsselte als auch für die nicht verschlüsselte Speicherung.

5.4.2.3 Leitlinie

Daten können unter anderem folgendermaßen gegen Manipulation geschützt werden:

— durch kryptographische Maßnahmen wie digitale Signaturen;

— durch Zugangssteuerung;

— durch Hardware-Schutzmaßnahmen.

5.4.2.4 Beurteilungskriterien

5.4.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SSM-2.

5.4.2.4.2 Erforderliche Informationen

[E.Doc.DT.SSM-2] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 14 für jeden Speichermechanismus in jedem Betriebszustand.

[E.Just.DT.SSM-2] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 14 für jeden sicheren Speichermechanismus in jedem Betriebszustand. Dies ist eine dokumentierte Analyse (z. B. auf Grundlage von Bedrohungsmodellen und der Beurteilung des Sicherheitsrisikos), Begründung und Entscheidung bezüglich der Angemessenheit von Mechanismen und Modi, um die Integrität der gespeicherten Werte sicherzustellen.

[E.Doc.SSM-2] Dokumentierte Liste von Sicherheitsmechanismen oder kryptographischen Modi, die zum Schutz der Integrität von Sicherheitswerten und Netzwerkwerten eingesetzt werden, während diese auf dem Gerät gespeichert sind.

[E.Doc.OperationalStates] Beschreibung der Betriebszustände des Geräts, wie sich diese Zustände vom üblichen Betriebszustand unterscheiden und unter welchen sicheren Bedingungen die Betriebszustände eintreten können.

5.4.2.4.3 Konzeptuelle Beurteilung

5.4.2.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle sicheren Speichermechanismen des Geräts die Integrität der Sicherheitswerte und Netzwerkwerte schützen.

5.4.2.4.3.2 Voraussetzungen

Keine.

5.4.2.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each secure storage mechanism;
:For each operational state;
if (Is the integrity of the assets sufficiently \nprotected to ensure that
   attacks on secure \nstorage do not lead to their manipulation?) then
    (Yes)
  #lightgreen :PASS\nIntegrity protected;
  detach;
else (No)
  #pink :FAIL\nIntegrity not protected;
  detach;
endif
@enduml
```

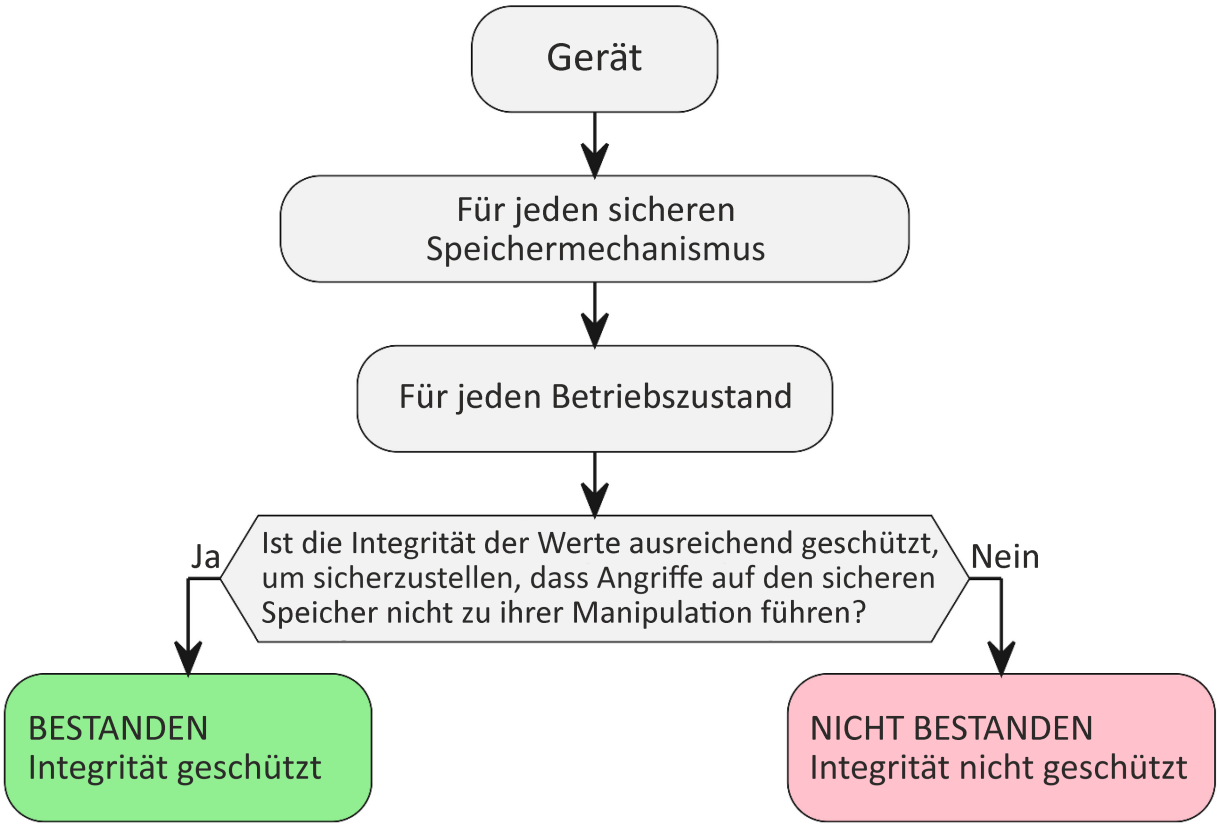

Bild 13 — Entscheidungsbaum für Anforderung SSM-2

Für jeden sicheren Speichermechanismus in [E.Doc.SSM-2] und für jeden in [E.Doc.OperationalStates] beschriebenen Betriebszustand ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.SSM-2] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.SSM-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SSM-2] dokumentierte Begründung zu untersuchen.

5.4.2.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.4.2.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.4.2.4.5 Beurteilung der funktionalen Suffizienz

5.4.2.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die sicheren Speichermechanismen den erforderlichen Integritätsschutz bieten.

5.4.2.4.5.2 Voraussetzungen

— Das Gerät muss sich im üblichen Betriebszustand befinden.

5.4.2.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob auf dem Gerät gespeicherte Netzwerkwerte durch eine nicht autorisierte Entität manipuliert werden können.

5.4.2.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— kein Nachweis vorliegt, dass der Integritätsschutz nicht wie dokumentiert implementiert ist;

— kein Manipulationsangriff erfolgreich war.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.4.3 [SSM-3] Angemessener Vertraulichkeitsschutz für sichere Speichermechanismen

5.4.3.1 Anforderung

Jeder sichere Speichermechanismus, der SSM-1 unterliegt, muss die Geheimhaltung der vertraulichen Sicherheitsparameter von dauerhaft gespeicherten Sicherheitswerten schützen.

5.4.3.2 Begründung

Vertrauliche Sicherheitsparameter für einen Wert benötigen während der Speicherung einen Schutz vor Offenlegung. Wenn ein vertraulicher Sicherheitsparameter für einen Wert nicht angemessen gesichert ist, kann ein Angreifer auf das Gerät und die gespeicherten Daten zugreifen und diese missbrauchen, was zu einem Missbrauch von Netzwerkressourcen führen könnte.

5.4.3.3 Leitlinie

Daten können unter anderem folgendermaßen vor Offenlegung geschützt werden:

— durch kryptographische Maßnahmen wie Verschlüsselung;

— durch Zugangssteuerung;

— durch Hardware-Schutzmaßnahmen.

5.4.3.4 Beurteilungskriterien

5.4.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SSM-3.

5.4.3.4.2 Erforderliche Informationen

[E.Doc.DT.SSM-3] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 15 für jeden Speichermechanismus in jedem Betriebszustand.

[E.Just.DT.SSM-3] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 15 für jeden sicheren Speichermechanismus in jedem Betriebszustand. Dies ist eine dokumentierte Analyse (z. B. auf Grundlage von Bedrohungsmodellen und der Beurteilung des Sicherheitsrisikos), Begründung und Entscheidung bezüglich der Angemessenheit von Mechanismen und Modi, um die Vertraulichkeit der gespeicherten Werte sicherzustellen.

[E.Doc.SSM-3] Dokumentierte Liste von Sicherheitsmechanismen oder kryptographischen Modi, die zum Schutz der Vertraulichkeit von sensiblen Sicherheitsparametern eingesetzt werden, während diese auf dem Gerät gespeichert sind.

[E.Doc.OperationalStates] Beschreibung der Betriebszustände des Geräts, wie sich diese Zustände vom üblichen Betriebszustand unterscheiden und unter welchen sicheren Bedingungen die Betriebszustände eintreten können.

5.4.3.4.3 Konzeptuelle Beurteilung

5.4.3.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle sicheren Speichermechanismen des Geräts die Vertraulichkeit der sensiblen Sicherheitsparameter schützen.

5.4.3.4.3.2 Voraussetzungen

Keine.

5.4.3.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each secure storage mechanism;
:For each operational state;
if (Is the confidentiality of the assets sufficiently \nprotected to ensure
   that attacks on secure \nstorage do not lead to their disclosure?) then
   (Yes)
```

```
  #lightgreen :PASS\nConfidentiality protected;
  detach;
else (No)
  #pink :FAIL\nConfidentiality not protected;
  detach;
endif
@enduml
```

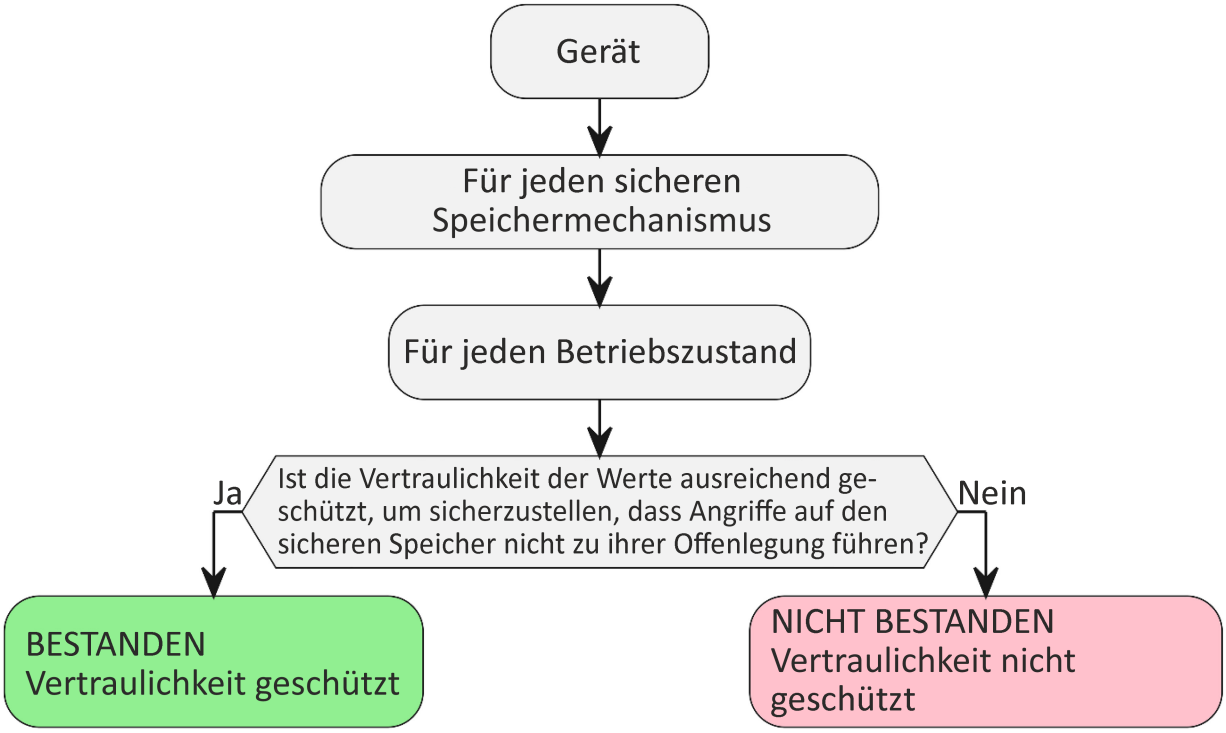

Bild 14 — Entscheidungsbaum für Anforderung SSM-3

Für jeden sicheren Speichermechanismus in [E.Doc.SSM-3] und für jeden in [E.Doc.OperationalStates] beschriebenen Betriebszustand ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.SSM-3] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.SSM-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SSM-3] dokumentierte Begründung zu untersuchen.

5.4.3.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.4.3.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.4.3.4.5 Beurteilung der funktionalen Suffizienz

5.4.3.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die sicheren Speichermechanismen den erforderlichen Vertraulichkeitsschutz bereitstellen.

5.4.3.4.5.2 Voraussetzungen

— Das Gerät muss sich im üblichen Betriebszustand befinden.

5.4.3.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob auf dem Gerät gespeicherte Netzwerkwerte für eine nicht autorisierte Entität offengelegt werden können.

5.4.3.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— kein Nachweis vorliegt, dass der Vertraulichkeitsschutz nicht wie dokumentiert implementiert ist;

— keine Sicherheits- und Netzwerkwerte für nicht autorisierte Entitäten offengelegt sind.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.5 [SCM] Sicherer Kommunikationsmechanismus (en: Secure Communication Mechanism)

5.5.1 [SSM-1] Anwendbarkeit von sicheren Kommunikationsmechanismen

5.5.1.1 Anforderung

Das Gerät muss sichere Kommunikationsmechanismen für den Austausch von Sicherheitswerten und Netzwerkwerten nutzen, außer

— der Kommunikationsmechanismus wird für die Interoperabilität mit Legacy-Netzwerken oder anderen Geräten benötigt, oder

— die Sicherheitswerte und Netzwerkwerte werden während der Übertragung durch die Umgebung geschützt, die einen physischen oder logischen Schutz bereitstellt.

5.5.1.2 Begründung

Die Werte des Geräts können an andere Kommunikationspartner übertragen werden, z. B. bei der Verwendung von Webdiensten. Angreifern, die Zugang zur Kommunikation haben, ist es möglich (bei drahtloser Kommunikation mit geringerem Aufwand), die Kommunikation abzuhören, zu manipulieren oder wiederzugeben. Das Gerät muss sicherstellen, dass die Kommunikation gegen diese Angriffe durch sichere Kommunikationsmechanismen geschützt ist.

5.5.1.3 Leitlinie

Es gibt unterschiedliche Kommunikationsmechanismen, die zur Sicherung der Gerätekommunikation verwendet werden können (vergleiche auch [CRY] Kryptographie). Die verwendeten Konfigurationen sollten bewährten Verfahrensweisen entsprechen, um zu verhindern, dass die Kommunikation abgehört, manipuliert und wiedergegeben wird. Übliche Maßnahmen sind eine Kombination aus Authentisierung, Integritätsschutz, Verschlüsselung und Wiedergabeschutz. Die Maßnahmen können beispielsweise auf den Kommunikationskanal angewendet oder für den Ende-zu-Ende-Schutz verwendet werden. Das Gerät muss anderen Kommunikationspartnern als Vorgabe bewährte Verfahrensweisen anbieten. Wenn eine „Legacy-Unterstützung“ benötigt wird,

sollten die sich daraus ergebenden Risiken für die „bewährten Verfahrensweisen für Sicherheit“ beurteilt werden. Die angemessenen Maßnahmen können sich abhängig von den der Kommunikation zugrundeliegenden Anwendungsfällen unterscheiden.

5.5.1.4 Beurteilungskriterien

5.5.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SCM-1.

5.5.1.4.2 Erforderliche Informationen

[E.Doc.DT.SCM-1] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 16 für jede Netzwerkschnittstelle.

[E.Just.DT.SCM-1] Begründung für den gewählten Pfad durch den Entscheidungsbaum in Bild 16 für jede Netzwerkschnittstelle.

[E.Doc.NetworkInterfaces] Vollständige Dokumentation aller Netzwerkschnittstellen.

[E.Doc.SecurityAsset.SCM] Vollständige Dokumentation der über die Netzwerkschnittstellen kommunizierten Sicherheitswerte.

[E.Doc.NetworkAsset.SCM] Vollständige Dokumentation der über die Netzwerkschnittstellen kommunizierten Netzwerkwerte.

[E.Doc.SCM] Dokumentation der sicheren Kommunikationsmechanismen, die den Satz von Mechanismen beschreibt, die zur Kommunikation der in [E.Doc.SecurityAsset.SCM] dokumentierten Sicherheitswerte und der in [E.Doc.NetworkAsset.SCM] dokumentierten Netzwerkwerte über die Netzwerkschnittstellen verwendet werden.

5.5.1.4.3 Konzeptuelle Beurteilung

5.5.1.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob sichere Kommunikationsmechanismen implementiert sind, wenn dies zum Schutz der über die Netzwerkschnittstellen kommunizierten Sicherheitsparameter erforderlich ist.

5.5.1.4.3.2 Voraussetzungen

Keine.

5.5.1.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:Equipment ;
if (Are security assets or network assets\ncommunicated over any network
   interface?) then ( Yes )
  :For every network interface communicating assets;
  if (Are the assets secured while \ncommunicated over the interface?) then
   ( Yes )
    #lightgreen :PASS\nApplicable and met;
    detach
  else (No)
```

```
    if (Is the communication mechanism required \nto communicate with legacy
   networks or devices) then ( Yes )
      #application :NOT APPLICABLE\nRequired for legacy;
      detach
    else ( No )
      if (Is the communication of assets protected \nby the environment
   providing physical or \nlogical protection? ) then ( Yes )
        #application :NOT APPLICABLE\nProtected by the environment;
        detach
      else ( No )
        #pink :FAIL\nApplicable but not met;
        detach
      endif
    endif
  endif
else (No)
  #application :NOT APPLICABLE\nNothing to protect;
  detach
endif
@enduml
```

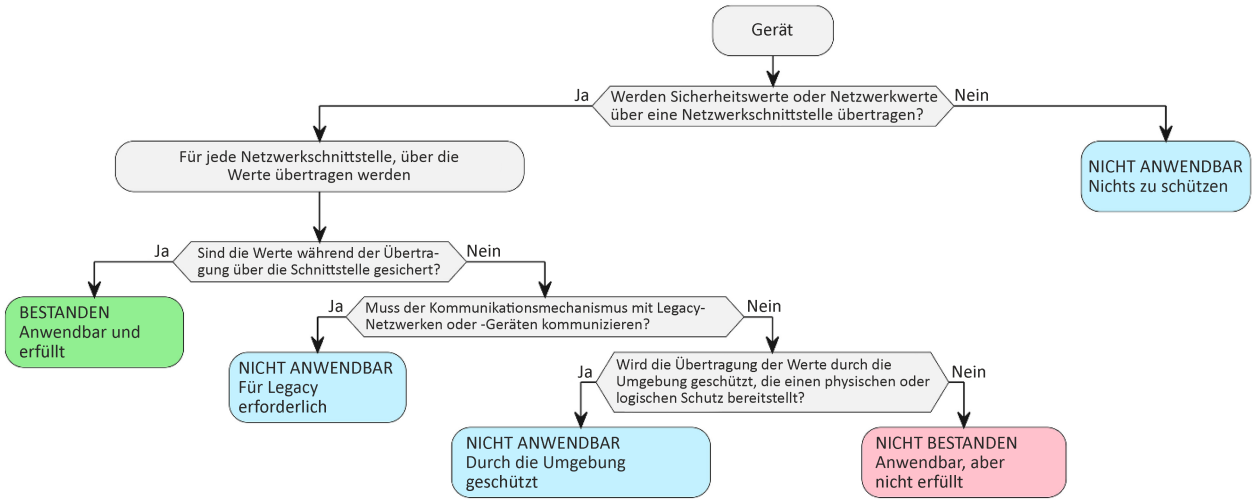

Bild 15 — Entscheidungsbaum für Anforderung SCM-1

Für jede in [E.Doc.NetworkInterfaces] dokumentierte Netzwerkschnittstelle ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.SCM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.SCM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SCM-1] dokumentierte Begründung zu untersuchen.

5.5.1.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.5.1.4.4 Beurteilung der funktionalen Vollständigkeit

5.5.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation vollständig ist.

5.5.1.4.4.2 Voraussetzungen

— Das Gerät muss sich im üblichen Betriebszustand befinden, und alle [E.Doc.NetworkInterfaces] sind entweder aktiviert oder konfiguriert, so dass jede Netzwerkschnittstelle geprüft werden kann.

— Wenn [E.Doc.SCM] implementiert sind, sind die notwendigen Sicherheitsparameter verfügbar oder konfiguriert, um jede Netzwerkschnittstelle prüfen zu können.

5.5.1.4.4.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob es Netzwerkschnittstellen gibt, die nicht in [E.Doc.NetworkInterfaces] aufgeführt sind.

Es ist funktional zu beurteilen, ob Sicherheitswerte kommuniziert werden, die nicht in [E.Doc.SecurityAssets.SCM] aufgeführt sind.

Es ist funktional zu beurteilen, ob Netzwerkwerte kommuniziert werden, die nicht in [E.Doc.NetworkAsset.SCM] aufgeführt sind.

Es ist funktional zu beurteilen, ob es sichere Kommunikationsmechanismen gibt, die nicht in [E.Doc.SCM] aufgeführt sind.

5.5.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Netzwerkschnittstellen in [E.Doc.NetworkInterfaces] dokumentiert sind; und

— alle kommunizierten Sicherheitswerte in [E.Doc.SecurityAsset.SCM] dokumentiert sind; und

— alle kommunizierten Netzwerkwerte in [E.Doc.NetworkAsset.SCM] dokumentiert sind; und

— alle sicheren Kommunikationsmechanismen in [E.Doc.SCM] dokumentiert sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.5.1.4.5 Beurteilung der funktionalen Suffizienz

5.5.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob sichere Kommunikationsmechanismen implementiert wurden, wo sie erforderlich sind.

5.5.1.4.5.2 Voraussetzungen

— Das Gerät muss sich im üblichen Betriebszustand befinden, und alle [E.Doc.NetworkInterfaces] sind entweder aktiviert oder konfiguriert, so dass jede Netzwerkschnittstelle geprüft werden kann.

— Wenn [E.Doc.SCM] implementiert sind, sind die notwendigen Sicherheitsparameter verfügbar oder konfiguriert, um jede Netzwerkschnittstelle prüfen zu können.

5.5.1.4.5.3 Beurteilungseinheiten

Für jeden in [E.Doc.SecNetAsset] dokumentierten Sicherheits- und Netzwerkwert ist das Vorhandensein von sicheren Kommunikationsmechanismen nach [E.Doc.SCM] funktional zu bestätigen.

5.5.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass sichere Kommunikationsmechanismen nicht wie beschrieben implementiert wurden.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass sichere Kommunikationsmechanismen nicht wie beschrieben implementiert wurden.

5.5.2 [SCM-2] Angemessener Integritäts- und Authentizitätsschutz für sichere Kommunikationsmechanismen

5.5.2.1 Anforderung

Jeder sichere Kommunikationsmechanismus, der SCM-1 unterliegt, muss die Integrität und Authentizität der kommunizierten Sicherheitswerte und Netzwerkwerte schützen.

5.5.2.2 Begründung

Sicherheitswerte und Netzwerkwerte benötigen während der Kommunikation einen Schutz gegen Manipulation. Ein Angreifer, der sich Zugang zum Netzwerk verschafft hat, könnte die Kommunikation abfangen und manipulieren (Man-in-the-Middle-Angriff). Das Gerät muss sicherstellen, dass die Kommunikation gegen diese Angriffe durch den Einsatz von Integritäts- und Authentizitätsschutzmechanismen geschützt ist.

Der Integritäts- und Authentizitätsschutz gilt sowohl für die verschlüsselte als auch für die nicht verschlüsselte Kommunikation.

5.5.2.3 Leitlinie

Es gibt unterschiedliche Sicherheitsmechanismen, die zur Sicherung der Kommunikation des Geräts verwendet werden können (siehe CRY-1). Die verwendeten Konfigurationen sollten bewährten Verfahrensweisen entsprechen, um zu verhindern, dass die Kommunikation manipuliert wird. Übliche Maßnahmen sind eine Kombination von Authentisierung und Integritätsschutz. Die Maßnahmen können beispielsweise auf den Kommunikationskanal angewendet oder für den „Ende-zu-Ende“-Schutz verwendet werden. Das Gerät muss anderen Kommunikationspartnern als Vorgabe bewährte Verfahrensweisen anbieten. Wenn eine „Legacy-Unterstützung“ benötigt wird, sollten die sich daraus ergebenden Risiken für die „bewährten Verfahrensweisen für Sicherheit“ beurteilt werden. Die angemessenen Maßnahmen können sich abhängig von den der Kommunikation zugrundeliegenden Anwendungsfällen unterscheiden.

Der kryptographische Modus, der zum Schutz der Integrität und Authentizität der kommunizierten Werte verwendet wird, ist in der Anforderung [CRY-1], Kryptographie, festgelegt.

5.5.2.4 Beurteilungskriterien

5.5.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SCM-2.

5.5.2.4.2 Erforderliche Informationen

[E.Doc.DT.SCM-2] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 17 für jeden Kommunikationsmechanismus in jedem Betriebszustand.

[E.Just.DT.SCM-2] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 17 für jeden Kommunikationsmechanismus in jedem Betriebszustand. Dies ist eine dokumentierte Analyse (z. B. auf Grundlage von Bedrohungsmodellen und Sicherheitsrisikobeurteilungen), Begründung und Entscheidung über die Angemessenheit der Mechanismen und Modi, die zum Schutz der Integrität und Authentizität des kommunizierten Werts eingesetzt werden.

[E.Doc.SecurityAsset.SCM] Vollständige Dokumentation der über die Netzwerkschnittstellen kommunizierten Sicherheitswerte.

[E.Doc.NetworkAsset.SCM] Vollständige Dokumentation der über die Netzwerkschnittstellen kommunizierten Netzwerkwerte.

[E.Doc.SCM-2] Dokumentierte Liste von Sicherheitsmechanismen und kryptographischen Modi, die zum Schutz der Integrität und Authentizität der kommunizierten, in [E.Doc.SecurityAsset.SCM] dokumentierten Sicherheitswerte oder der in [E.Doc.NetworkAsset.SCM] dokumentierten Netzwerkwerte über die in [E.Doc.NetworkInterfaces] beschriebenen Netzwerkschnittstellen verwendet werden.

[E.Doc.CommunicationProtocol] Beschreibung des Kommunikationsprotokolls, das für die Kommunikation über die Netzwerkschnittstellen verwendet wird, und wie die [E.Doc.SCM-2] im Protokoll angewendet werden.

[E.Doc.OperationalStates] Beschreibung der Betriebszustände des Geräts, wie sich diese Zustände vom üblichen Betriebszustand unterscheiden und unter welchen sicheren Bedingungen die Betriebszustände eintreten können.

5.5.2.4.3 Konzeptuelle Beurteilung

5.5.2.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle sicheren Kommunikationsmechanismen des Geräts die Integrität und Authentizität der Sicherheitswerte und Netzwerkwerte schützen.

5.5.2.4.3.2 Voraussetzungen

Keine.

5.5.2.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each secure communication mechanism;
:For each operational state;
```

```
if (Is the integrity and authenticity of the assets \nsufficiently protected
    to ensure that attacks \non secure communication sessions do not \nlead
    to their manipulation?) then (Yes)
  #lightgreen :PASS;
  detach;
else (No)
  #pink :FAIL;
  detach;
endif
@enduml
```

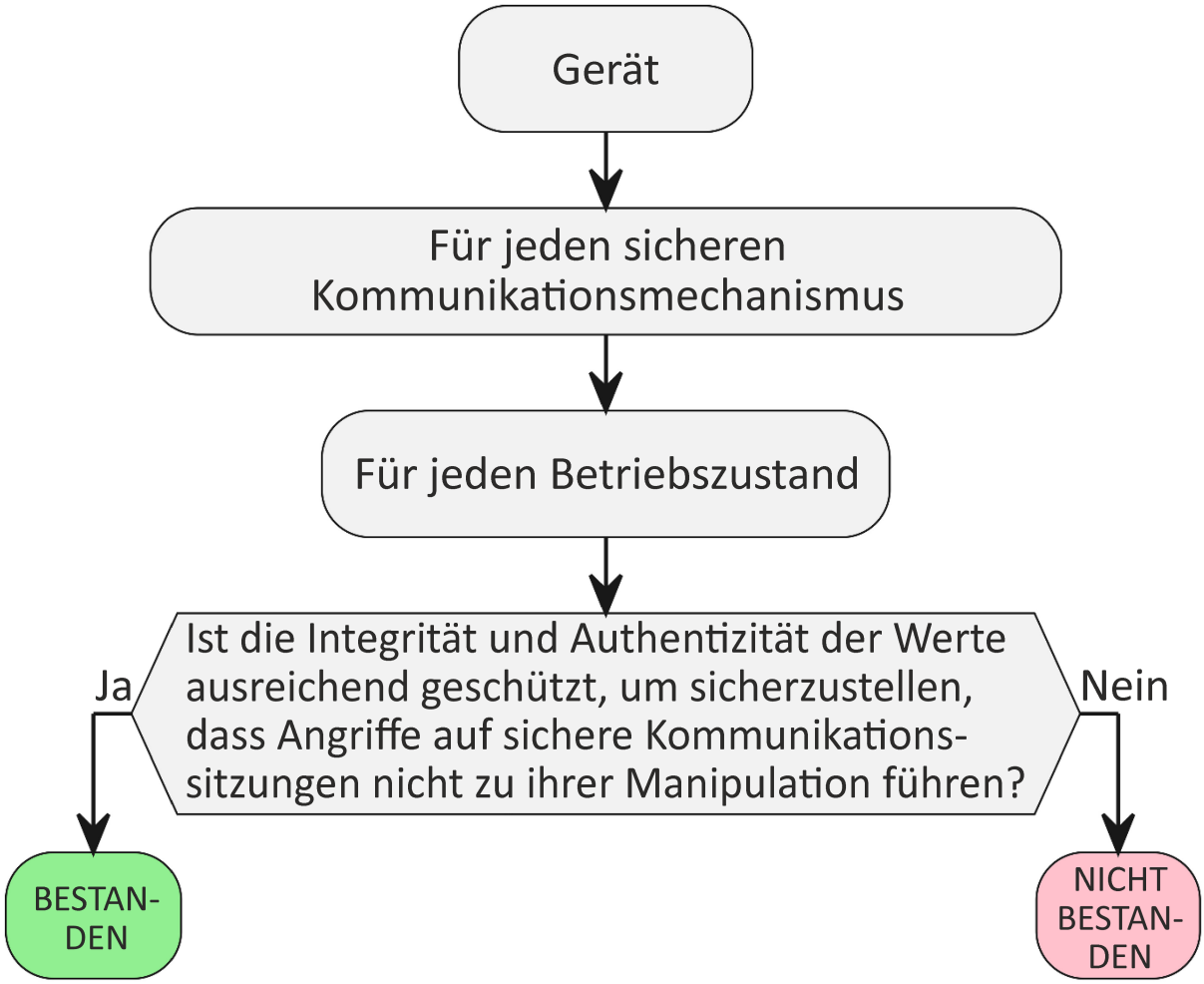

Bild 16 — Entscheidungsbaum für Anforderung SCM-2

Für jeden sicheren Kommunikationsmechanismus in [E.Doc.SCM-2] und für jeden in [E.Doc.OperationalStates] beschriebenen Zustand ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.SCM-2] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.SCM-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SCM-2] dokumentierte Begründung zu untersuchen.

ANMERKUNG 1 Verfahren zur Eindämmung des Risikos von Angriffen auf laufende Kommunikationssitzungen sind unter anderem:

— Der Schutz der Integrität und Authentizität kommunizierter Daten durch auf Verschlüsselung basierende Mitteilungsauthentisierungscode-(MAC-)Techniken.

5.5.2.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.5.2.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.5.2.4.5 Beurteilung der funktionalen Suffizienz

5.5.2.4.5.1 Zweck der Beurteilung

Der Zweck dieses Prüffalls ist die funktionale Beurteilung, ob die kommunizierten Werte vor unbemerkter Manipulation geschützt sind.

5.5.2.4.5.2 Voraussetzungen

— Das Gerät muss sich im üblichen Betriebszustand befinden, und alle [E.Doc.NetworkInterfaces], die Teil der bestimmungsgemäßen Verwendung sind, sind entweder aktiviert oder so konfiguriert, dass jede Netzwerkschnittstelle geprüft werden kann.

— Bei Schnittstellen, für die [E.Doc.SCM-2] implementiert sind, sind die notwendigen CSPs zur Verfügung gestellt oder konfiguriert, um jede gesicherte Kommunikationsschnittstelle in [E.Doc.NetworkInterfaces] prüfen zu können.

— Prüf-Tools wie unter anderem Protokollanalysatoren für [E.Doc.CommunicationProtocol].

5.5.2.4.5.3 Beurteilungseinheiten

Zwischen dem Gerät und einem rechtmäßigen Kommunikationsendpunkt wird eine rechtmäßige Kommunikationssitzung auf den [E.Doc.NetworkInterfaces] unter Verwendung des [E.Doc.CommunicationProtocol] eingerichtet. Es wird ein Versuch unternommen, die Kommunikation der übertragenen sensiblen Sicherheitsparameter zu manipulieren.

5.5.2.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— alle sicheren Kommunikationsmechanismen korrekt und wie dokumentiert implementiert sind;

— alle Versuche, Schadcode-Datenkommunikationsblöcke während der Kommunikationssitzungen einzuschleusen, nicht zu einer Unterbrechung der sicheren Kommunikationsmechanismen führen;

— keine erfolgreiche Manipulation durch einen Man-in-the-Middle-Angriff stattfindet.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.5.3 [SCM-3] Angemessener Vertraulichkeitsschutz für sichere Kommunikationsmechanismen

5.5.3.1 Anforderung

Jeder sichere Kommunikationsmechanismus, der SCM-1 unterliegt, muss die Geheimhaltung von vertraulichen Sicherheitsparametern des übertragenen Werts schützen.

5.5.3.2 Begründung

Während der Kommunikation benötigen vertrauliche Sicherheitsparameter einen Abhörschutz. Ein Angreifer, der sich Zugang zum Netzwerk verschafft hat, könnte die Kommunikation überwachen. Das Gerät muss sicherstellen, dass die Kommunikation gegen diese Angriffe geschützt ist, indem mithilfe von Verschlüsselungsmaßnahmen Vertraulichkeit hergestellt wird.

5.5.3.3 Leitlinie

Es gibt unterschiedliche Sicherheitsmechanismen, die zur Sicherung der Vertraulichkeit der Kommunikation angewendet werden können (siehe 4.15, Kryptographie). Es sollten bewährte Verfahrensweisen für die Konfiguration verwendet werden, um zu verhindern, dass die Kommunikation abgehört wird. Dies wird üblicherweise durch symmetrische Verschlüsselungsverfahren erreicht. Die Verfahren können auf den Kommunikationskanal angewendet oder für den „Ende-zu-Ende"-Schutz verwendet werden. Es wird empfohlen, standardmäßig für Vertraulichkeit zwischen den kommunizierenden Entitäten zu sorgen und bewährte Verfahrensweisen für Kryptographie einzusetzen. Wenn eine „Legacy-Unterstützung" benötigt wird, sollten die sich daraus ergebenden Risiken für die „bewährten Verfahrensweisen für Sicherheit" beurteilt werden. Die angemessenen Maßnahmen können sich abhängig von den der Kommunikation zugrundeliegenden Anwendungsfällen unterscheiden.

Die Verschlüsselungsverfahren, die zum Schutz der Vertraulichkeit der übertragenen Daten verwendet werden, sind in der Anforderung 4.15, Kryptographie, festgelegt.

ANMERKUNG Authentisierte Verschlüsselung (en: Authenticated Encryption, AE) kann eingesetzt werden, um die Vertraulichkeit und Authentizität der Daten mit einem einzigen Verschlüsselungsverfahren sicherzustellen. Diese Verfahren können auch verwendet werden, um die Anforderung von 5.5.2 zu erfüllen.

5.5.3.4 Beurteilungskriterien

5.5.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SCM-3.

5.5.3.4.2 Erforderliche Informationen

[E.Doc.DT.SCM-3] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 18 für jeden Kommunikationsmechanismus in jedem Betriebszustand.

[E.Just.DT.SCM-3] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 18 für jeden Kommunikationsmechanismus in jedem Betriebszustand. Dies ist eine dokumentierte Analyse (z. B. auf Grundlage von Bedrohungsmodellen und Sicherheitsrisikobeurteilungen), Begründung und Entscheidung bezüglich der Angemessenheit von Mechanismen und Verfahren, die zum Schutz der Vertraulichkeit des übertragenen Werts eingesetzt werden.

[E.Doc.SecurityAsset.SCM-3] Vollständige Dokumentation der über die Netzwerkschnittstellen übertragenen vertraulichen Sicherheitsparameter.

[E.Doc.SCM-3] Dokumentierte Liste von Sicherheitsmechanismen und kryptographischen Verfahren, die zum Schutz der Vertraulichkeit der vertraulichen, in [E.Doc.SecurityAsset.SCM-3] dokumentierten Sicherheitsparameter verwendet werden, die über die in [E.Doc.NetworkInterfaces] beschriebenen Netzwerkschnittstellen übertragen werden.

[E.Doc.CommunicationProtocol] Beschreibung des Kommunikationsprotokolls, das für die Kommunikation über die Netzwerkschnittstellen verwendet wird, und wie [E.Doc.SCM-3] im Protokoll angewendet wird.

[E.Doc.OperationalStates] Beschreibung der Betriebszustände des Geräts, wie sich diese Zustände vom üblichen Betriebszustand unterscheiden und unter welchen sicheren Bedingungen die Betriebszustände eintreten können.

5.5.3.4.3 Konzeptuelle Beurteilung

5.5.3.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle sicheren Kommunikationsmechanismen des Geräts die Vertraulichkeit von vertraulichen Sicherheitsparametern schützen.

5.5.3.4.3.2 Voraussetzungen

Keine.

5.5.3.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each secure communication mechanism;
:For each operational state;
if (Is the confidentiality of the assets sufficiently \nprotected to ensure
   that attacks on secure \ncommunication sessions do not lead to their
   \ndisclosure?) then (Yes)
  #lightgreen :PASS;
  detach;
else (No)
  #pink :FAIL;
  detach;
endif
@enduml
```

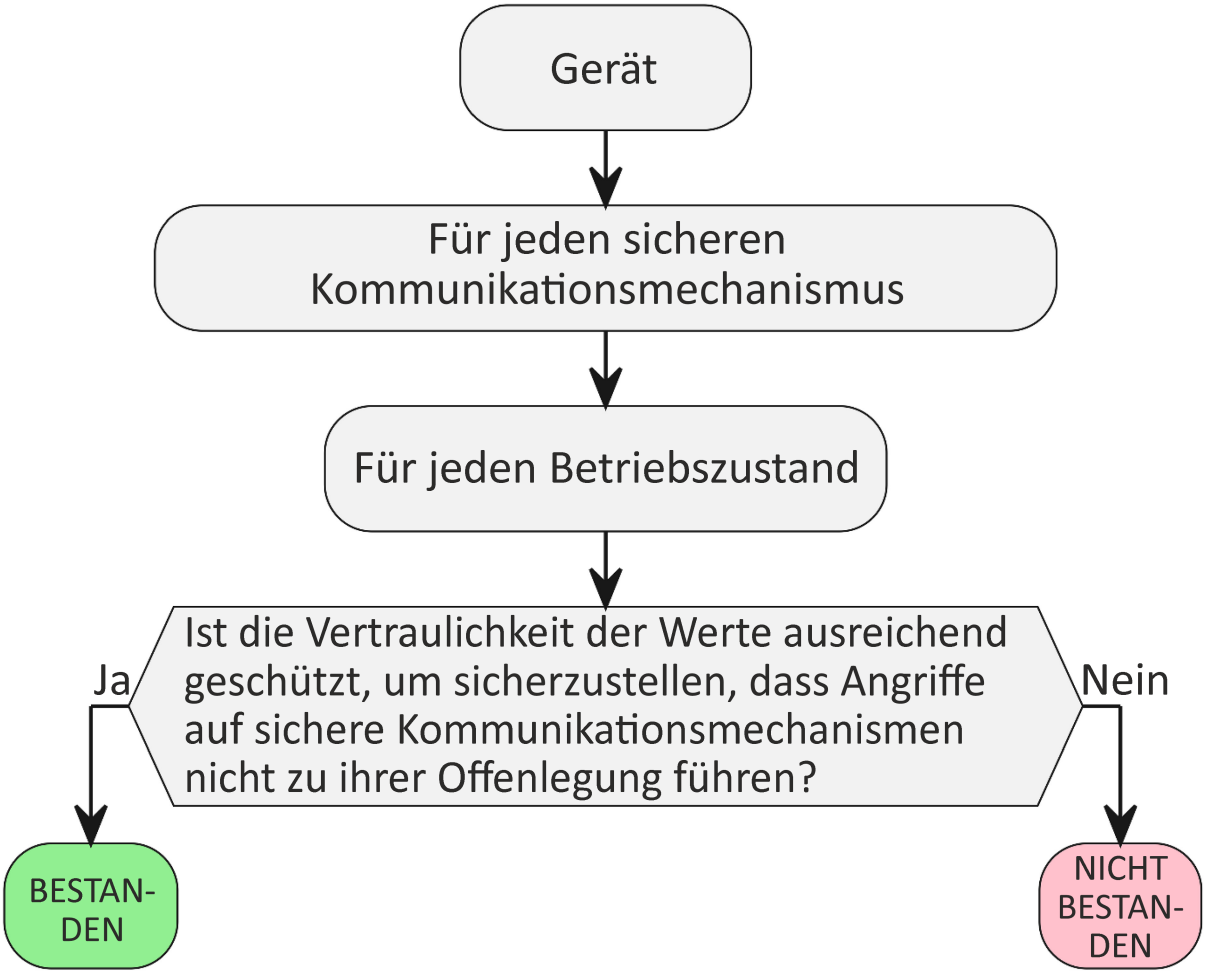

Bild 17 — Entscheidungsbaum für Anforderung SCM-3

Für jeden sicheren Kommunikationsmechanismus in [E.Doc.SCM-3] und für jeden in [E.Doc.OperationalStates] beschriebenen Zustand ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.SCM-3] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.SCM-3] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SCM-3] dokumentierte Begründung zu untersuchen.

5.5.3.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.5.3.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.5.3.4.5 Beurteilung der funktionalen Suffizienz

5.5.3.4.5.1 Zweck der Beurteilung

Der Zweck dieses Prüffalls ist die funktionale Beurteilung, ob die kommunizierten Werte vor unbemerktem Abhören geschützt sind.

5.5.3.4.5.2 Voraussetzungen

— Das Gerät muss sich im üblichen Betriebszustand befinden, und alle [E.Doc.NetworkInterfaces], die Teil der bestimmungsgemäßen Verwendung sind, sind entweder aktiviert oder so konfiguriert, dass jede Netzwerkschnittstelle geprüft werden kann.

— Bei Schnittstellen, für die [E.Doc.SCM-3] implementiert sind, stehen die notwendigen Zugangsdaten zur Verfügung, um die Kommunikation zu einem Gegenüber einzurichten, und die benötigten CSPs sind bereitgestellt oder konfiguriert, um jede gesicherte Kommunikationsschnittstelle [E.Doc.NetworkInterfaces] prüfen zu können.

— Prüf-Tools wie unter anderem Protokollanalysatoren für [E.Doc.CommunicationProtocol].

5.5.3.4.5.3 Beurteilungseinheiten

Zwischen dem Gerät und einem rechtmäßigen Kommunikationsendpunkt wird eine rechtmäßige Kommunikationssitzung auf den [E.Doc.NetworkInterfaces] unter Verwendung des [E.Doc.CommunicationProtocol] eingerichtet. Der Prüffall deckt Abhörangriffe bezüglich der Kommunikation der übertragenen vertraulichen Sicherheitsparameter ab.

5.5.3.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— alle sicheren Kommunikationsmechanismen korrekt und wie dokumentiert implementiert sind;

— kein Abhörangriff erfolgreich war.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.5.4 [SCM-4] Angemessener Wiederholungsschutz für sichere Kommunikationsmechanismen

5.5.4.1 Anforderung

Jeder sichere Kommunikationsmechanismus, der SCM-1 unterliegt, muss die übertragenen Sicherheitswerte und Netzwerkwerte gegen Wiederholungsangriffe schützen, außer

— eine zweifache Übertragung von Sicherheitswerten und Netzwerkwerten verursacht keine Bedrohung durch einen Wiederholungsangriff.

5.5.4.2 Begründung

Ein Wiederholungsangriff ist eine Netzwerkangriffsart, bei der eine gültige Datenübertragung böswillig wiederholt wird. Ein Angreifer, der sich Zugang zum Netzwerk verschafft hat, könnte die Kommunikation aufzeichnen und unverändert wieder abspielen, was zu unerwünschten Auswirkungen bei der empfangenden Entität führen kann.

Wird beispielsweise während eines Benutzer-Anmeldevorgangs das Passwort verschlüsselt, aber ohne Wiederholungsschutz übertragen, könnte ein Angreifer in der Lage sein, den Teil der Kommunikation mit der verschlüsselten Anmeldung zu wiederholen und so böswillig einen autorisierten Zugang zum Gerät zu erhalten.

Das Gerät muss die Kommunikation vor dieser Klasse von Angriffen schützen.

Auf der Grundlage einer Gefährdungseinschätzung könnten Anwendungsfälle identifiziert werden, für die möglicherweise kein Wiederholungsschutz erforderlich ist, z. B. wenn die übertragenen Daten nicht zu einer Zustandsänderung bei der empfangenden Entität führen. So stellt beispielsweise die Anforderung, ein X.509-Zertifikat von einem Server abzurufen, möglicherweise kein Risiko für einen Wiederholungsangriff dar.

5.5.4.3 Leitlinie

Wiederholungsangriffe können üblicherweise verhindert werden, indem jedes Datenpaket einer Kommunikationssitzung mit einer Sitzungs-ID und einem Zähler gekennzeichnet wird. Die Sitzungs-ID verhindert Wiederholungsangriffe der gesamten Kommunikation, während der Zähler die Wiederholung eines spezifischen Datenpakets innerhalb einer Kommunikationssitzung verhindert.

5.5.4.4 Beurteilungskriterien

5.5.4.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung SCM-4.

5.5.4.4.2 Erforderliche Informationen

[E.Doc.DT.SCM-4] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 19 für jeden Kommunikationsmechanismus in jedem Betriebszustand.

[E.Just.DT.SCM-4] Begründung des gewählten Pfads durch den Entscheidungsbaum in Bild 19 für jeden Kommunikationsmechanismus in jedem Betriebszustand. Dies ist eine dokumentierte Analyse (z. B. auf Grundlage von Bedrohungsmodellen und Sicherheitsrisikobeurteilungen), Begründung und eine Entscheidung bezüglich der Angemessenheit von Mechanismen und Verfahren zum Schutz des übertragenen Werts vor Wiederholungsangriffen.

[E.Doc.SecurityAsset.SCM] Vollständige Dokumentation der über die Netzwerkschnittstellen kommunizierten Sicherheitswerte.

[E.Doc.NetworkAsset.SCM] Vollständige Dokumentation der über die Netzwerkschnittstellen kommunizierten Netzwerkwerte.

[E.Doc.SCM-4] Dokumentierte Liste von Sicherheitsmechanismen und kryptographischen Verfahren, die zum Schutz der in [E.Doc.SecurityAsset.SCM] dokumentierten Sicherheitswerte und der übertragenen, in [E.Doc.NetworkAsset.SCM] dokumentierten Netzwerkwerte vor Wiederholungsangriffen über die in [E.Doc.NetworkInterfaces] beschriebenen Netzwerkschnittstellen verwendet werden.

[E.Doc.CommunicationProtocol] Beschreibung des Kommunikationsprotokolls, das für die Kommunikation über die Netzwerkschnittstellen verwendet wird, und wie [E.Doc.SCM-4] im Protokoll angewendet wird.

[E.Doc.OperationalStates] Beschreibung der Betriebszustände des Geräts, wie sich diese Zustände vom üblichen Betriebszustand unterscheiden und unter welchen sicheren Bedingungen die Betriebszustände eintreten können.

5.5.4.4.3 Konzeptuelle Beurteilung

5.5.4.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle sicheren Kommunikationsmechanismen des Geräts die Kommunikation der übertragenen Sicherheitswerte und Netzwerkwerte vor Wiederholungsangriffen schützen.

5.5.4.4.3.2 Voraussetzungen

Keine.

5.5.4.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each secure communication mechanism;
:For each operational state;
if (Does the duplicate transfer of an asset \npose a threat of a replay
   attack?) then (Yes)
  if (Is the transfer of the asset information\nprotected against replay
   attacks?) then (Yes)
    #lightgreen :PASS\nProtected;
    detach;
  else (No)
    #pink :FAIL\nNot protected;
    detach;
  endif
else (No)
  #application :NOT APPLICABLE \nRisk does not exist;
  detach;
@enduml
```

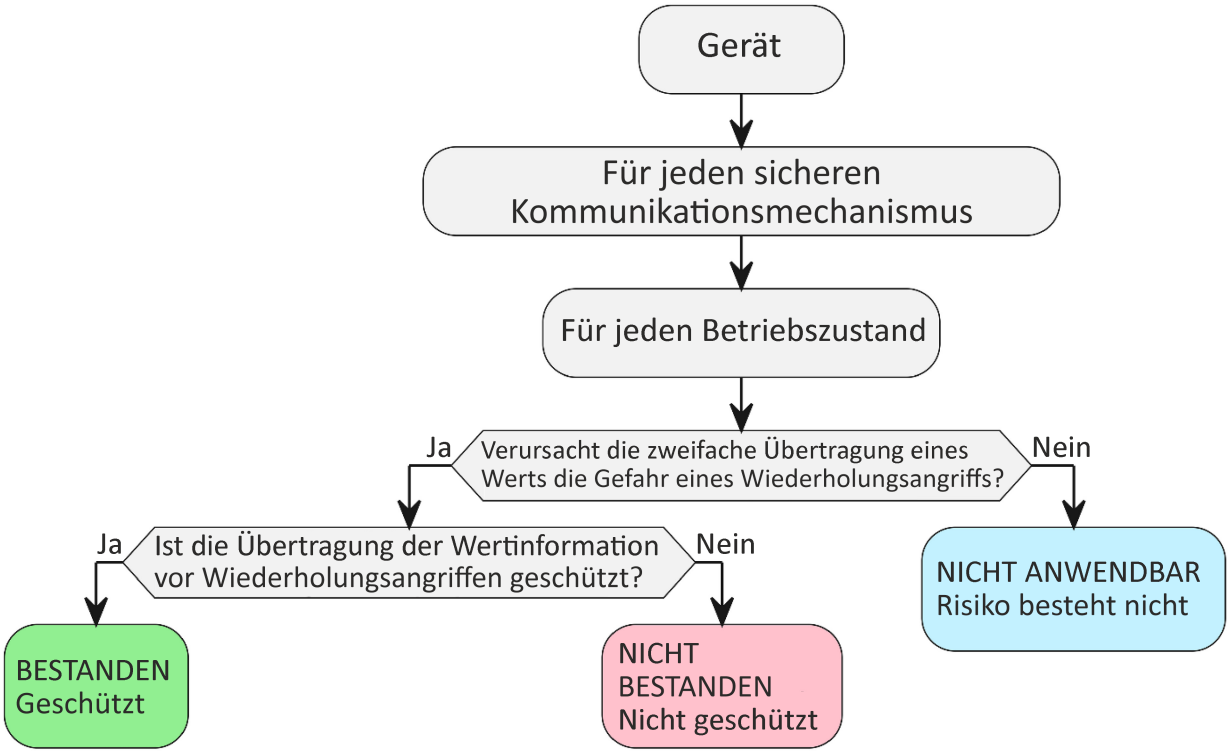

Bild 18 — Entscheidungsbaum für Anforderung SCM-4

Für jeden sicheren Kommunikationsmechanismus in [E.Doc.SCM-4] und für jeden in [E.Doc.OperationalStates] beschriebenen Zustand ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.SCM-4] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.SCM-4] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.SCM-4] dokumentierte Begründung zu untersuchen.

5.5.4.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle dokumentierten Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle dokumentierten Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.5.4.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.5.4.4.5 Beurteilung der funktionalen Suffizienz

5.5.4.4.5.1 Zweck der Beurteilung

Der Zweck dieses Prüffalls ist die funktionale Beurteilung, ob die kommunizierten Werte vor Wiederholungsangriffen geschützt sind.

5.5.4.4.5.2 Voraussetzungen

— Das Gerät muss sich im üblichen Betriebszustand befinden, und alle [E.Doc.NetworkInterfaces], die Teil der bestimmungsgemäßen Verwendung sind, sind entweder aktiviert oder so konfiguriert, dass jede Netzwerkschnittstelle geprüft werden kann.

— Bei Schnittstellen, für die [E.Doc.SCM-4] implementiert sind, sind die notwendigen CSPs zur Verfügung gestellt oder konfiguriert, um jede gesicherte Kommunikationsschnittstelle in [E.Doc.NetworkInterfaces] prüfen zu können.

— Prüf-Tools wie unter anderem Protokollanalysatoren für [E.Doc.CommunicationProtocol].

5.5.4.4.5.3 Beurteilungseinheiten

a) Zwischen dem Gerät und einem rechtmäßigen Kommunikationsendpunkt ist eine rechtmäßige Kommunikationssitzung auf den [E.Doc.NetworkInterfaces] unter Verwendung des [E.Doc.CommunicationProtocol] einzurichten. Die Kommunikation von Sicherheitswerten und Netzwerkwerten wird aufgezeichnet.

b) Es wird ein Versuch unternommen, Teile der Kommunikation oder die vollständige aufgezeichnete Kommunikation zu wiederholen.

5.5.4.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— alle sicheren Kommunikationsmechanismen korrekt und wie dokumentiert implementiert sind;

— kein Wiederholungsangriff erfolgreich war.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.6 [RLM] Resilienzmechanismus (en: Resilience Mechanism)

5.6.1 [RLM-1] Anwendbarkeit von Resilienzmechanismen

5.6.1.1 Anforderung

Das Gerät muss Resilienzmechanismen nutzen, um die Auswirkungen von DoS-Angriffen auf Netzwerkschnittstellen einzudämmen und diese nach dem Angriff wieder in einen definierten Zustand zu versetzen, außer:

— die Netzwerkschnittstelle des Geräts wird nur in einem lokalen Netzwerk verwendet, das nicht mit anderen Netzwerken interagiert;

— Geräte im Netzwerk bieten ausreichenden Schutz vor DoS-Angriffen und dem Verlust der grundlegenden Gerätefunktionalität für den Netzwerkbetrieb.

5.6.1.2 Begründung

Denial-of-Service-Angriffe stören die Verfügbarkeit von Netzwerkressourcen und können eine dauerhafte Unterbrechung des Netzwerkbetriebs verursachen, wenn das Gerät nach einem Denial-of-Service-Angriff nicht ordnungsgemäß wiederhergestellt wird.

5.6.1.3 Leitlinie

Um die Auswirkungen solcher Angriffe auf Netzwerkschnittstellen zu begrenzen, sollten Geräte so ausgelegt sein, dass sie Funktionen zur Begrenzung der Auswirkungen solcher Angriffe auf Netzwerkdienste und -ressourcen nutzen können.

Dies bedeutet, dass die Geräte so ausgelegt sind, dass sie nach einem Denial-of-Service-Angriff wieder in einen definierten Zustand versetzt werden. Der definierte Zustand wird vom Gerätehersteller für die bestimmungsgemäße Verwendung festgelegt und kann Resilienzmechanismen beinhalten, die es ermöglichen, dass das Gerät grundlegende Funktionen aufrechterhält, während es den Auswirkungen von Denial-of-Service-Angriffen auf eine oder mehrere seiner Netzwerkschnittstellen ausgesetzt ist.

Das Gerät erreicht während des Angriffs einen definierten Zustand und kehrt nach Ende des Angriffs in einen definierten Betriebszustand zurück. Das Ziel ist es sicherzustellen, dass das Gerät während eines gerade stattfindenden Angriffs auf die Netzwerkschnittstellen weiterhin arbeitet. Beispiele für Resilienzmechanismen, die je nach der bestimmungsgemäßen Verwendung des Geräts anwendbar sein können, sind:

— Schutz vor Netzwerk-Sturm-Angriffen;

— Netzwerk-Paketfiltermechanismen;

— Techniken zur Begrenzung des Netzwerkverkehrs;

— Strategien zur Reservierung interner Geräteressourcen (zur Begrenzung der Ressourcennutzung und zum Schutz vor Überlastung).

5.6.1.4 Beurteilungskriterien

5.6.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung RLM-1.

5.6.1.4.2 Erforderliche Informationen

[E.Doc.DT.RLM-1] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 20 für jede Netzwerkschnittstelle.

[E.Just.DT.RLM-1] Begründung für den gewählten Pfad durch den Entscheidungsbaum in Bild 20 für jede Netzwerkschnittstelle.

(Falls das Gerät über Netzwerkschnittstellen mit dem Netzwerk kommuniziert) [E.Doc.NetworkInterfaces] Vollständige Dokumentation der Netzwerkschnittstellen.

(Falls das Gerät über einen Resilienzmechanismus zur Eindämmung der Auswirkungen von DoS-Angriffen auf die Netzwerkschnittstellen verfügt) [E.Doc.RLM] Vollständige Dokumentation des Satzes von Resilienzmechanismen, die zur Eindämmung der Auswirkungen von DoS-Angriffen auf die Netzwerkschnittstellen eingesetzt werden und die das Gerät nach dem Angriff in einen definierten Zustand versetzen.

5.6.1.4.3 Konzeptuelle Beurteilung

5.6.1.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob ein Resilienzmechanismus implementiert wurde, wo er erforderlich ist.

5.6.1.4.3.2 Voraussetzungen

Keine.

5.6.1.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:Equipment;
:For each network interface;
if (Is the network interface intended to be \nused to communicate with other
   \nequipment in a local network only? ) then (Yes, local \nnetwork only )
            #application :NOT APPLICABLE \ncondition for the network
   \ninterface;
            detach
    else (No)
      if (Does equipment in the network provide \nsufficient protection
   against loss of \n function of the equipment? ) then (Yes, resources in
   \nthe network )
            #application :NOT APPLICABLE \ncondition for the network
   \ninterface;
            detach
      else (No)
        if (Does the equipment use resilience \nmechanisms to mitigate the
   effects \nof DoS Attacks on the network \ninterfaces and return to a
   defined \nstate after attack? ) then (Yes )
            #lightgreen :PASS for network interface: \napplicable and met;
```

```
            detach
        else (No)
          #pink :FAIL for network interface: \nApplicable but not met;
          detach
        endif
      endif
    endif
@enduml
```

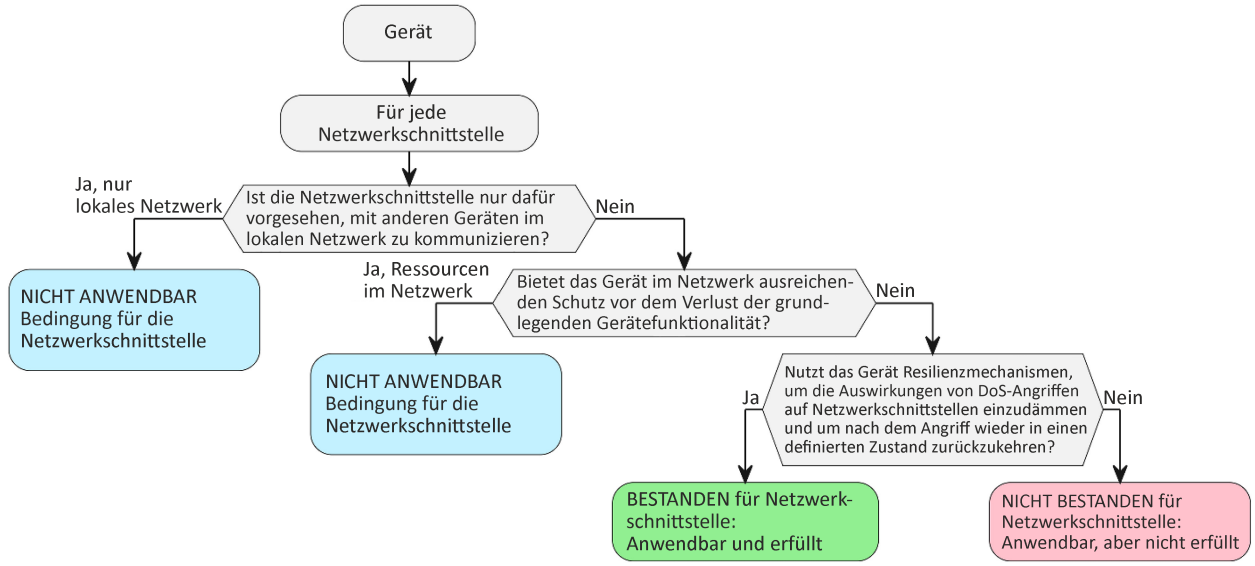

Bild 19 — Entscheidungsbaum für Anforderung RLM-1

Für jede in [E.Doc.NetworkInterfaces] dokumentierte Netzwerkschnittstelle ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.RLM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.RLM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.RLM-1] dokumentierte Begründung zu untersuchen.

5.6.1.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.6.1.4.4 Beurteilung der funktionalen Vollständigkeit

5.6.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Validierung, ob die implementierten Resilienzmechanismen die Auswirkungen von DoS-Angriffen auf die Netzwerkschnittstellen eindämmen und ob das Gerät nach dem Angriff wieder in einen definierten Zustand zurückkehrt, wobei die Vollständigkeit der Dokumentation und die ordnungsgemäße Implementation zu berücksichtigen sind.

5.6.1.4.4.2 Voraussetzungen

— Das Gerät befindet sich im Betriebszustand, und alle [E.Doc.NetworkInterfaces] müssen entweder aktiviert oder konfiguriert sein, so dass jede Netzwerkschnittstelle geprüft werden kann.

— Falls [E.Doc.RLM] verwendet werden, steht die Information zur Verfügung, welche Konfiguration zur Prüfung der implementierten Mechanismen erforderlich ist.

5.6.1.4.4.3 Beurteilungseinheiten

— Es ist funktional zu beurteilen, ob es Netzwerkschnittstellen gibt, die nicht in [E.Doc.NetworkInterfaces] aufgeführt sind.

— Es ist funktional zu beurteilen, ob die Resilienzmechanismen wie in [E.Doc.RLM] dokumentiert implementiert sind.

5.6.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle identifizierten Netzwerkschnittstellen in [E.Doc.NetworkInterfaces] dokumentiert sind; und

— alle konfigurierten Resilienzmechanismen in [E.Doc.RLM] dokumentiert sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn mindestens eine gefundene Netzwerkschnittstelle nicht in [E.Doc.NetworkInterfaces] dokumentiert ist oder wenn die Resilienzmechanismen nicht wie in [E.Doc.RLM] dokumentiert implementiert sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.6.1.4.5 Beurteilung der funktionalen Suffizienz

5.6.1.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob Resilienzmechanismen implementiert wurden, wo sie erforderlich sind.

5.6.1.4.5.2 Voraussetzungen

— Das Gerät befindet sich im Betriebszustand, und alle [E.Doc.NetworkInterfaces] sind entweder aktiviert oder konfiguriert.

— Falls [E.Doc.RLM] verwendet werden, steht die Information zur Verfügung, welche Konfiguration zur Prüfung der implementierten Mechanismen erforderlich ist.

— Prüf-Tools. Der Zweck der Prüf-Tools ist es festzustellen, ob das Gerät, wenn es simulierten DoS-Angriffen auf die Netzwerkschnittstellen ausgesetzt wird, nach den simulierten Angriffsszenarien zu einem definierten Zustand zurückkehren kann. Beispiele für Tools sind:

— Netzwerk-Scanning-Tools;

— Flutungs-Prüf-Tools;

— Anwendungs-Scanning-Tools, um zugängliche Dienste zu erkennen, und gegebenenfalls Fuzzing-Tools wie beispielsweise:

  — Protokoll-Fuzzing-Tools;

  — Anwendungs-Fuzzing-Tools.

5.6.1.4.5.3 Beurteilungseinheiten

Es ist funktional zu bestätigen, dass die in [E.Doc.RLM] dokumentierten und in der Begründung [E.Just.DT.RLM-1] verwendeten Resilienzmechanismen [vorhanden sind/genutzt werden].

Es ist funktional zu beurteilen, ob die Resilienzmechanismen die Auswirkungen von DoS-Angriffen auf die Netzwerkschnittstellen eindämmen und ob das Gerät nach einem Angriff wieder in einen definierten Zustand zurückkehrt, wobei die bestimmungsgemäße Verwendung des Geräts und die vorgesehene Betriebsumgebung zu berücksichtigen sind.

5.6.1.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die Resilienzmechanismen nicht wie dokumentiert [vorhanden sind/genutzt werden].

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die Resilienzmechanismen nicht wie dokumentiert [vorhanden sind/genutzt werden].

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.7 [NMM] Netzwerküberwachungsmechanismus (en: Network Monitoring Mechanism)

5.7.1 [NMM-1] Anwendbarkeit eines angemessenen Netzwerküberwachungsmechanismus

5.7.1.1 Anforderung

Netzwerkeinrichtungen müssen über Netzwerküberwachungsmechanismen verfügen, um Nachweise von DoS-Angriffen zu erkennen, die vom Gerät empfangen werden, außer:

— die Netzwerkeinrichtung ist nicht dafür vorgesehen, andere Geräte mit öffentlichen Netzwerken zu verbinden.

5.7.1.2 Begründung

Um die Cyber-Resilienz eines Gesamtsystems gegen bei bestimmungsgemäßer Verwendung des Geräts ungewöhnlichen Netzwerkverkehr zu verbessern, der zu einem Denial-of-Service-(DoS-)Angriff führen könnte, muss jede Netzwerkeinrichtung als Komponente eines solchen Geräts in der Lage sein, Anzeichen für solche DoS-Ereignisse zu erkennen. Hierfür ist es erforderlich, dass das Gerät ungewöhnlichen Verkehr und Muster erkennen kann, die mit einem DoS-Angriff in Zusammenhang stehen könnten.

5.7.1.3 Leitlinie

Ungewöhnlicher Verkehr, der zu berücksichtigen ist, sind Netzwerkdatenpakete, die zu einem teilweisen oder vollständigen Denial-of-Service des Netzwerks führen können.

Ein DoS-Ereignis kann durch eine unbeabsichtigte Fehlfunktion einer beliebigen Netzwerkressource oder durch einen absichtlichen Angriff verursacht werden.

Um die Auswirkungen eines DoS-Ereignisses erkennen zu können, muss das Gerät in der Lage sein, eine Analyse der Häufigkeit von Datenpaketen und deren Auswirkung auf die Verfügbarkeit der Dienste des Geräts durchzuführen. Die Erkennung von DoS-Ereignissen kann verhaltens- oder signaturbasiert sein, je nachdem, welches Verfahren für das Gerät, die bestimmungsgemäße Verwendung und die vorgesehene Betriebsumgebung angemessen ist.

Eine allgemeine Maßnahme gegen DoS-Ereignisse ist die Deaktivierung von über Netzwerkschnittstellen zugänglichen Diensten, die nicht für die bestimmungsgemäße Verwendung des Geräts erforderlich sind.

Beispiele für Maßnahmen, die zur Überwachung des Netzwerkverkehrs bezüglich möglicher DoS-Angriffe implementiert werden könnten, sind:

— Überwachung der Anzahl von Datenpaketen innerhalb eines bestimmten Zeitraums;

— Überwachung, ob Datenpakete vorhanden sind, die von einem unbekannten Netzwerk stammen oder die ein Zielnetzwerk haben, das außerhalb des für die Netzwerkeinrichtung konfigurierten Netzwerks liegt;

— Überwachung, ob eine ungewöhnliche Anzahl von Datenpaketen vorhanden ist, die eine ungewöhnliche Umlaufzeit aufweisen oder bei denen eine Zeitüberschreitung auftritt.

5.7.1.4 Beurteilungskriterien

5.7.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung NMM-1.

5.7.1.4.2 Erforderliche Informationen

— [E.Doc.DT.NMM-1] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 21 für den Netzwerküberwachungsmechanismus.

— [E.Just.DT.NMM-1] Begründung für den gewählten Pfad durch den Entscheidungsbaum in Bild 21 für den Netzwerküberwachungsmechanismus.

Wenn das Gerät eine Netzwerkeinrichtung ist, die Verbindung zu anderen Geräten in öffentlichen Netzwerken hat:

— [E.Doc.NMM] Dokumentation des zur Überwachung und Analyse des Verkehrs zwischen Netzwerken implementierten Überwachungsmechanismus, der mittels der Netzwerkschnittstellen der Netzwerkeinrichtung verarbeitet wird.

— [E.Just.network.Risk] Dokumentierte Analyse, Begründung und Beurteilung der Risiken für Sicherheits- und Netzwerkwerte, die von der Netzwerkeinrichtung zwischen Netzwerken verarbeitet, kontrolliert oder bedient werden, im Kontext der bestimmungsgemäßen Verwendung und der vorgesehenen Betriebsumgebung.

5.7.1.4.3 Konzeptuelle Beurteilung

5.7.1.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob ein Netzwerküberwachungsmechanismus implementiert wurde, wo er erforderlich ist.

5.7.1.4.3.2 Voraussetzungen

Keine.

5.7.1.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
if (Is the equipment a \nNetwork Equipment? ) then (Yes)
      if (Is the Network Equipment intended to \nconnect other equipment to
   a public network?) then (No)
      #application :NOT APPLICABLE\ncondition for\nnon-applicability met;
      detach;
    else (Yes)
      if (Does the Network Equipment provide a network monitoring mechanism
   ) then (No)
          #pink :FAIL\napplicable but not met;
          detach;
        else (Yes)
          #lightgreen :PASS\napplicable and met;
          detach;
        endif
    endif
else (No)
  #application :NOT APPLICAPLE\ncondition for requirement's\napplicability
   not met;
  detach;
endif
@enduml
```

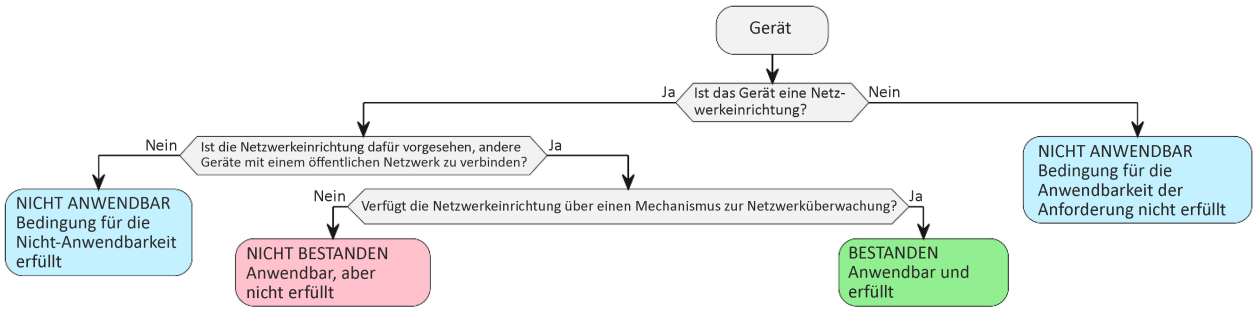

Bild 20 — Entscheidungsbaum für Anforderung NMM-1

Für jeden in [E.Doc.DT.NMM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.NMM-1] dokumentierte Begründung zu untersuchen.

Es ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.NMM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

5.7.1.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.7.1.4.4 Beurteilung der funktionalen Vollständigkeit

5.7.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Validierung, ob der durch die Netzwerkeinrichtung kontrollierte oder verarbeitete Verkehr zwischen Netzwerken überwacht und analysiert wird, um das Risiko für Sicherheits- und Netzwerkwerte in den durch das Gerät kontrollierten oder bedienten Netzwerken einzudämmen, und zwar in Bezug auf die Vollständigkeit der Dokumentation und die korrekte Implementation.

5.7.1.4.4.2 Voraussetzungen

Das Gerät muss sich im Betriebszustand befinden und, falls verfügbar, muss die Einrichtung oder Konfiguration in Bezug auf den Verkehr zwischen den Netzwerken durchgeführt worden sein.

Die physische Netzwerkverbindung für die Kommunikation zwischen Netzwerken ist eingerichtet.

5.7.1.4.4.3 Beurteilungseinheiten

— Funktionale Beurteilung, ob der von der Netzwerkeinrichtung kontrollierte oder verarbeitete Verkehr zwischen Netzwerken wie in [E.Doc.NMM] beschrieben überwacht und analysiert wird.

— Versuch der Aufdeckung des gesamten, durch das Gerät kontrollierten oder verarbeiteten Verkehrs zwischen Netzwerken, auch wenn der entsprechende Verkehr nicht in [E.Just.network.Risk] beschrieben oder dokumentiert ist.

5.7.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— alle Verkehrsarten zwischen Netzwerken in [E.Just.networkRisk] dokumentiert sind; und

— für alle in [E.Doc.NMM] beschriebenen Überwachungsmechanismen nachgewiesen ist, dass sie wie vorgesehen arbeiten. Es liegt kein Nachweis vor, dass die Implementation der Netzwerküberwachungsmechanismen von der Dokumentation abweicht.

Die Entscheidung NICHT ANWENDBAR wird zugewiesen, wenn:

— Die Netzwerkeinrichtung nicht dafür vorgesehen ist, andere Geräte mit öffentlichen Netzwerken zu verbinden.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.7.1.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.8 [TCM] Verkehrssteuerungsmechanismus (en: Traffic Control Mechanism)

5.8.1 [TCM-1] Anwendbarkeit eines angemessenen Verkehrssteuerungsmechanismus

5.8.1.1 Anforderung

Wenn das Gerät eine Netzwerkeinrichtung ist, die der Verbindung anderer Geräte mit einem öffentlichen Netzwerk dient, dann muss das Gerät über mindestens einen Netzwerksteuerungsmechanismus verfügen.

5.8.1.2 Begründung

Durch ein kompromittiertes Gerät kann unter Umständen schädlicher Datenverkehr erzeugt werden. Zwar können Betreiber öffentlicher Netzwerke auf Grundlage der Netzwerkinformationen von Datenpaketen Maßnahmen ergreifen, um die Auswirkungen von schädlichem Verkehr einzudämmen, aber die Kenntnis der Netzwerkeigenschaften kann effektive Gegenmaßnahmen behindern. Netzwerkeinrichtungen, die bestimmungsgemäß der Verbindung mit öffentlichen Netzwerken dienen, können über ausreichende Informationen zur Erkennung schädlichen Verkehrs verfügen, und ein Verkehrssteuerungsmechanismus ermöglicht den Schutz des öffentlichen Netzwerks vor entsprechenden Schäden.

5.8.1.3 Leitlinie

Zu den übliche Gerätekategorien, deren bestimmungsgemäße Verwendung die Weiterleitung von Datenpaketen an öffentliche Netzwerke einschließt, gehören beispielsweise Home-Router, die private IP-Netzwerke mit dem Internet verbinden, oder mobile Netzwerkzugangspunkte (d. h. Basisstationen), die anderen Geräten den Zugang zu öffentlichen Mobilnetzen ermöglichen.

Um den Datenverkehr auf Netzwerkebene auf Grundlage von Netzwerkadressen zu kontrollieren, muss die Netzwerkeinrichtung bestimmte Datenpakete aufgrund ihrer Quell- oder Zieladresse blockieren oder umleiten können.

5.8.1.4 Beurteilungskriterien

5.8.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung TCM-1.

5.8.1.4.2 Erforderliche Informationen

[E.Doc.DT.TCM-1] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 22 für den Verkehrssteuerungsmechanismus.

[E.Just.DT.TCM-1] Begründung für den gewählten Pfad durch den Entscheidungsbaum in Bild 22 für den Verkehrssteuerungsmechanismus.

[E.Doc.TCM] das Dokument beschreibt den von der Netzwerkeinrichtung wie in [E.Doc.NetworkEquipment] dokumentiert implementierten Verkehrssteuerungsmechanismus.

5.8.1.4.3 Konzeptuelle Beurteilung

5.8.1.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob ein Verkehrssteuerungsmechanismus implementiert wurde, wo er erforderlich ist.

5.8.1.4.3.2 Voraussetzungen

Keine.

5.8.1.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
if (Is the equipment a \nNetwork Equipment? ) then (Yes)
      if (Is the Network Equipment intended to \nconnect other devices to a
   public network?) then (No)
      #application :NOT APPLICABLE\ncondition for\nnon-applicability met;
      detach;
    else (Yes)
      if (Does the Network Equipment \nprovide a traffic control mechanism?
   ) then (No)
         #pink :FAIL\napplicable but not met;
         detach;
       else (Yes)
         #lightgreen :PASS\napplicable and met;
         detach;
       endif
    endif
else (No)
  #application :NOT APPLICAPLE\ncondition for requirement's\napplicability
   not met;
  detach;
endif
@enduml
```

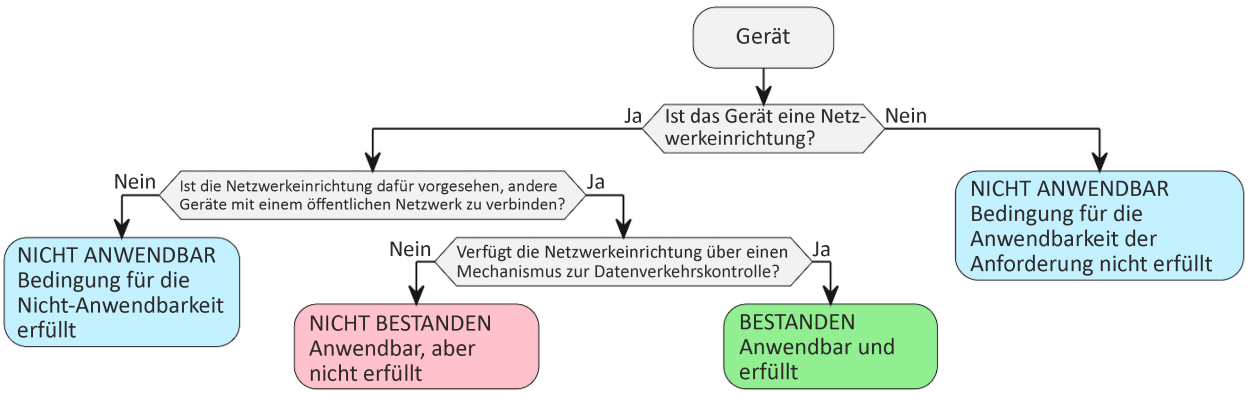

Bild 21 — Entscheidungsbaum für Anforderung TCM-1

Für jeden in [E.Doc.DT.TCM-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.TCM-1] dokumentierte Begründung zu untersuchen.

Es ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.TCM-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

5.8.1.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.8.1.4.4 Beurteilung der funktionalen Vollständigkeit

5.8.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Validierung, ob der durch die Netzwerkeinrichtung zu einem öffentlichen Netzwerk weitergeleitete Verkehr kontrolliert wird, um die Schädigung oder Verletzung von Sicherheits- und Netzwerkwerten in den Netzwerken zu verhindern, die von der Netzwerkeinrichtung kontrolliert oder bedient werden, und zwar in Bezug auf die Vollständigkeit der Dokumentation und die korrekte Implementation.

5.8.1.4.4.2 Voraussetzungen

Das Gerät muss sich im Betriebszustand befinden und, falls verfügbar, muss die Einrichtung oder Konfiguration in Bezug auf den Verkehr zwischen den Netzwerken durchgeführt worden sein.

5.8.1.4.4.3 Beurteilungseinheiten

— Funktionale Beurteilung, ob der durch die Netzwerkeinrichtung an ein öffentliches Netzwerk weitergeleitete Verkehr wie in [E.Doc.TCM] beschrieben kontrolliert wird.

5.8.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— alle Steuerungsmechanismen in [E.Doc.TMC] dokumentiert sind; und

— für alle in [E.Doc.TCM] beschriebenen Steuerungsmechanismen nachgewiesen ist, dass sie wie vorgesehen arbeiten.

Die Entscheidung NICHT ANWENDBAR wird zugewiesen, wenn:

— die Netzwerkeinrichtung nicht dafür vorgesehen ist, den durch die Netzwerkeinrichtung zu einem öffentlichen Netzwerk weitergeleiteten Verkehr zu kontrollieren.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.8.1.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.9 [CCK] Vertrauliche kryptographische Schlüssel (en: Confidential Cryptographic Keys)

5.9.1 [CCK-1] Angemessene vertrauliche kryptographische Schlüssel (CCKs)

5.9.1.1 Anforderung

Vertrauliche kryptographische Schlüssel zum Schutz des Zugangs zu Netzwerk- und/oder Sicherheitswerten müssen bewährten Verfahrensweisen für Kryptographie entsprechen, außer das Gerät erzwingt ihre Erzeugung bei der ersten Verwendung.

5.9.1.2 Begründung

Geräte können Kryptographie und damit CCKs für viele und unterschiedliche Zwecke nutzen, wie beispielsweise zur Authentisierung, um eine Kontrolle des Zugangs zu Werten zu erzwingen, zum Schutz der Vertraulichkeit oder Integrität von Werten während der Speicherung oder während der Übertragung zu einer anderen Entität, oder zur Ableitung anderer CCKs. Wenn die Vertraulichkeit oder Integrität eines CCK kompromittiert wird, können die vom CCK geschützten Werte unter Umständen ebenfalls kompromittiert werden. Ein CCK eines Geräts, der für einen kryptographischen Schutzalgorithmus generiert wurde, ist angemessen, wenn

— von einem erfolgreichen Angriff auf den CCK keine anderen, von diesem oder einem anderen Gerät verwendeten oder generierten CCKs betroffen sind und der Algorithmus bei Verwendung dieses CCK ausreichend stark ist, um bei seiner Nutzung auftretenden Angriffen zu widerstehen, deren Ziel die Zerstörung der Vertraulichkeit und Integrität ist.

5.9.1.3 Leitlinie

Die Lebensdauer eines CCK ist ein wichtiger Aspekt, der über die erforderliche Widerstandskraft des CCK gegenüber Angriffen bestimmt. Langfristige CCKs, die über lange Zeitspannen gespeichert und wiederholt genutzt werden, benötigen im Vergleich zu kurzfristigen CCKs, die üblicherweise auf dem Gerät erzeugt und nur für kurze Zeit genutzt werden, eine zeitlich längere Widerstandsfähigkeit gegen Angriffe. Typische Beispiele für kurzfristige Schlüssel sind Sitzungsschlüssel, die zur Verschlüsselung der während einer einzigen Kommunikationssitzung übertragenen Werte verwendet werden.

Die Stärke von CCKs hängt von 3 Parametern ab:

— von ihrer Entropie;

— von ihrer Länge; und

— vom kryptographischen Algorithmus, mit dem sie verwendet werden.

CCKs müssen eine Länge und Entropie aufweisen, die für ihre erwartete Lebensdauer, für den kryptographischen Algorithmus, mit dem sie verwendet werden, und für ihre bestimmungsgemäße Verwendung angemessen ist. Für weitere Leitlinien siehe [CRY-1] Bewährte Verfahrensweisen für Kryptographie. Besondere Sorgfalt ist bei CCKs geboten, die nicht mehr verwendet werden; diese sind beispielsweise zu löschen. Es wird empfohlen, hierbei bewährte Verfahrensweisen zu befolgen.

Weitere bewährte Sicherheitsverfahren müssen ebenfalls berücksichtigt werden. Beispielsweise entspricht es bewährten Sicherheitsverfahren, einen CCK nur für einen Zweck zu verwenden. Es wird auch empfohlen, den gleichen CCK nicht zu replizieren und auf anderen Ausführungen/Einheiten dieses Geräts zu verwenden.

5.9.1.4 Beurteilungskriterien

5.9.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung CCK-1.

5.9.1.4.2 Erforderliche Informationen

[E.Doc.CCK] Liste der vom Gerät verwendeten CCKs. Für jeden CCK in der Liste:

1. Angabe des Verwendungszwecks (Verschlüsselung, Integritätsschutz und Authentisierung).
2. Angabe des Algorithmus und der Algorithmenmodi, mit denen er verwendet wird.
3. Festlegung der Länge.
4. Bereitstellung von Informationen über die Entropie.
    4.1 Es sind Empfehlungen für bewährte Verfahrensweisen anzugeben, gefolgt von der gewählten Länge und Entropie.
    4.2 Falls keine bewährten Verfahrensweisen befolgt werden, ist zu erläutern, warum diese Länge und Entropie als für den Algorithmus und seinen Verwendungszweck angemessen gelten.
5. Seine Lebensdauer. Es ist zu präzisieren, ob der CCK eine begrenzte Lebensdauer oder eine begrenzte Anzahl von Nutzungen hat. Falls zutreffend, sind die Lebensdauer bzw. ist die zulässige Anzahl von Nutzungen anzugeben.
6. Wie auf den CCK zugegriffen wird.
7. Ob der CCK auf dem Gerät erzeugt oder vor der Vermarktung vorinstalliert wird.
8. Das Verfahren, mit dem der CCK erzeugt wird bzw. wurde.

5.9.1.4.3 Konzeptuelle Beurteilung

5.9.1.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle vertraulichen kryptographischen Schlüssel in [E.Doc.CCK] aufgeführt sind, und die Bereitstellung aller erforderlichen Informationen zu jedem vertraulichen kryptographischen Schlüssel.

5.9.1.4.3.2 Voraussetzungen

Keine.

5.9.1.4.3.3 Beurteilungseinheiten

Es ist zu prüfen, ob alle vom Gerät verwendeten kryptographischen Schlüssel tatsächlich in [E.Doc.CCK] aufgeführt sind. Insbesondere sind die beschriebenen Mechanismen für die sichere Kommunikation, die Zugangssteuerung und die sichere Speicherung zu prüfen. Sind alle vom Gerät für einen dieser Mechanismen verwendeten kryptographischen Schlüssel in [E.Doc.CCK] aufgeführt?

5.9.1.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn

— alle vom Gerät für die sichere Kommunikation entsprechend SCM verwendeten kryptographischen Schlüssel in [E.Doc.CCK] aufgeführt sind;

— alle vom Gerät für die sichere Speicherung entsprechend SSM verwendeten kryptographischen Schlüssel in [E.Doc.CCK] aufgeführt sind;

— alle vom Gerät für die Zugangssteuerung entsprechend ACM verwendeten kryptographischen Schlüssel in [E.Doc.CCK] aufgeführt sind; und

— keine anderen Nachweise vorliegen, dass [E.Doc.CCK] unvollständig ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.9.1.4.4 Beurteilung der funktionalen Vollständigkeit

5.9.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist es festzustellen, ob die bereitgestellten Informationen und die Begründung für die Angemessenheit der durch das Gerät genutzten CCKs korrekt sind.

5.9.1.4.4.2 Voraussetzungen

Keine.

5.9.1.4.4.3 Beurteilungseinheiten

Für jeden im Dokument [E.Doc.CCK] angegebenen CCK muss beurteilt werden, ob der CCK den bewährten Verfahren für Kryptographie entspricht; vergleiche Anforderung CRY-1.

Insbesondere sind zu beurteilen:

— die Länge des CCK;

— die für seine Erzeugung verwendete Entropie;

— der Algorithmus, mit dem der CCK verwendet wird;

— die Lebensdauer bzw. die Anzahl der möglichen Nutzungen des CCK; und

— wie auf den CCK zugegriffen wird.

5.9.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn die Beurteilungen CRY-1 alle zum Ergebnis BESTANDEN führen.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.9.1.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.9.2 [CCK-2] Mechanismen zur Erzeugung vertraulicher kryptographischer Schlüssel

5.9.2.1 Anforderung

Die Erzeugung vertraulicher kryptographischer Schlüssel auf dem Gerät muss bewährten Verfahrensweisen entsprechen.

5.9.2.2 Begründung

CCKs, die vom Gerät erzeugt und zum Schutz von Werten verwendet werden, müssen angemessen sein, um erfolgreiche Angriffe aufgrund schwacher CCKs zu verhindern. Ein angemessener CCK-Erzeugungs-

mechanismus stellt sicher, dass die CCKs über die notwendigen Eigenschaften verfügen, die für die Risiken und die Betriebsbedingungen des Geräts angemessen sind.

5.9.2.3 Leitlinie

Die Sicherheitseigenschaften eines erzeugten CCKs hängen üblicherweise von einem oder mehreren der folgenden Faktoren ab:

— dem gewählten Algorithmus (darunter unter anderem der Satz möglicher CCK-Werte);

— den Eigenschaften des verwendeten Zufallszahlengenerators (der unter anderem einen Einfluss auf die Informationsmenge hat, die ein Angreifer erraten muss, um einen CCK zu rekonstruieren); und

— den Eigenschaften anderer verwendeter Informationen (wie beispielsweise anderer CCKs).

Zu den Risiken durch CCKs im Zusammenhang mit dem geschützten Wert können die erwarteten Schäden gehören, die durch einen nicht autorisierten Zugriff eines Angreifers auf einen geschützten Wert entstehen, und zwar durch:

— das Erraten eines CCKs; oder

— die Rekonstruktion eines CCKs auf Grundlage von zugänglichen Informationen.

Es ist daher entscheidend, dass der Mechanismus zur Erzeugung der CCKs keine schwachen CCKs erzeugt und keine Informationen über die CCK-Erzeugung bereitstellt.

Der mögliche Schaden, der bei einem nicht autorisierten Zugang zu einem geschützten Wert durch einen Angreifer entsteht, hängt ab von der Kritikalität des Werts, der bestimmungsgemäßen Verwendung und der für die Nutzung vorgesehenen Betriebsumgebung.

ANMERKUNG 1 Es gibt eine Reihe von anerkannten Normen für Schlüsselerzeugungsmechanismen. Anerkannte bewährte Verfahrensweisen für Zufallszahlgeneratoren sind beispielsweise NIST SP800-90A[9], NIST SP800-90B[10], NIST SP800-90C [11], BSI AIS31 [16].

Anerkannte bewährte Verfahrensweisen für die Ableitung von Schlüsseln sind beispielsweise hier beschrieben: NIST SP 800-108r1 [12], NIST SP 800-132 [13], SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms.

5.9.2.4 Beurteilungskriterien

5.9.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung CCK-2.

5.9.2.4.2 Erforderliche Informationen

[E.Doc.CCK] Liste der vom Gerät verwendeten CCKs. Für jeden CCK in der Liste:

1. Angabe des Verwendungszwecks (Verschlüsselung, Integritätsschutz und Authentisierung).

2. Angabe des Algorithmus und der Algorithmenmodi, mit denen er verwendet wird.

3. Festlegung der Länge.

4. Bereitstellung von Informationen über die Entropie.

    4.1 Es sind Empfehlungen für bewährte Verfahrensweisen anzugeben, gefolgt von der gewählten Länge und Entropie.

4.2 Falls keine bewährten Verfahrensweisen befolgt werden, ist zu erläutern, warum diese Länge und Entropie als für den Algorithmus und seinen Verwendungszweck angemessen gelten.

5. Seine Lebensdauer. Es ist zu präzisieren, ob der CCK eine begrenzte Lebensdauer oder eine begrenzte Anzahl von Nutzungen hat. Falls zutreffend, sind die Lebensdauer bzw. ist die zulässige Anzahl von Nutzungen anzugeben.

6. Wie auf den CCK zugegriffen wird.

7. Ob der CCK auf dem Gerät erzeugt oder vor der Vermarktung vorinstalliert wird.

8. Das Verfahren, mit dem der CCK erzeugt wird bzw. wurde.

Das Dokument [E.Doc.CCK-2] beschreibt Folgendes für jeden CCK-Erzeugungsmechanismus:

— Die Zufallszahlenquellen. Es sind die bewährten Verfahrensweisen anzugeben, gefolgt von der Zufallszahlenquelle. Es ist anzugeben, ob diese nach einem international anerkannten Sicherheitszertifizierungsschema zertifiziert ist, z. B. EUCC/SOGIS Common Criteria, FIPS 140-2 [17], FIPS 140-3 [18].

— Der Zufallszahlengenerator (RNG). Es ist anzugeben, ob es ein deterministischer oder nichtdeterministischer RNG ist. Es sind die bewährten Verfahrensweisen anzugeben, die der RNG befolgt. Es ist anzugeben, ob der RNG nach einer der international anerkannten Sicherheitszertifizierungen zertifiziert ist, z. B. EUCC/SOGIS Common Criteria, FIPS 140-2 [17], FIPS 140-3 [18].

— Es sind die Mechanismen zur Ableitung/Erstellung des CCK anzugeben. Es sind die dafür verwendeten Algorithmen anzugeben. Es ist anzugeben, welche bewährten Verfahrensweisen der Mechanismus zur CCK-Ableitung/CCK-Erstellung befolgt.

5.9.2.4.3 Konzeptuelle Beurteilung

5.9.2.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist es festzustellen, ob alle in [E.Doc.CCK-2] aufgeführten CCK-Erzeugungsmechanismen angemessen sind.

5.9.2.4.3.2 Voraussetzungen

Keine.

5.9.2.4.3.3 Beurteilungseinheiten

Es ist zu prüfen, ob alle von einem in [E.Doc.CCK-2] aufgeführten Mechanismus erzeugten CCKs bewährte Verfahrensweisen der Kryptographie befolgen; vergleiche die vorhergehende Anforderung und Anforderung CRY-.

5.9.2.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn die Beurteilungseinheiten erfolgreich validiert wurden.

— Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.9.2.4.4 Beurteilung der funktionalen Vollständigkeit

5.9.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist es festzustellen,

— ob alle CCK-Erzeugungsmechanismen auf dem Gerät in [E.Doc.CCK-2] aufgeführt sind und

— ob das Dokument [E.Doc.CCK-2] für jeden CCK-Erzeugungsmechanismus vollständige Informationen enthält, wie in CCK-1 gefordert.

5.9.2.4.4.2 Voraussetzungen

Keine.

5.9.2.4.4.3 Beurteilungseinheiten

a) Durch eine Konsistenzprüfung mit [E.Doc.CCK] ist zu prüfen, ob keine Nachweise für andere CCK-Erzeugungsmechanismen auf dem Gerät vorliegen.

b) Für jeden CCK-Erzeugungsmechanismus in [E.Doc.CCK-2] ist zu verifizieren, ob die vollständigen Informationen wie in CCK-1 gefordert bereitgestellt werden.

5.9.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn Beurteilungseinheit a) und Beurteilungseinheit b) erfolgreich validiert wurden.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.9.2.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.9.3 [CCK-3] Keine fest einprogrammierten vertraulichen kryptographischen Schlüssel

5.9.3.1 Anforderung

Vertrauliche kryptographische Schlüssel dürfen in der Software des Geräts nicht fest einprogrammiert sein.

5.9.3.2 Begründung

Fest einprogrammierte vertrauliche kryptographische Schlüssel, wie beispielsweise fest codierte Passwörter oder PINs, können leicht durch potentielle Angreifer entdeckt werden, beispielsweise mittels Firmware-Analyse. Darüber hinaus ermöglicht die Identifizierung eines fest einprogrammierten Parameters häufig skalierbare Angriffe auf verschiedene Geräte, die die gleichen Parameter verwenden.

5.9.3.3 Leitlinie

Das Hauptziel ist die Verhinderung der Implementation statischer Sicherheitszugangsdaten auf dem Gerät. Es sind andere Sicherheitskonzepte für individuelle und temporäre Zugangsdaten verfügbar.

5.9.3.4 Beurteilungskriterien

5.9.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung CCK-3.

5.9.3.4.2 Erforderliche Informationen

[E.Doc.CCK] Liste der vom Gerät verwendeten CCKs. Für jeden CCK in der Liste.

1. Angabe des Verwendungszwecks (Verschlüsselung, Integritätsschutz und Authentisierung).

2. Angabe des Algorithmus und der Algorithmenmodi, mit denen er verwendet wird.

3. Festlegung der Länge.

4. Bereitstellung von Informationen über die Entropie.

    4.1 Es sind Empfehlungen für bewährte Verfahrensweisen anzugeben, gefolgt von der gewählten Länge und Entropie.

    4.2 Falls keine bewährten Verfahrensweisen befolgt werden, ist zu erläutern, warum diese Länge und Entropie als für den Algorithmus und seinen Verwendungszweck angemessen gelten.

5. Seine Lebensdauer. Es ist zu präzisieren, ob der CCK eine begrenzte Lebensdauer oder eine begrenzte Anzahl von Nutzungen hat. Falls zutreffend, sind die Lebensdauer bzw. ist die zulässige Anzahl von Nutzungen anzugeben.

6. Wie auf den CCK zugegriffen wird

7. Ob der CCK auf dem Gerät erzeugt oder vor der Vermarktung vorinstalliert wird.

8. Das Verfahren, mit dem der CCK erzeugt wird bzw. wurde.

[E.Doc.CCK.preinstalled] Vollständige Dokumentation der vertraulichen kryptographischen Schlüssel, die auf dem Gerät vorinstalliert sind. Dies muss eine Untermenge von [E.Doc.CCK] sein. Für jeden vertraulichen kryptographischen Schlüssel sind die gleichen Informationen anzugeben wie für [E.Doc.CCKs]:

1. Angabe des Verwendungszwecks (Verschlüsselung, Integritätsschutz und Authentisierung).

2. Angabe des Algorithmus und der Algorithmenmodi, mit denen er verwendet wird.

3. Festlegung der Länge.

4. Bereitstellung von Informationen über die Entropie.

    4.1 Es sind Empfehlungen für bewährte Verfahrensweisen anzugeben, gefolgt von der gewählten Länge und Entropie.

    4.2 Falls keine bewährten Verfahrensweisen befolgt werden, ist zu erläutern, warum diese Länge und Entropie als für den Algorithmus und seinen Verwendungszweck angemessen gelten.

5. Seine Lebensdauer. Es ist zu präzisieren, ob der CCK eine begrenzte Lebensdauer oder eine begrenzte Anzahl von Nutzungen hat. Falls zutreffend, sind die Lebensdauer bzw. ist die zulässige Anzahl von Nutzungen anzugeben.

6. Wie auf den CCK zugegriffen wird

7. Ob der CCK auf dem Gerät erzeugt oder vor der Vermarktung vorinstalliert wird. (Anmerkung: In unserem Fall werden alle CCKs in [E.Doc.CCK.preinstalled] vor der Vermarktung vorinstalliert.)

8. Das Verfahren, mit dem der CCK erzeugt wird bzw. wurde.

Und zusätzlich

9. Das Verfahren, wie der CCK auf dem Gerät gespeichert wird.

[E.Doc.CCK.generated] Vollständige Dokumentation der vertraulichen kryptographischen Schlüssel, die durch einen Erzeugungsmechanismus für vertrauliche kryptographische Schlüssel erzeugt werden sollen. Dies muss eine Untermenge von [E.Doc.CCK] sein.

5.9.3.4.3 Konzeptueller Beurteilungsfall

5.9.3.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob keine vertraulichen kryptographischen Schlüssel in der Software des Geräts fest einprogrammiert sind.

5.9.3.4.3.2 Voraussetzungen

Keine.

5.9.3.4.3.3 Beurteilungseinheiten

Für jeden in [E.Doc.CCK.preinstalled] dokumentierten vertraulichen kryptographischen Schlüssel ist zu prüfen, ob er laut Dokumentation in der Software des Geräts fest einprogrammiert ist.

5.9.3.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— laut [E.Doc.CCK.preinstalled] KEINE vertraulichen kryptographischen Schlüssel in der Software des Geräts fest einprogrammiert sind; und

— kein Nachweis vorliegt, dass [E.Doc.CCK.preinstalled] unvollständig ist; und

— kein Nachweis vorliegt, dass [E.Doc.CCK.preinstalled] fehlerhaft bezüglich der Tatsache ist, ob ein vertraulicher kryptographischer Schlüssel in der Software des Geräts fest einprogrammiert ist.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.9.3.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.9.3.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.9.4 [CCK-4] Verhinderung von statischen Vorgabewerten für vertrauliche kryptographische Schlüssel

5.9.4.1 Anforderung

Vorinstallierte vertrauliche kryptographische Schlüssel zum Schutz des Zugangs zu Netzwerk- und/oder Sicherheitswerten müssen faktisch eindeutig für jedes Gerät sein, außer:

— das Gerät erzwingt ihre Erzeugung bei der ersten Verwendung, oder

— der betreffende kryptographische Schlüssel ist ein geteilter Parameter, der für den Betrieb des Geräts unabdingbar ist.

5.9.4.2 Begründung

Geräte können Verschlüsselung und damit CCKs zum Schutz der Werte auf dem Gerät (d. h. der Netzwerkressourcen) einsetzen. Die CCKs werden manchmal vordefiniert, z. B. während der Herstellung. CCKs, die für den oben genannten Zweck verwendet werden, müssen angemessen sein, um erfolgreiche, durch schwache CCKs verursachte Angriffe zu verhindern, besonders wenn sie vorinstalliert sind.

Wenn für vorinstallierte CCKs Vorgabewerte verwendet werden, wird durch die Erzwingung ihrer Festlegung bei der ersten Benutzung sichergestellt, dass die Risiken aufgrund der Verwendung von Vorgabewerten für vorinstallierte CCKs verringert werden.

5.9.4.3 Leitlinie

CCKs können bei der Herstellung auf dem Gerät vorinstalliert werden. Vorinstallierte, für jede Geräteinstanz eindeutige CCKs, die Brute-Force-Angriffen standhalten, können das mit der spezifischen Verwendung des CCK verbundene Cyber-Sicherheitsrisiko eindämmen. Ein Angreifer darf durch die Kenntnis des CCK eines Geräts nicht in der Lage sein, den entsprechenden CCK eines anderen Geräts abzuleiten – dies ist die Bedeutung von „faktisch eindeutig".

Die erforderliche Widerstandskraft des CCK gegenüber Angriffen hängt auch von der CCK-Lebensdauer ab. Beispielsweise müssen langfristige CCKs, die über lange Zeitspannen gespeichert und wiederholt während der gesamten Lebensdauer des Geräts genutzt werden, eine entsprechend stärkere Widerstandsfähigkeit gegen Angriffe aufweisen im Vergleich zu kurzfristigen CCKs, die üblicherweise auf dem Gerät erzeugt und nur für kurze Zeit genutzt werden.

Es entspricht bewährten Sicherheitspraktiken, einen CCK nur für einen einzigen Zweck zu nutzen, und wenn ein CCK auf einer Instanz des Geräts kompromittiert wird, dürfen die CCKs auf anderen Instanzen nicht gefährdet sein.

5.9.4.4 Beurteilungskriterien

5.9.4.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung CCK-4.

5.9.4.4.2 Erforderliche Informationen

[E.Doc.DT.CCK-4] Beschreibung des gewählten Pfads durch den in Bild 23 gezeigten Entscheidungsbaum für jeden vertraulichen kryptographischen Schlüssel.

[E.Just.DT.CCK-4] Begründung für den gewählten Pfad durch den in Bild 23 gezeigten Entscheidungsbaum für jeden vertraulichen kryptographischen Schlüssel.

[E.Doc.CCK.preinstalled] Vollständige Dokumentation der auf dem Gerät vorhandenen vertraulichen kryptographischen Schlüssel.

[E.Doc.CCK-3.generator] Dokumentation des Verfahrens, das zur Erzeugung der in [E.Doc.CCK.preinstalled] aufgeführten vertraulichen kryptographischen Schlüssel verwendet wurde.

Für jeden vertraulichen kryptographischen Schlüssel, dessen Erzeugung/Festlegung nicht bei der ersten Verwendung erzwungen wird: [E.Doc.CCK-3.generator] Dokumentation des Verfahrens, das zur Erzeugung des vertraulichen kryptographischen Schlüssels verwendet wurde.

5.9.4.4.3 Konzeptueller Beurteilungsfall

5.9.4.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die vorinstallierten vertraulichen kryptographischen Schlüssel ausreichend unabhängig voneinander sind.

5.9.4.4.3.2 Voraussetzungen

Keine.

5.9.4.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each confidential cryptographic key;
if (Is this CCK used for protecting\none or several network\nand/or security
   assets? ) then (Yes)
    if (Does the equipment enforce\nthe generation of this CCK on first use?
   ) then (Yes)
      #application :NOT APPLICABLE\ncondition for
   requirement's\napplicability not met for this CCK;
      detach;
    else (No)
      switch (Is this CCK practically unique per unit? )
      case ( \nYes)
        #lightgreen :PASS;
        detach;
      case ( \nNo)
       #pink :FAIL;
        detach;
      endswitch
    endif
else (No)
  #application :NOT APPLICAPLE\ncondition for requirement's\napplicability
   not met for this CCK;
  detach;
endif
@enduml
```

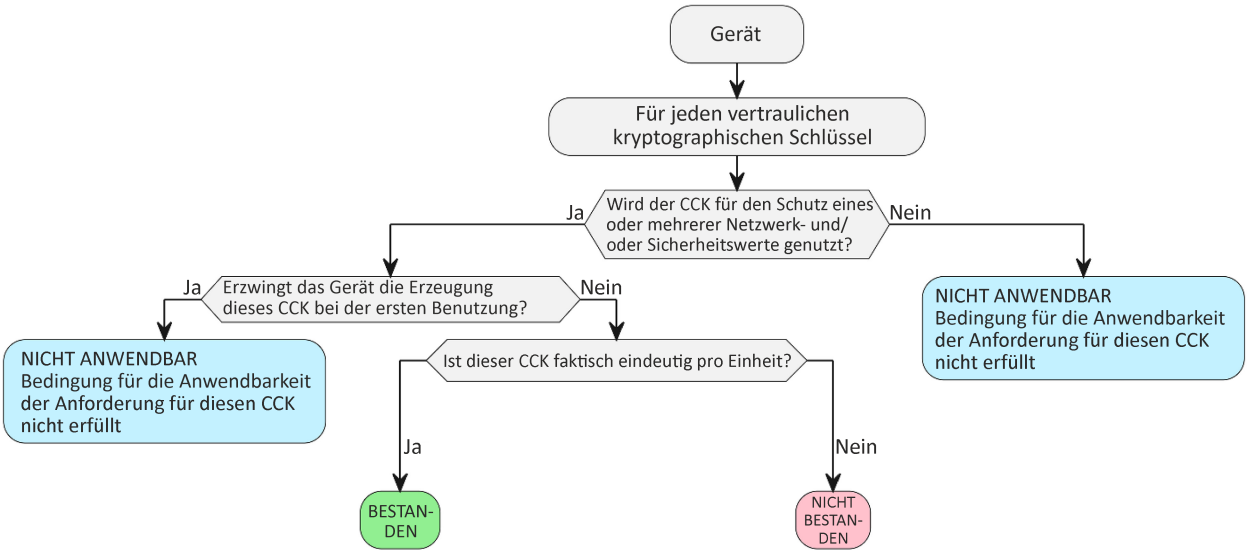

Bild 22 — Entscheidungsbaum für Anforderung CCK-4

Für jeden in [E.Doc.CCK.preinstalled] dokumentierten vertraulichen kryptographischen Schlüssel ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.CCK-4] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“endet.

Für jeden in [E.Doc.DT.CCK-4] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.CCK-4] dokumentierte Begründung zu untersuchen.

5.9.4.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.9.4.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.9.4.4.5 Beurteilung der funktionalen Suffizienz

5.9.4.4.5.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die vorinstallierten vertraulichen kryptographischen Schlüssel ausreichend unabhängig voneinander sind.

5.9.4.4.5.2 Voraussetzungen

Für diese Prüfung werden zwei Instanzen des Geräts benötigt. Beide befinden sich im Betriebszustand.

5.9.4.4.5.3 Beurteilungseinheiten

Für jeden in [E.Doc.CCK.preinstalled] dokumentierten vertraulichen kryptographischen Schlüssel ist funktional zu bestätigen, dass die entsprechenden CCKs der beiden Geräte faktisch eindeutig sind, d. h. dass sie nicht gleich sind und dass es kein offensichtliches Verfahren gibt, um den einen vom anderen abzuleiten. Diese funktionale Prüfung ist möglicherweise nicht immer durchführbar, da die Prüfperson üblicherweise keinen Zugriff auf die CCKs hat. Wenn die vertraulichen kryptographischen Schlüssel zusammen mit den damit verbundenen öffentlichen kryptographischen Schlüsseln bereitgestellt werden (z. B. als Paare von privaten/öffentlichen Schlüsseln), kann die Prüfperson zumindest die öffentlichen kryptographischen Schlüssel vergleichen und prüfen, ob sie sich zwischen den beiden Geräten unterscheiden.

5.9.4.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn kein Nachweis vorliegt, dass die vertraulichen kryptographischen Schlüssel nicht faktisch eindeutig sind.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn ein Nachweis vorliegt, dass die vertraulichen kryptographischen Schlüssel nicht faktisch eindeutig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT ANWENDBAR zugewiesen.

5.10 [GEC] Allgemeine Gerätefähigkeiten (en: General Equipment Capabilities)

5.10.1 [GEC-1] Aktuelle Software und Hardware ohne öffentlich bekannte ausnutzbare Schwachstellen

5.10.1.1 Anforderung

Das Gerät darf keine öffentlich bekannten ausnutzbaren Schwachstellen aufweisen, die, wenn sie ausgenutzt werden, Sicherheits- und Netzwerkwerte gefährden, außer:

— die öffentlich bekannte Schwachstelle kann unter den spezifischen Bedingungen des Geräts nicht ausgenutzt werden;

— die öffentlich bekannte ausnutzbare Schwachstelle wurde eingedämmt.

5.10.1.2 Begründung

Geräte können aus Hardware und Software bestehen, die von vielen Lieferanten stammen, und der Hersteller hat möglicherweise keine Einsicht in die Sicherheitspraktiken dieser Lieferanten, was ein Risiko für den Hersteller darstellt.

Das Management der Sicherheitsrisiken von Hardware- und Software-Lieferketten geht über den Anwendungsbereich dieses Dokuments hinaus, aber um diese Anforderung zu erfüllen, ist es wichtig, dass der Hersteller öffentlich bekannte ausnutzbare Schwachstellen in der auf den Geräten eingesetzten Dritthersteller-Hardware und -Software identifizieren kann, sowohl bei kommerzieller als auch bei Open-Source-Software, und dass er mit diesen Schwachstellen umgehen kann.

Durch den Einsatz von sichererer Hardware und Software wird das durch die Angriffsflächen verursachte Risiko reduziert.

5.10.1.3 Leitlinie

Um die Überwachung von Software-Schwachstellen zu erleichtern, erstellt der Gerätehersteller eine technische Dokumentation der Gerätesoftware, und zwar sowohl für die Open-Source-Software als auch für die kommerziellen Standardkomponenten. Gleichermaßen kann die technische Hardware-Dokumentation die Identifikation von Hardware-Schwachstellen unterstützen.

Um die öffentlich bekannten ausnutzbaren Schwachstellen der Gerätehardware und -software zu identifizieren, zieht der Hersteller die NVD-Schwachstellendatenbank zu Rate.

Zu den unterschiedlichen Faktoren, die der Hersteller bei der Beurteilung der öffentlich bekannten ausnutzbaren Schwachstellen berücksichtigt, gehören unter anderem:

— die Angriffsfläche des Geräts und die Vektoren/Pfade, über die sich der Angreifer Zugang zum Gerät verschaffen kann, um die Schwachstelle auszunutzen;

— der Nachweis, dass die Schwachstelle aktiv ausgenutzt wurde oder dass es für sie bereits dokumentierte Machbarkeitsnachweise oder Code-Ausnutzungen gibt;

— die im Gerät implementierten Sicherheitsfähigkeiten und Mechanismen, die die Ausnutzung der Schwachstelle eindämmen können;

— die „bestimmungsgemäße Verwendung des Geräts“;

— die „für die Nutzung“ des Geräts vorgesehene Betriebsumgebung“, einschließlich Bedrohungsumfeld, Sicherheitsfähigkeiten und zusätzlicher, durch die Umgebung bereitgestellter Gegenmaßnahmen, die die Ausnutzung der Schwachstelle eindämmen oder beheben können.

5.10.1.4 Beurteilungskriterien

5.10.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-1.

5.10.1.4.2 Erforderliche Informationen

[eDoc.SoftwareDocumentation] Beschreibung der Gerätesoftware, einschließlich ihrer Versionen, soweit es die Sicherheitswerte und Netzwerkwerte betrifft.

[eDoc.HardwareDocumentation] Beschreibung der Gerätehardware, soweit es die Sicherheitswerte und Netzwerkwerte betrifft.

[E.Doc.ListOfVulnerabilities] Dokumentierte Liste aller öffentlich bekannten, ausnutzbaren Hardware- oder Software-Schwachstellen des geprüften Geräts. Das Dokument beinhaltet auch die Begründung des Herstellers zur Behebung, Eindämmung und Nicht-Ausnutzung der aufgeführten, öffentlich bekannten ausnutzbaren Schwachstellen der Hardware oder Software.

5.10.1.4.3 Konzeptuelle Beurteilung

5.10.1.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die in der Hardware und Software der geprüften Geräte vorhandenen, öffentlich bekannten Hardware- und Software-Schwachstellen bei Werksvoreinstellung eingedämmt oder behoben wurden bzw. ob sie nicht ausnutzbar sind.

5.10.1.4.3.2 Voraussetzungen

Keine.

5.10.1.4.3.3 Beurteilungseinheiten

Für die gesamte, in [eDoc.SoftwareDocumentation] und [eDoc.HardwareDocumentation] dokumentierte Hardware und Software ist die Vollständigkeit der Liste öffentlich bekannter ausnutzbarer Schwachstellen in [E.Doc.ListOfVulnerabilities] zu beurteilen.

5.10.1.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn das Dokument [E.Doc.ListOfVulnerabilities] alle öffentlich bekannten ausnutzbaren Schwachstellen aufführt und einen Status dazu nennt (d. h. eingedämmt, behoben oder nicht ausnutzbar) (Vollständigkeit der Liste öffentlich bekannter ausnutzbarer Schwachstellen).

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.1.4.4 Beurteilung der funktionalen Vollständigkeit

5.10.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung des geprüften Geräts, um die Vollständigkeit der Dokumentation in Bezug darauf zu verifizieren, ob nur die in [E.Doc.ListOfVulnerabilities] aufgeführten Schwachstellen vorhanden sind, und ob deren Ausnutzung, die Auswirkungen ihrer Ausnutzung oder beides wie dokumentiert behoben oder eingedämmt wurden oder dass sie nicht ausgenutzt werden.

5.10.1.4.4.2 Voraussetzungen

Das Gerät muss in Betrieb und im Werksvoreinstellungszustand sein.

Die Quelle, die für die Liste öffentlich bekannter, für die Beurteilung verwendeter ausnutzbarer Schwachstellen herangezogen wird, muss aktuell sein.

5.10.1.4.4.3 Beurteilungseinheiten

Beurteilung der Herstellerbegründung (d. h. behoben, eingedämmt oder nicht ausnutzbar) für jede öffentlich bekannte ausnutzbare Schwachstelle in [E.Doc.ListOfVulnerabilities].

a) Es ist funktional zu beurteilen, ob das geprüfte Gerät andere öffentlich bekannte ausnutzbare Schwachstellen aufweist, die nicht in [E.Doc.ListOfVulnerabilities] aufgeführt sind.

b) Für alle öffentlich bekannten ausnutzbaren Schwachstellen in [E.Doc.ListOfVulnerabilities] ist die Herstellerbegründung für deren Eindämmung, Behebung oder Nicht-Ausnutzbarkeit funktional zu beurteilen.

c) Für alle öffentlich bekannten ausnutzbaren Schwachstellen in [E.Doc.ListOfVulnerabilities] kann in der Beurteilung Punkt b) durch eine Geräteprüfung ergänzt werden, die bei einer öffentlich bekannten Ausnutzungsbedingung (d. h. einem ausnutzbaren Code in Verbindung mit einem CVE) durchgeführt wird.

5.10.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— alle öffentlich bekannten Schwachstellen in [E.Doc.ListOfVulnerabilities] dokumentiert sind; und

— für keine der in [E.Doc.ListOfVulnerabilities] aufgeführten öffentlich bekannten Schwachstellen ein Nachweis vorliegt, dass sie ausgenutzt werden kann, während das geprüfte Gerät verwendet und unter den dokumentierten Bedingungen betrieben wird.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.1.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.10.2 [GEC-2] Begrenzung der Offenlegung von Diensten über entsprechende Netzwerkschnittstellen

5.10.2.1 Anforderung

In der Werksvoreinstellung darf das Gerät Netzwerkschnittstellen oder Dienste über Netzwerkschnittstellen, von denen Sicherheits- oder Netzwerkwerte betroffen sind, nur dann offenlegen, wenn dies für die Einrichtung oder den grundlegenden Betrieb des Geräts in der für die Nutzung vorgesehenen Betriebsumgebung erforderlich ist.

5.10.2.2 Begründung

Zugängliche Dienste sind ein wichtiger Faktor zur Reduzierung des möglichen Risikos einer Kompromittierung von Geräten, beispielsweise um das Netzwerk zu schädigen. Daher müssen die zugänglichen Dienste auf solche beschränkt werden, die für die Einrichtung des Geräts und für dessen Betrieb in der für die Nutzung vorgesehenen Betriebsumgebung erforderlich sind.

5.10.2.3 Leitlinie

Die Gerätekonfiguration kann sich unterscheiden, abhängig davon, wie das Gerät hergestellt wird.

Allgemein muss zwischen zwei Gerätearten unterschieden werden:

— Mehrzweckgeräte (z. B. Smartphones, Laptops): Die von Mehrzweckgeräten bereitgestellten Dienste und deren Funktionalität sind nur bis zur Auslieferung unter Kontrolle des Herstellers. Die aktivierten (und dokumentierten) Netzwerkdienste können nur vor Auslieferung des Geräts beeinflusst werden.

— Geräte mit einer kontrollierten, festgelegten Funktionalität (z. B. Sensoren, Router): Die bereitgestellten Dienste und die Gerätefunktionalität sind in eine gerätespezifische Software (Firmware) eingebettet, die vom Hersteller bereitgestellt wird. Die aktivierten (und dokumentierten) Netzwerkdienste können während des Lebenszyklus des Geräts beeinflusst werden.

5.10.2.4 Beurteilungskriterien

5.10.2.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-2.

5.10.2.4.2 Erforderliche Informationen

[E.Doc.NetworkInterfaces.exposure] Dokumentation der Netzwerkschnittstellen und der in Werksvoreinstellung des Geräts über Netzwerkschnittstellen zugänglichen Dienste. Diese Dokumentation enthält Informationen und Beschreibungen aller Netzwerkschnittstellen bzw. über Netzwerkschnittstellen zugänglichen Dienste, und ob diese für den grundlegenden Betrieb oder die Einrichtung des Geräts benötigt werden oder ob sie optional sind.

[E.Doc.SecurityAsset.GEC-2] Dokumentation jedes Sicherheitswerts, der über Netzwerkschnittstellen zugänglich ist.

[E.Doc.NetworkAsset.GEC-2] Dokumentation jedes Netzwerkwerts, der über Netzwerkschnittstellen zugänglich ist.

[E.Just.NetworkInterfaces.exposureRisk] Dokumentierte Analyse, Begründung und Entscheidung für die in [E.Doc.SecurityAsset.GEC-2] dokumentierten Sicherheitswerte und die in [E.Doc.NetworkAsset.GEC-2] dokumentierten Netzwerkwerte in Bezug auf die Offenlegung von Netzwerkschnittstellen bzw. Diensten über Netzwerkschnittstellen bei Werksvoreinstellung.

Wenn für das Gerät ein Einrichtungsprozess implementiert ist

[E.Doc.setup] Dokumentation, wie das Gerät einzurichten ist.

5.10.2.4.3 Konzeptuelle Beurteilung

5.10.2.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Offenlegungen von Netzwerkschnittstellen oder von Diensten über Netzwerkschnittstellen bei Werksvoreinstellung auf solche beschränkt wurden, die für die Einrichtung oder den grundlegenden Betrieb des Geräts erforderlich sind, und ob das Risiko in Bezug auf Sicherheits- und Netzwerkwerte für jede Netzwerkschnittstelle und jeden Dienst, der über eine Netzwerkschnittstelle zugänglich ist, begründet wurde.

5.10.2.4.3.2 Voraussetzungen

Keine.

5.10.2.4.3.3 Beurteilungseinheiten

— Beurteilung auf Grundlage von [E.Just.NetworkInterfaces.exposureRisk] für alle Netzwerkschnittstellen und über Netzwerkschnittstellen zugänglichen Dienste in [E.Doc.NetworkInterfaces.exposure], ob das damit verbundene Risiko in Bezug auf Sicherheits- und Netzwerkwerte begründet wurde.

— Beurteilung auf Grundlage von [E.Doc.NetworkInterfaces.exposure], ob die Offenlegung von Netzwerkschnittstellen und von Diensten über Netzwerkschnittstellen auf solche begrenzt ist, die für die Einrichtung wie in [E.Doc.Setup] beschrieben oder für den grundlegenden Betrieb des Geräts erforderlich sind.

5.10.2.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn für jede Netzwerkschnittstelle und jeden über eine Netzwerkschnittstelle zugänglichen Dienst des Geräts gilt:

— das damit verbundene, in [E.Just.NetworkInterfaces.exposureRisk] beschriebene Risiko in Bezug auf die Sicherheits- und Netzwerkwerte wurde begründet;

— die in [E.Doc.NetworkInterfaces.exposure] beschriebene Offenlegung ist auf Netzwerkschnittstellen und über Netzwerkschnittstellen zugängliche Dienste beschränkt, die für die Einrichtung oder für den grundlegenden Betrieb des Geräts erforderlich sind.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.2.4.4 Beurteilung der funktionalen Vollständigkeit

5.10.2.4.4.1 Zweck der Beurteilung

Der Zweck dieses Prüffalls ist die funktionale Beurteilung, um sicherzustellen, dass bei Werksvoreinstellung nur solche Netzwerkschnittstellen oder über Netzwerkschnittstellen zugängliche Dienste offengelegt sind, die für die Einrichtung oder den grundlegenden Betrieb des Geräts in der für die Nutzung vorgesehenen Betriebsumgebung erforderlich sind, und zwar in Bezug auf die Vollständigkeit der Dokumentation und die korrekte Implementation.

5.10.2.4.4.2 Voraussetzungen

Das Gerät muss mit Werksvoreinstellung in Betrieb sein, und es hat, falls verfügbar, bisher keine Einrichtung oder sonstige Konfiguration stattgefunden.

Eine Netzwerkverbindung zur Prüfung der über Netzwerkschnittstellen offengelegten Dienste ist eingerichtet.

5.10.2.4.4.3 Beurteilungseinheiten

— Funktionale Beurteilung, ob bei Werksvoreinstellung weitere Netzwerkschnittstellen oder über Netzwerkschnittstellen zugängliche Dienste vorhanden sind, die nicht in [E.Doc.NetworkInterfaces.exposure] aufgeführt sind, oder die nicht für die Einrichtung nach [E.Doc.Setup] oder für den grundlegenden Betrieb des Geräts erforderlich sind.

— Es ist eine Suche durchzuführen, um alle durch das Gerät offengelegten Netzwerkschnittstellen oder Dienste bei Werksvoreinstellung aufzudecken, selbst wenn die entsprechenden Netzwerkschnittstellen oder Dienste nicht aktiviert und nicht in [E.Doc.NetworkInterfaces.exposure] dokumentiert sind.

5.10.2.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— alle erkannten Netzwerkschnittstellen oder bei Werksvoreinstellung über Netzwerkschnittstellen zugänglichen Dienste dokumentiert sind; und

— für alle Netzwerkschnittstellen oder bei Werksvoreinstellung über Netzwerkschnittstellen zugänglichen Dienste nachgewiesen ist, dass diese für die Einrichtung des Geräts oder für den grundlegenden Betrieb nach [E.Doc.Setup] und [E.Doc.NetworkInterfaces.exposure] erforderlich sind. Es liegt kein Nachweis vor, dass die Implementation der Netzwerkschnittstellen oder der über Netzwerkschnittstellen zugänglichen Dienste von der Dokumentation abweicht.

Die Entscheidung NICHT ANWENDBAR wird zugewiesen, wenn

— bei Werksvoreinstellung des Geräts keine physische Verbindung über Netzwerkschnittstellen verfügbar ist.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.2.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.10.3 [GEC-3] Konfiguration von optionalen Diensten und zugehörigen offengelegten Netzwerkschnittstellen

5.10.3.1 Anforderung

Bei optionalen Netzwerkschnittstellen oder über Netzwerkwerkschnittstellen zugänglichen Diensten, von denen Sicherheits- oder Netzwerkwerte betroffen sind und die Teil der Werksvoreinstellung des Geräts sind, muss es für einen autorisierten Benutzer möglich sein, den Dienst zu aktivieren und zu deaktivieren.

5.10.3.2 Begründung

Dies reduziert die Angriffsfläche in Bezug auf Netzwerkschnittstellen und darüber zugängliche Dienste.

5.10.3.3 Leitlinie

Das Gerät verfügt über die Funktionalität zur Konfiguration (Aktivierung/Deaktivierung) der optionalen Dienste und der zugehörigen offengelegten Netzwerkschnittstellen.

Die Konfiguration netzwerkbezogener Dienste sollte entsprechend Zugangssteuerungsmechanismus (ACM) und Authentisierungsmechanismus (AUM) geschützt sein.

5.10.3.4 Beurteilungskriterien

5.10.3.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-3.

5.10.3.4.2 Erforderliche Informationen

[E.Doc.NetworkInterfaces.exposure] Dokumentation der Netzwerkschnittstellen und der über Netzwerkschnittstellen zugänglichen Dienste, die Teil der Werksvoreinstellung sind. Diese Dokumentation muss zu allen Netzwerkschnittstellen oder über Netzwerkschnittstellen zugänglichen Dienste die Information enthalten, ob diese für den grundlegenden Betrieb oder die Einrichtung des Geräts benötigt werden, oder ob sie optional sind.

[E.Doc.configuration] Konfigurationsanweisungen.

[E.Doc.SecurityAsset.GEC-3] Dokumentation aller Sicherheitswerte, die über Netzwerkschnittstellen zugänglich sind.

[E.Doc.NetworkAsset.GEC-3] Dokumentation aller Netzwerkwerte, die über Netzwerkschnittstellen zugänglich sind.

[E.Just.NetworkInterfaces.exposureRisk] Dokumentierte Analyse, Begründung und Entscheidung bezüglich des Risikos für die in [E.Doc.SecurityAsset.GEC-3] dokumentierten Sicherheitswerte und die in [E.Doc.NetworkAsset.GEC-3] dokumentierten Netzwerkwerte bei der Offenlegung von Netzwerkschnittstellen und Diensten über Netzwerkschnittstellen, die Teil der Werksvoreinstellung sind.

5.10.3.4.3 Konzeptuelle Beurteilung

5.10.3.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle optionalen, über Netzwerkschnittstellen zugänglichen Dienste, die Teil der Werksvoreinstellung des Geräts sind, konfigurierbar sind, mindestens mit der Option, den Dienst zu aktivieren und zu deaktivieren.

5.10.3.4.3.2 Voraussetzungen

Keine.

5.10.3.4.3.3 Beurteilungseinheiten

— Beurteilung auf Grundlage von [E.Just.NetworkInterfaces.exposureRisk] für alle über das Netzwerk zugänglichen Dienste in [E.Doc.NetworkInterfaces.exposure], ob das damit verbundene Risiko in Bezug auf Sicherheits- und Netzwerkwerte begründet wurde.

— Beurteilung auf Grundlage von [E.Doc.NetworkInterfaces.exposure] und von [E.Doc.configuration], ob die als Teil der Werksvoreinstellung offengelegten optionalen Netzwerkschnittstellen und die über Netzwerkschnittstellen zugänglichen optionalen Dienste mit mindestens der Option zur Aktivierung und Deaktivierung der optionalen Netzwerkschnittstelle oder der über die Netzwerkschnittstellen zugänglichen Dienste konfigurierbar sind.

5.10.3.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn für jede Netzwerkschnittstelle und jeden über eine Netzwerkschnittstelle zugänglichen Dienst des Geräts gilt:

— die Konfiguration, zumindest die Option zur Aktivierung und Deaktivierung der Netzwerkschnittstellen oder der über Netzwerkschnittstellen zugänglichen Dienste, die Teil der Werksvoreinstellung sind und die in [E.Doc.configuration] und in [E.Doc.NetworkInterfaces.exposure] beschrieben sind, ist für alle optionalen Netzwerkschnittstellen und alle über Netzwerkschnittstellen zugänglichen Dienste möglich;

— in [E.Doc.NetworkInterfaces.exposure] ist keine optionale dokumentierte Offenlegung von Diensten in Bezug auf das Netzwerk vorhanden.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.3.4.4 Beurteilung der funktionalen Vollständigkeit

5.10.3.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Validierung, um nachzuweisen, dass alle optionalen Netzwerkschnittstellen und über das Netzwerk zugänglichen optionalen Dienste, die Teil der Werksvoreinstellung sind, mindestens mit der Option konfigurierbar sind, den Dienst zu aktivieren und zu deaktivieren. Hierfür muss die Vollständigkeit der Dokumentation und die korrekte Implementation untersucht werden.

5.10.3.4.4.2 Voraussetzungen

Das Gerät ist in Betrieb und die Einrichtung, falls verfügbar, ist abgeschlossen.

Eine physische Netzwerkverbindung zur Prüfung der Offenlegung von Diensten über Netzwerkschnittstellen ist eingerichtet.

5.10.3.4.4.3 Beurteilungseinheiten

— Funktionale Beurteilung, ob optionale Netzwerkschnittstellen oder über Netzwerkschnittstellen zugängliche Dienste vorhanden sind, die nicht in [E.Doc.NetworkInterfaces.exposure] oder [E.Doc.configuration] aufgeführt sind oder die nicht aktiviert sind.

— Es ist eine Suche durchzuführen, um alle durch das Gerät offengelegten Netzwerkschnittstellen oder über Netzwerkschnittstellen zugänglichen Dienste aufzudecken, selbst wenn die entsprechenden Dienste nicht aktiviert sind oder nicht in [E.Doc.NetworkInterfaces.exposure] dokumentiert sind.

5.10.3.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— alle erkannten, über das Netzwerk zugänglichen Schnittstellen oder Dienste dokumentiert sind; und

— für alle Netzwerkschnittstellen oder über Netzwerkschnittstellen zugänglichen optionalen Dienste nachgewiesen ist, dass sie konfigurierbar sind, zumindest mit der Option zur Aktivierung und Deaktivierung;

— es liegt kein Nachweis vor, dass die Implementation der optionalen Netzwerkschnittstellen und der über Netzwerkschnittstellen zugänglichen optionalen Dienste von der Dokumentation abweicht.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.3.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.10.4 [GEC-4] Dokumentation von über Netzwerkschnittstellen zugänglichen Diensten

5.10.4.1 Anforderung

Die Benutzerdokumentation des Geräts muss eine Beschreibung aller Dienste enthalten, die über Netzwerkschnittstellen zugänglich sind und die als Teil der Werksvoreinstellung bereitgestellt werden.

5.10.4.2 Begründung

Das Gerät selbst und das umgebende Netzwerk müssen ordnungsgemäß konfiguriert sein, um die Funktionalität des Geräts sicherzustellen und die Netzwerksicherheit zu unterstützen. Daher ist es wichtig, Benutzerinformationen zu den zugänglichen Netzwerkdiensten bereitzustellen.

5.10.4.3 Leitlinie

Alle Dienste, die über Netzwerkschnittstellen zugänglich sind, müssen in der Dokumentation aufgeführt sein. Zusätzlich zur Liste der Dienste könnte in der Beschreibung der Dienste der Zweck für jeden Dienst dokumentiert sein.

Der Einfluss des Herstellers auf die Konfiguration kann variieren.

Allgemein muss zwischen zwei Gerätearten unterschieden werden:

— Mehrzweckgeräte (z. B. Smartphones, Laptops): Die von Mehrzweckgeräten bereitgestellten Dienste und deren Funktionalität sind nur bis zur Auslieferung unter Kontrolle des Herstellers. Die aktivierten und dokumentierten Netzwerkdienste können nur vor der Auslieferung des Geräts beeinflusst werden. Dienste, die von Allzweckbetriebssystemen wie beispielsweise Windows oder Android bereitgestellt werden, könnten ausgeschlossen werden, sofern sie nicht der Kontrolle des Herstellers unterliegen.

— Geräte mit einer kontrollierten, festgelegten Funktionalität (z. B. Sensoren, Router): Die bereitgestellten Dienste und die Gerätefunktionalität sind in eine gerätespezifische Software (Firmware) eingebettet, die vom Hersteller bereitgestellt wird. Die aktivierten und dokumentierten Netzwerkdienste können während des Lebenszyklus des Geräts beeinflusst werden.

5.10.4.4 Beurteilungskriterien

5.10.4.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-4.

5.10.4.4.2 Erforderliche Informationen

[E.Doc.UserDoc.NetworkInterfaces.exposure] Benutzerdokumentation der Netzwerkschnittstellen und der bei Werksvoreinstellung des Geräts über Netzwerkschnittstellen zugänglichen Dienste. Diese Dokumentation muss Informationen und Beschreibungen aller Netzwerkschnittstellen oder über Netzwerkschnittstellen zugänglichen Dienste enthalten und angeben, ob diese für den grundlegenden Betrieb oder die Einrichtung des Geräts benötigt werden oder ob sie optional sind.

5.10.4.4.3 Konzeptuelle Beurteilung

5.10.4.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob alle Dienste, die über Netzwerkschnittstellen zugänglich sind und die als Teil der Werksvoreinstellung bereitgestellt werden, in der Benutzerdokumentation beschrieben sind.

5.10.4.4.3.2 Voraussetzungen

Keine.

5.10.4.4.3.3 Beurteilungseinheiten

— Beurteilung auf Grundlage von [E.Doc.UserDoc.NetworkInterfaces.exposure] für alle vom Netzwerk zugänglichen Dienste, ob sie in der Benutzerdokumentation beschrieben sind, und ob angegeben ist, ob die Dienste für die Einrichtung oder für den Betrieb des Geräts in der für die Nutzung vorgesehenen Betriebsumgebung erforderlich sind, oder ob es optionale Dienste sind.

5.10.4.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird für jeden über das Netzwerk zugänglichen Dienst des Geräts zugewiesen, wenn:

— eine Beschreibung in der Benutzerdokumentation vorhanden ist und auch angegeben ist, ob der Dienst für die Einrichtung oder für den Betrieb des Geräts in der für die Nutzung vorgesehenen Betriebsumgebung erforderlich ist oder ob es sich um einen optionalen Dienst handelt;

— die Beschreibung in der Benutzerdokumentation steht nicht im Widerspruch zu der in [E.Doc.UserDoc.NetworkInterfaces.exposure] bereitgestellten Information.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.4.4.4 Beurteilung der funktionalen Vollständigkeit

Keine.

5.10.4.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.10.5 [GEC-5] Keine unnötigen externen Schnittstellen

5.10.5.1 Anforderung

Das Gerät darf nur externe Schnittstellen bereitstellen, die nötig sind für:

— die „bestimmungsgemäße Verwendung des Geräts“; und

— die „für die Nutzung vorgesehene Betriebsumgebung“.

5.10.5.2 Begründung

Externe Kommunikationsschnittstellen müssen so gering wie möglich gehalten werden, um die mögliche Angriffsfläche zu minimieren.

5.10.5.3 Leitlinie

Falls eine unnötige externe Schnittstelle physisch durch die für die Nutzung vorgesehene Betriebsumgebung geschützt wird und nicht angegriffen werden kann, dann gilt diese als nicht vom Gerät bereitgestellt. Deaktivierte oder blockierte Schnittstellen gelten als nicht vom Gerät bereitgestellt.

Externe Geräteschnittstellen können Schnittstellen einschließen, die bestimmungsgemäß für die interne Systemkommunikation verwendet werden.

5.10.5.4 Beurteilungskriterien

5.10.5.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-5.

5.10.5.4.2 Erforderliche Informationen

Wenn für das Gerät ein Einrichtungsprozess implementiert ist:

— [E.Doc.setup] vollständige Dokumentation für die Einrichtung des Geräts.

Wenn externe, nicht netzwerkbezogene Schnittstellen verfügbar sind:

— [E.Doc.NonNetworkInterfaces] Dokumentation der externen, nicht netzwerkbezogenen Schnittstellen.

— [E.Doc.SecurityAsset.GEC-5] Dokumentation aller Sicherheitswerte, die über nicht netzwerkbezogene Schnittstellen zugänglich sind.

— [E.Doc.NetworkAsset.GEC-5] Dokumentation aller Netzwerkwerte, die über nicht netzwerkbezogene Schnittstellen zugänglich sind.

— [E.Just.NonNetworkInterfaces.exposureRisk] Dokumentierte Analyse, Begründung und Entscheidung bezüglich des Risikos für die in [E.Doc.SecurityAsset.GEC-3] dokumentierten Sicherheitswerte und die in [E.Doc.NetworkAsset.GEC-3] dokumentierten Netzwerkwerte in Bezug auf die Offenlegung über nicht netzwerkbezogene Schnittstellen.

5.10.5.4.3 Konzeptuelle Beurteilung

5.10.5.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob bei Werksvoreinstellung des Geräts die Offenlegung von Netzwerkschnittstellen auf solche beschränkt ist, die für die Einrichtung oder für die bestimmungsgemäße Nutzung in der vorgesehenen Betriebsumgebung erforderlich sind.

5.10.5.4.3.2 Voraussetzungen

Keine.

5.10.5.4.3.3 Beurteilungseinheiten

Auf Grundlage von [E.Just.NonNetworkInterfaces.exposureRisk] ist für jede nicht netzwerkbezogene, extern zugängliche Schnittstelle in [E.Doc.NonNetworkInterfaces] zu prüfen, ob die Schnittstelle für die in [E.Doc.setup] beschriebene Einrichtung des Geräts erforderlich ist oder ob sie erforderlich ist, um das Gerät bestimmungsgemäß und in der für die Nutzung vorgesehenen Betriebsumgebung zu betreiben, und auch, ob das damit verbundene Risiko in Bezug auf die Sicherheits- und Netzwerkwerte begründet wurde.

5.10.5.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird für jede nicht netzwerkbezogene Schnittstelle des Geräts zugewiesen, wenn:

— die Offenlegung der in [E.Doc.NonNetworkInterfaces] aufgeführten externen Kommunikationsschnittstellen auf nicht netzwerkbezogene externe Schnittstellen begrenzt ist, die für die in [E.Doc.setup] beschriebene Einrichtung oder für den bestimmungsgemäßen Betrieb des Geräts in der für die Nutzung vorgesehenen Betriebsumgebung erforderlich sind;

— das damit verbundene, in [E.Just.NonNetworkInterfaces.exposureRisk] beschriebene Risiko wurde in Bezug auf die Sicherheits- und Netzwerkwerte und unter Berücksichtigung der bestimmungsgemäßen Nutzung und der für die Nutzung vorgesehenen Betriebsumgebung begründet.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— keine nicht netzwerkbezogenen externen Schnittstellen am Gerät vorhanden sind.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.5.4.4 Beurteilung der funktionalen Vollständigkeit

5.10.5.4.4.1 Zweck der Beurteilung

Der Zweck dieses Prüffalls ist die funktionale Beurteilung, um sicherzustellen, dass nur solche externen Schnittstellen offengelegt sind, die für die Einrichtung oder den bestimmungsgemäßen Betrieb des Geräts in der für die Nutzung vorgesehenen Betriebsumgebung erforderlich sind, und zwar in Bezug auf die Vollständigkeit der Dokumentation und die korrekte Implementation.

5.10.5.4.4.2 Voraussetzungen

Das Gerät befindet sich in Werksvoreinstellung und, falls vorhanden, hat die Einrichtung und Konfiguration bereits stattgefunden.

5.10.5.4.4.3 Beurteilungseinheiten

— Funktionale Beurteilung, ob weitere, nicht netzwerkbezogene externe Schnittstellen offengelegt sind, die nicht in [E.Doc.NonNetworkInterfaces] aufgeführt sind, oder die nicht für die Einrichtung nach

[E.Doc.Setup] oder für den bestimmungsgemäßen Betrieb des Geräts in der für die Nutzung vorgesehenen Betriebsumgebung erforderlich sind.

— Es ist eine Suche durchzuführen, um alle durch das Gerät offengelegten, nicht netzwerkbezogenen externen Schnittstellen aufzudecken, selbst wenn die entsprechende Funktion nicht aktiviert oder in [E.Doc.NonNetworkInterfaces] dokumentiert ist.

5.10.5.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn:

— alle zugänglichen, nicht netzwerkbezogenen externen Schnittstellen dokumentiert sind; und

— für alle nicht netzwerkbezogenen externen Schnittstellen nachgewiesen ist, dass sie für die Einrichtung nach [E.Doc.Setup] oder für den bestimmungsgemäßen Betrieb des Geräts in der für die Nutzung vorgesehenen Betriebsumgebung erforderlich sind;

— wenn nicht netzwerkbezogene Schnittstellen erkannt wurden, die für die Einrichtung nach [E.Doc.Setup] oder zum bestimmungsgemäßen Betrieb des Geräts in der für die Nutzung vorgesehenen Betriebsumgebung nicht erforderlich sind, wird in der entsprechenden Risikobeschreibung in [E.Just.NonNetworkInterfaces.exposureRisk] das damit verbundene Risiko in Bezug auf die Sicherheits- und Netzwerkwerte beschrieben und begründet, warum die Schnittstelle dennoch zugänglich ist;

— es liegt kein Nachweis vor, dass die Implementation von externen, nicht netzwerkbezogenen Schnittstellen von der Dokumentation abweicht.

Die Entscheidung NICHT ANWENDBAR wird zugewiesen, wenn

— keine nicht netzwerkbezogenen externen Schnittstellen am Gerät vorhanden sind.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.5.4.5 Beurteilung der funktionalen Suffizienz

Keine.

5.10.6 [GEC-7] Eingabevalidierung

5.10.6.1 Anforderung

Das Gerät muss eine Funktion zur Validierung von Eingaben über externe Schnittstellen nutzen, um die Verfälschung, die Extraktion oder den Missbrauch von Sicherheitswerten und Netzwerkwerten und den Verlust von Funktionalität zu verhindern.

5.10.6.2 Begründung

Die Eingabevalidierung ist notwendig, um zu validieren, dass alle Eingaben am Gerät den erwarteten Eingaben entsprechen und die Eigenschaften aufweisen, die für die korrekte Bearbeitung der Daten erforderlich sind.

Die unzureichende Eingabevalidierung wird als einer der häufigsten und gefährlichsten Software-Schwachpunkte angesehen, der auch zu einigen anderen Softwareschwächen beiträgt, wie beispielsweise zu Schreibvorgängen außerhalb des zulässigen Bereichs und zu einer unzureichenden Neutralisierung; dies kann zu verschiedenen Injection-Schwachstellen führen (z. B. SQL-Injection, OS-Command-Injection und Path Traversal).

Besonders Daten aus potentiell nicht vertrauenswürdigen Quellen, wie beispielsweise alle über Netzwerkschnittstellen empfangenen Eingaben, müssen einer Eingabevalidierung unterzogen werden, bei der die Eingaben sowohl bezüglich Syntax als auch bezüglich korrekter Semantik geprüft werden. Diese Prüfungen sollten so

früh wie möglich bei der Verarbeitung von Eingaben durchgeführt werden, um die Verbreitung von ungültigen und möglicherweise sogar böswilligen Eingaben zu verhindern. Die erforderliche Strenge hängt ab von:

— den Risiken für die Werte; und

— den Syntax- und Semantikprüfungen für den Eingabedatentyp; und

— der Vertrauenswürdigkeit der Quelle, aus der die Eingabe stammt.

5.10.6.3 Leitlinie

Eine unzureichende Eingabevalidierung ist eine der Hauptursachen für viele Sicherheitsschwachstellen; die Eingabe kann nur erfolgreich verarbeitet werden, wenn durch syntaktische und semantische Prüfung sowohl der Rohdaten als auch der Metadaten festgestellt wurde, dass die Eingabe gültig ist.

Bei der Syntaxvalidierung wird geprüft, ob die Eingabe die richtige Struktur aufweist, beispielsweise durch Prüfung:

— des Formats einer Datumseingabe (z. B. TT-MM-JJJJ oder MM-TT-JJJJ);

— der Verwendung eines Dezimalpunkts oder -kommas bei numerischen Eingaben;

— der Länge von Texteingaben;

— der richtigen Header und Strukturen von unterschiedlichen Dateitypen (z. B. Validierung einer .ZIP-, .BMP- oder .JPEG-Dateistruktur);

— einer gültige json-, xml- oder html-Datei.

Bei der Semantikvalidierung wird geprüft, ob die Eingabe mit den richtigen Werten erfolgt, beispielsweise:

— ob ein Wert außerhalb des erwarteten Bereichs liegt (z. B. eine Zahl, die zu klein oder zu groß ist, ein Geburtsdatum in der Zukunft);

— ob Sonderzeichen enthalten sind, die bei Texteingaben nicht zulässig sind, z. B. spezielle Escape-Zeichen, die bei SQL-Injection verwendet werden;

— ob fehlerhafte Datengrößen und Offset-Werte in einer Struktur vorhanden sind (eine fehlerhafte Größe könnte zu einem Pufferüberlauf führen, wenn Daten ohne Prüfung kopiert werden, oder ein negativer Offset könnte fehlerhafte Daten aus dem Stack kopieren).

Die Verwendung regulärer Ausdrücke ist ein Verfahren, um beispielsweise Texteingaben zu validieren; Entwickler könnten auch andere Verfahren wie Filterung und Codierung in Betracht ziehen, um sicherzustellen, dass eine Eingabe erfolgreich verarbeitet werden kann.

Weitere zu berücksichtigende Leitlinien sind:

— Common Weakness Enumeration: Improper Input Validation (CWE-20), Improper Encoding or Escaping of Output (CWE-116), Improper Neutralization of Special Elements (CWE-138) und Improper Filtering of Special Elements (CWE-790);

— Open Web Application Security Project (OWASP) Input Validation Cheat Sheet;

— EN IEC 62443-4-2 [2] CR 3.5 (Input Validation); und

— ETSI EN 303 645 [5] 5.13 (Validate Input Data).

5.10.6.4 Beurteilungskriterien

5.10.6.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung GEC-7.

5.10.6.4.2 Erforderliche Informationen

[E.Doc.DT.GEC-7] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 24 für jede externe Netzwerkschnittstelle und Benutzungsschnittstelle.

[E.Just.DT.GEC-7] Begründung für den gewählten Pfad durch den Entscheidungsbaum in Bild 24 für jede externe Netzwerkschnittstelle und Benutzungsschnittstelle.

[E.Doc.GEC-7] Vollständige Dokumentation aller externen Netzwerkschnittstellen und Benutzungsschnittstellen, einschließlich Informationen zu allen verwendeten APIs, Protokollen, Eingabedatentypen, Dateiformaten und darüber, ob die syntaktische und semantische Richtigkeit geprüft wird.

5.10.6.4.3 Konzeptuelle Beurteilung

5.10.6.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die Eingabevalidierungsfunktionalität des Geräts für die externen Netzwerkschnittstellen und die Benutzungsschnittstellen angewendet wird, und ob sie ausreichenden Schutz vor häufigen Angriffen bei bestimmungsgemäßer Verwendung des Geräts und in seiner für die Nutzung vorgesehenen Betriebsumgebung bietet.

5.10.6.4.3.2 Voraussetzungen

Keine.

5.10.6.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each external interface;
  if (Is the interface capable of recieving input?) then (Yes)
    if (Is this a user interface?) then (\n\nYes)
      if (Is the intended use and functionality \nof the user interface
   documented \nincluding any relevant input \ndata types supported?) then
   (Yes)
        if (Is the syntactic and semantic \ncorrectness checked?) then (No)
           #pink :FAIL\nInput not validated;
           detach;
       else (Yes)
           #lightgreen :PASS\nInput validated;
       endif
        detach;
    else (No)
           #pink :FAIL\nDocumentation\nincomplete;
           detach;
    endif
    else (No)
```

```
      if (Is the intended use and functionality \nof the interface
    documented including \nany relevant input data types, APIs, \nprotocols,
    file formats, etc.?) then (No)
            #pink :FAIL\nDocumentation\nincomplete;
         detach;
       else (Yes)
         if (Is the syntactic and semantic \ncorrectness checked?) then (No)
            #pink :FAIL\nInput not validated;
            detach;
        else (Yes)
            #lightgreen :PASS\nInput validated;
        endif
       endif
       endif
       detach;
   detach;
   else (No)
    #application :NOT APPLICABLE\nInterface does not \nprocess input;
    detach;
   endif
@enduml
```

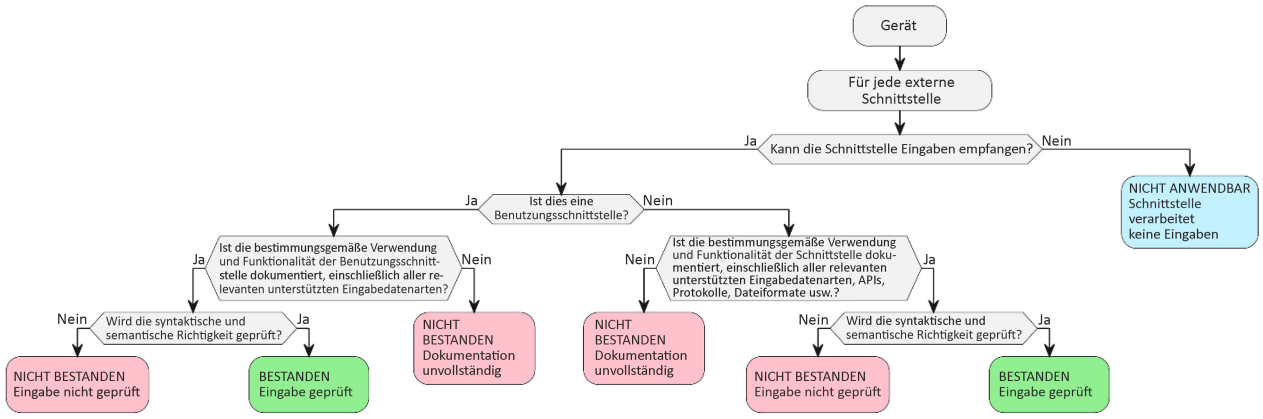

Bild 23 — Entscheidungsbaum für Anforderung GEC-7

Für jede in [E.Doc.GEC-7] dokumentierte externe Schnittstelle ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.GEC-7] dokumentierten Entscheidungsbaum mit „BESTANDEN“ oder „NICHT ANWENDBAR“ endet.

Für jeden in [E.Doc.DT.GEC-7] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.GEC-7] dokumentierte Begründung zu untersuchen.

5.10.6.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „BESTANDEN“ oder „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.6.4.4 Beurteilung der funktionalen Vollständigkeit

5.10.6.4.4.1 Zweck der Beurteilung

Der Zweck dieses Prüffalls ist die funktionale Beurteilung der Techniken zur Verifizierung, ob die Dokumentation vollständig ist.

5.10.6.4.4.2 Voraussetzungen

— Das Gerät befindet sich im Betriebszustand, und alle externen Netzwerkschnittstellen und Benutzungsschnittstellen, die Teil der bestimmungsgemäßen Verwendung sind, sind entweder aktiviert oder so konfiguriert, dass sie aktiviert werden können, so dass alle Netzwerkschnittstellen und Benutzungsschnittstellen geprüft werden können.

— Wenn für den Zugang zu einer externen Schnittstelle eine Authentisierung erforderlich ist, wird ein Mittel bereitgestellt, um die Schnittstelle prüfen zu können.

5.10.6.4.4.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob es weitere Netzwerkschnittstellen und Benutzungsschnittstellen gibt, die nicht in [E.Doc.GEC-7] aufgeführt sind.

5.10.6.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn alle externen Netzwerkschnittstellen und Benutzungsschnittstellen dokumentiert sind.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.10.6.4.5 Beurteilung der funktionalen Suffizienz

5.10.6.4.5.1 Zweck der Beurteilung

Der Zweck dieses Prüffalls ist die funktionale Beurteilung der Techniken, um die Implementation der dokumentierten Techniken zu verifizieren.

5.10.6.4.5.2 Voraussetzungen

— Das Gerät befindet sich im Betriebszustand, und alle externen Netzwerkschnittstellen und Benutzungsschnittstellen, die Teil der bestimmungsgemäßen Verwendung sind, sind entweder aktiviert oder so konfiguriert, dass sie aktiviert werden können, so dass alle Netzwerkschnittstellen und Benutzungsschnittstellen geprüft werden können.

— Wenn für den Zugang zu einer externen Schnittstelle eine Authentisierung erforderlich ist, wird ein Mittel bereitgestellt, um die Schnittstelle prüfen zu können.

— Prüf-Tools wie unter anderem Protokollanalysatoren, Prüf-Tools für die Eingabevalidierung und Fuzzing-Tools.

5.10.6.4.5.3 Beurteilungseinheiten

Es ist funktional zu beurteilen, ob die externen Netzwerkschnittstellen und Benutzungsschnittstellen resilient gegenüber häufigen Angriffen auf Eingänge sind, wobei ihre Funktionalität, die bestimmungsgemäße Verwendung des Geräts und die für die Nutzung vorgesehene Betriebsumgebung zu berücksichtigen sind.

5.10.6.4.5.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird zugewiesen, wenn Angriffsversuche auf die Eingabevalidierung nicht zum Ausfall der Funktionalität des Geräts führten und keine Werte verfälscht, extrahiert oder missbraucht werden konnten.

Andernfalls wird die Entscheidung NICHT BESTANDEN zugewiesen.

5.11 [CRY] Kryptographie (en: Cryptography)

5.11.1 [CRY-1] Bewährte Verfahrensweisen für Kryptographie

5.11.1.1 Anforderung

Das Gerät muss bewährte Verfahrensweisen für Kryptographie nutzen, die zum Schutz der Sicherheits- oder Netzwerkwerte eingesetzt werden.

5.11.1.2 Begründung

Kryptographie, die für den Schutz von Werten eingesetzt wird und die nicht stark genug für den Anwendungsfall ist, weil sie beispielsweise nicht geeignet oder fehlerhaft ist, stellt für diese Werte ein Sicherheitsrisiko dar. Der Einsatz bewährter Verfahrensweisen oder sogar einer fortschrittlicheren, offensichtlich geeigneten Kryptographie schafft Vertrauen in den kryptographischen Schutz dieser Werte.

Wenn ein kryptographischer Algorithmus geknackt wird oder kryptographische Elemente kompromittiert werden, kann es erforderlich sein, das Gerät entsprechend zu aktualisieren (siehe Anforderung SUM), um den Schutz der durch Kryptographie geschützten Werten zu erhalten. Zwar gibt es keine absolute Garantie, dass dies nicht bei Kryptographieverfahren vorkommt, die als bewährte Verfahrensweisen gelten, aber es ist wahrscheinlicher, dass die Kryptographie für einen bestimmten Anwendungsfall ungeeignet ist, wenn bereits Hinweise vorliegen, dass die Kryptographie während der vorhergesehenen Lebensdauer des Geräts veralten wird.

Allerdings kann das Gerät unter Umständen nicht für die Aktualisierung der Kryptographie vorbereitet werden, beispielsweise wenn hardwarebasierte Krypto-Beschleuniger eingesetzt werden, die selbst über das Internet kommunizieren können. In diesen Fällen ist es wichtig, dass keine Hinweise vorliegen, dass die Kryptographie während der vorhergesehenen Lebensdauer nicht mehr zu den bewährten Verfahrensweisen zählen wird.

5.11.1.3 Leitlinie

Es gibt verschiedene Sicherheitsleitlinien, die zur Identifizierung bewährter Verfahrensweisen für Kryptographie verwendet werden können; siehe entsprechende ISO/IEC-Normen, öffentliche, von SDOs und Behörden bereitgestellte Krypto-Kataloge wie beispielsweise sogis.eu, „SOGIS agreed Cryptographic Mechanisms“ Version 1.3 vom Februar 2023 und von ENISA und nationalen Behörden bereitgestellte Leitlinien.

Ein häufig für einen bestimmten Anwendungsfall eingesetztes kryptographisches Verfahren, für das kein Nachweis möglicher Angriffe mit aktuell einfach verfügbaren Techniken vorliegt, kann als bewährte Verfahrensweise gelten.

Es ist aber auch möglich, den Nachweis zu liefern, dass eine neue Kryptographie für einen bestimmten Anwendungsfall geeignet ist und daher als bewährte Verfahrensweise für Kryptographie gelten kann.

Kryptographie wird häufig für den Schutz entsprechender Werte eingesetzt, beispielsweise:

— Authentisierung (siehe AUM);

— sichere Aktualisierung (siehe SUM);

— sichere Speicherung (siehe SSM);

— sichere Kommunikation (siehe SCM); und

— Erzeugung vertraulicher kryptographischer Schlüssel (siehe CCK-2).

Der kryptographische Schutz entspricht möglicherweise nicht bewährten Verfahrensweisen, wenn die Interoperabilität mit Legacy-Systemen gefordert ist.

Wenn überprüfte oder bewertete Implementationen öffentlich verfügbar sind, die dem Stand der Technik entsprechen, können diese bevorzugt eingesetzt werden, um Netzwerk- und Sicherheitsfunktionen bereitzustellen, insbesondere im Bereich der Kryptographie.

Um während der vorhergesehenen Lebensdauer des Geräts bewährte Verfahrensweisen für Kryptographie zu nutzen, sollte zusätzlich das Konzept der Krypto-Agilität in Betracht gezogen werden, das es ermöglicht, die Kryptographie auf dem Gerät in Übereinstimmung mit [SUM] zu aktualisieren.

Elemente, die bei der Vorbereitung der Kryptographie für die Aktualisierung zu beachten sind, sind unter anderem:

— kryptographische Verfahren, Protokolle, Algorithmen, Konstruktoren und Primzahlen;

— die Art der verwendeten sensiblen Sicherheitsparameter; und

— spezifische SSPs, wie beispielsweise Vertrauensgrundlagen.

Bei Geräten, deren kryptographische Algorithmen oder Elemente nicht aktualisiert werden können, beispielsweise weil die Implementation oder das Teil eine hardwarebasierte Vertrauensgrundlage verwenden, ist es wichtig, dass die vorhergesehene Lebensdauer des Geräts nicht länger ist als die empfohlene Lebensdauer für die Nutzung der vom Gerät verwendeten kryptographischen Algorithmen und Elemente.

5.11.1.4 Beurteilungskriterien

5.11.1.4.1 Beurteilungsziel

Die Beurteilung betrifft die Anforderung CRY-1.

5.11.1.4.2 Erforderliche Informationen

[E.Doc.DT.CRY-1] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 25 für jeden Sicherheits- und Netzwerkwert.

[E.Just.DT.CRY-1] Begründung für den gewählten Pfad durch den Entscheidungsbaum in Bild 25 für jeden Sicherheits- und Netzwerkwert.

[E.Doc.SecurityAsset.CRY] Dokumentation aller Sicherheitswerte, die durch Kryptographie geschützt sind.

[E.Doc.NetworkAsset.CRY] Dokumentation aller Netzwerkwerte, die durch Kryptographie geschützt sind.

[E.Doc.SecurityAsset.CRY.CryptoProtect] Dokumentation für jeden kryptographischen Schutz für alle in [E.Doc.SecurityAsset.CRY] dokumentierten Sicherheitswerte.

[E.Doc.NetworkAsset.CRY.CryptoProtect] Dokumentation für jeden kryptographischen Schutz für alle in [E.Doc.NetworkAsset.CRY] dokumentierten Netzwerkwerte.

ANMERKUNG Die Dokumentation eines kryptographischen Schutzes schließt die von der Kryptographie bereitgestellten Sicherheitseigenschaften ein.

[E.Doc.CRY-1] Dokumentation für jede verwendete Kryptographie für jeden kryptographischen Schutz aller Sicherheits- und Netzwerkwerte.

ANMERKUNG Kryptographie, die für den kryptographischen Schutz eingesetzt wird, kann unter anderem kryptographische Verfahren, Algorithmen, Konstruktoren und Primzahlen nutzen.

5.11.1.4.3 Konzeptuelle Beurteilung

5.11.1.4.3.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die konzeptuelle Beurteilung, ob die zum Schutz von Sicherheits- oder Netzwerkwerten implementierte Kryptographie als bewährte Verfahrensweise gilt.

5.11.1.4.3.2 Voraussetzungen

Keine.

5.11.1.4.3.3 Beurteilungseinheiten

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
    :For each security and network asset;
      if (Does the equipment use cryptography\nfor the protection of the
   security or network asset?) then (No)
        #application :NOT APPLICABLE\nCryptogaphy not used for protection;
        detach;
      else (Yes)
        :For each cryptoraphic protection of the security or network asset;
          :For each cryptography used for cryptographic protection;
            if (Is the cryptography best practices\nconcerning the
   protection of the \nsecurity asset or network asset?) then (No)
              #pink :FAIL\nCryptogaphy is not best practice;
              detach;
            else (Yes)
              #lightgreen :PASS\nCryptogaphy is best practice;
              detach;
            endif
      endif
@enduml
```

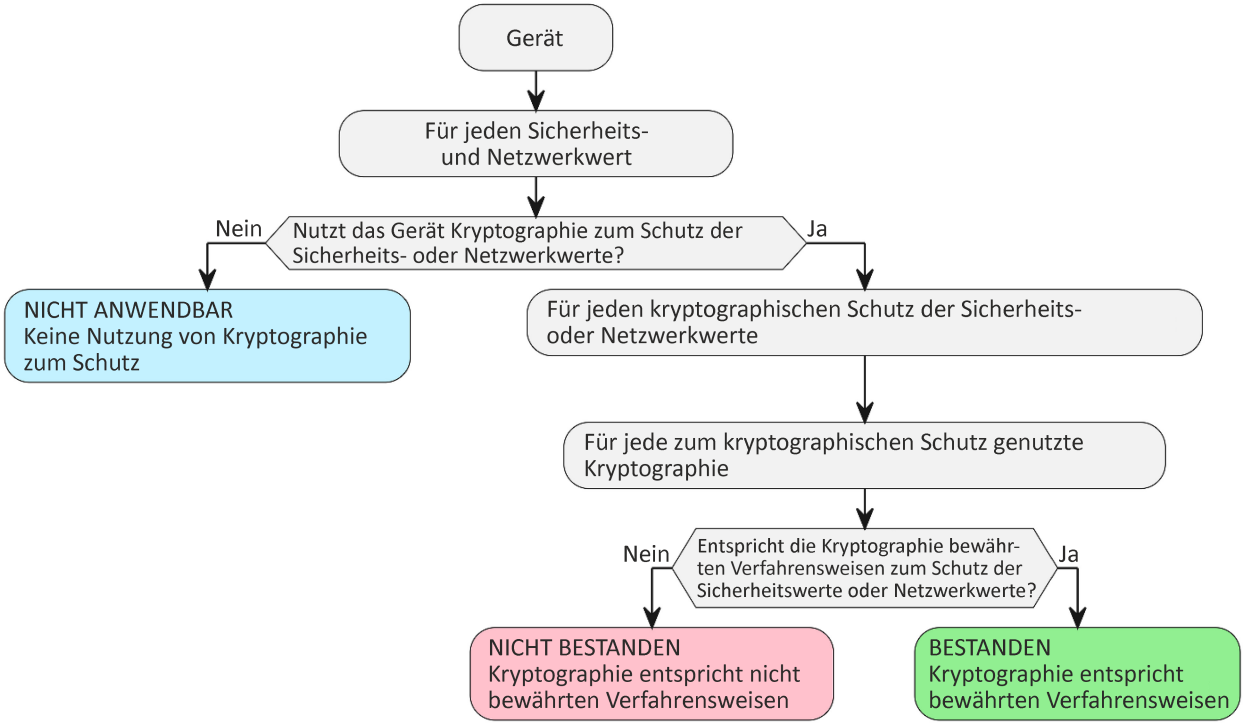

Bild 24 — Entscheidungsbaum für Anforderung CRY-1

Für jeden in [E.Doc.SecurityAsset.CRY] dokumentierten Sicherheitswert und jeden in [E.Doc.NetworkAsset.CRY] dokumentierten Netzwerkwert, für jeden kryptographischen Schutz [E.Doc.SecurityAsset.CRY.CryptoProtect] und [E.Doc.NetworkAsset.CRY.CryptoProtect] und für jede in [E.Doc.CRY-1] dokumentierte Kryptographie ist zu prüfen, ob der Pfad durch den in [E.Doc.DT.CRY-1] dokumentierten Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DT.CRY-1] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DT.CRY-1] dokumentierte Begründung zu untersuchen.

5.11.1.4.3.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn:

— mindestens ein Pfad durch den Entscheidungsbaum mit „BESTANDEN“ endet; und

— kein Pfad durch den Entscheidungsbaum mit „NICHT BESTANDEN“ endet; und

— alle Begründungen gültig sind.

Die Entscheidung NICHT ANWENDBAR wird dem Beurteilungsfall zugewiesen, wenn:

— alle Pfade durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ enden; und

— alle Begründungen gültig sind.

Andernfalls wird dem Beurteilungsfall die Entscheidung NICHT BESTANDEN zugewiesen.

5.11.1.4.4 Beurteilung der funktionalen Vollständigkeit

5.11.1.4.4.1 Zweck der Beurteilung

Der Zweck dieses Beurteilungsfalls ist die funktionale Beurteilung, ob die Dokumentation in [E.Doc.CRY-1] vollständig ist.

5.11.1.4.4.2 Voraussetzungen

Das Gerät befindet sich im Betriebszustand.

5.11.1.4.4.3 Beurteilungseinheiten

Für jeden in [E.Doc.SecurityAsset.CRY.CryptoProtect] und [E.Doc.NetworkAsset.CRY.CryptoProtect] dokumentierten kryptographischen Schutz ist funktional zu beurteilen, ob auf dem Gerät Kryptographie eingesetzt wird, die nicht in [E.Doc.CRY-1] dokumentiert ist.

5.11.1.4.4.4 Entscheidungszuweisung

Die Entscheidung BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn jede auf dem Gerät gefundene Kryptographie in [E.Doc.CRY-1] dokumentiert ist.

Die Entscheidung NICHT BESTANDEN wird dem Beurteilungsfall zugewiesen, wenn eine Kryptographie auf dem Gerät gefunden wird, die nicht in [E.Doc.CRY-1] dokumentiert ist.

5.11.1.4.5 Beurteilung der funktionalen Suffizienz

Keine.

Anhang A
(informativ)

Begründung

A.1 Allgemeines

Dieser Anhang enthält eine Begründung für die Begriffe und Konzepte in Zusammenhang mit diesem Dokument.

A.2 Begründung

A.2.1 Normenfamilie

Dieses Dokument gehört zu einem Satz von drei Normen, die die in Artikel 3.3.d, Artikel 3.3.e und Artikel 3.3.f der Verordnung 2014/53/EU festgelegten und von der Delegierten Verordnung (EU) 2022/30 der Kommission aktivierten grundlegenden Anforderungen behandeln. Ein erster Schritt, um mit der Durchsetzung von Cybersicherheits-Anforderungen für die europäische Markteinführung von Funkanlagen zu beginnen, war die Nutzung der Funkanlagen-Richtlinie, denn die mangelhafte Sicherheit insbesondere bei Endverbraucher-IoT-Geräten war und ist ein zunehmendes gesellschaftliches Problem.

Zwar liegt der Schwerpunkt der drei Normen auf unterschiedlichen grundlegenden Anforderungen (Netzwerkschäden, personenbezogene Daten und Privatsphäre sowie Schutz vor (finanziellem) Betrug), aber sie umfassen sowohl spezifische als auch sich überlappende Anforderungen, für die eine wachsende Anzahl stärkerer Sicherheitskontrollen implementiert werden muss, um das Netzwerk, die Privatsphäre und die finanziellen Werte in einem Umfeld zunehmender Bedrohungen zu schützen.

Ob für eine bestimmte Funkanlage eine oder mehrere Normen gelten, ist eine Erwägung, die der Wirtschaftsteilnehmer anstellen muss, indem er eine Risikobeurteilung zur Notwendigkeit der Erfüllung grundlegender Anforderungen der Funkanlagen-Richtlinie durchführt. Der „RED Guide“ und der „Blue Guide“ der Europäischen Kommission enthalten weitere Leitlinien zu diesem Thema.

A.2.2 Sicherheit durch Gestaltung (en: Security by Design)

Ein effektives Sicherheitsmanagement erfordert etablierte Security-by-Design-Prozesse. In diesem Dokument, das häufige Sicherheitsanforderungen für Geräte festlegt, wird dies nicht abgedeckt. Beispiele für Security-by-Design-Prozessnormen, die bei der Erfüllung von Sicherheitsanforderungen unterstützen können, sind unter anderem:

— IEC 62443-4-1 [1]: *Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements*

— NIST 800-160 [14]: *Systems Security Engineering; Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*

— NIST 800-218 [15]: *Secure Software Development Framework (SSDF)*

— Microsoft Security Development Lifecycle (SDL)

— SAFECode Fundamental Practices for Secure Software Development

A.2.3 Werte

Um sicherzustellen, dass Anforderungen über die drei horizontalen Normen hinweg - die alle spezifische grundlegende Anforderungen behandeln - angeglichen werden können, wurden Werte (abgeleitet von den grundlegenden Anforderungen) als Hauptziele eingeführt, an denen die Anforderungen auszurichten sind:

Tabelle A.1 —

	3.3.d	3.3.e	3.3.f
Sicherheitswert	√	√	√
Netzwerkwert	√		
Datenschutzwert		√	
Finanzieller Wert			√

Beim Schutz von Werten geht es nicht nur um den Schutz der spezifischen gespeicherten und kommunizierten oder anderweitig durch das Gerät verarbeiteten Daten, sondern auch um den Schutz der vom Gerät genutzten Funktionen und der Konfiguration von Funktionen. Daher wird auch die Sicherheitsfunktionalität, insbesondere wenn sie dem Schutz der Geräteintegrität dient, als Sicherheitswert bezeichnet.

A.2.4 Mechanismen

In dieser Norm wird das Konzept von Mechanismen verwendet, um spezifische Sicherheitsanforderungen zu behandeln und die Anwendbarkeit und Angemessenheit der Anforderungen für verschiedene Geräteimplementationen und Anwendungsbereiche zu ermöglichen. Da dies eine horizontale Norm ist, muss sie einen weiten Bereich von Produkten und Anwendungsfällen abdecken.

Ob und wie allgemeine Sicherheitsziele zu erreichen sind, hängt von der bestimmungsgemäßen Verwendung und der für die Nutzung vorgesehenen Betriebsumgebung ab. Diese beeinflussen, welche Implementationen von Sicherheitsmaßnahmen tatsächlich bei einem bestimmten Gerät erforderlich sind und wie stark die Kontrollen sein müssen. Eine spezifische Sicherheitsmaßnahme kann für ein Produkt angemessen sein, kann aber für andere Produkte oder das gleiche Produkt beim Einsatz in einer anderen Umgebung zu schwach oder zu stark sein.

Die Norm enthält spezifische Einschränkungen und Bewertungsfragen; diese sollen als Anleitung dienen und um eine vollständige Abhängigkeit von der Sorgfalt des Herstellers zu vermeiden, soweit es die notwendigen Sicherheitsmaßnahmen bei bestimmungsgemäßer Verwendung in der für die Nutzung vorgesehenen Betriebsumgebung betrifft.

Um Benutzer dieses Dokuments dabei anzuleiten, wann ein bestimmter Mechanismus anzuwenden ist, behandelt die erste Anforderung die Anwendbarkeit des Mechanismus. Diese Anforderungen dürfen eine Komponente enthalten, die mit „außer“ beginnt; sie gibt mögliche Bedingungen an, bei denen der Mechanismus nicht erforderlich ist. Wenn festgelegt wurde, dass der Mechanismus nicht anwendbar ist, dann sind alle weiteren Anforderungen in diesem spezifischen Abschnitt nicht länger verpflichtend.

Falls ein Mechanismus erforderlich ist, wird die Suffizienz bestimmt, indem die Angemessenheit der Anforderung und die Beurteilungskriterien bewertet werden. Alle unterstützenden Anforderungen in diesem Abschnitt sind dann ebenfalls anwendbar.

Diese Entscheidung muss für jede angegebene Einheit getroffen werden; beispielsweise wird bei der Prüfung der Anwendbarkeit einer Anforderung auf externe Schnittstellen die Entscheidung, ob die Anforderung und alle weiteren Anforderungen erfüllt werden müssen, unabhängig für jede externe Schnittstelle getroffen.

A.2.5 Beurteilungskriterien

Die Sicherheitsmechanismen, die Funktionalität oder andere für das Gerät geltenden Verpflichtungen wurden in möglichst präzisen und objektiven Begriffen beschrieben, ohne den technologieagnostischen Grundton der Norm in Frage zu stellen. Wie diese jeweils vom Gerät implementiert werden, wird durch den Hersteller festgelegt, der die Vorgaben für die Konformitätsprüfung liefert.

A.2.5.1 Entscheidungsbäume

Ob ein Mechanismus oder eine Anforderung anwendbar und/oder angemessen ist, hängt von der bestimmungsgemäßen Verwendung und der für die Nutzung vorgesehenen Betriebsumgebung ab. Dieses Dokument verwendet Entscheidungsbäume, um die Entscheidungsfindung und Beurteilung zu unterstützen und klare Anweisungen vorzugeben. Ein Beispiel ist im Folgenden dargestellt.

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each asset;
    if (Is protection required? ) then (Yes)
      if (Various questions to determine\nif the protection is adequate?)
   then (Yes)
        #lightgreen :PASS\nProtection is appropriate;
        detach;
        else (No)
         #pink :FAIL\nProtection is not appropriate;
         detach;
      endif
      detach;
    else (No)
      #application :NOT APPLICABLE\nNothing to protect;
      detach;
    endif
@enduml
```

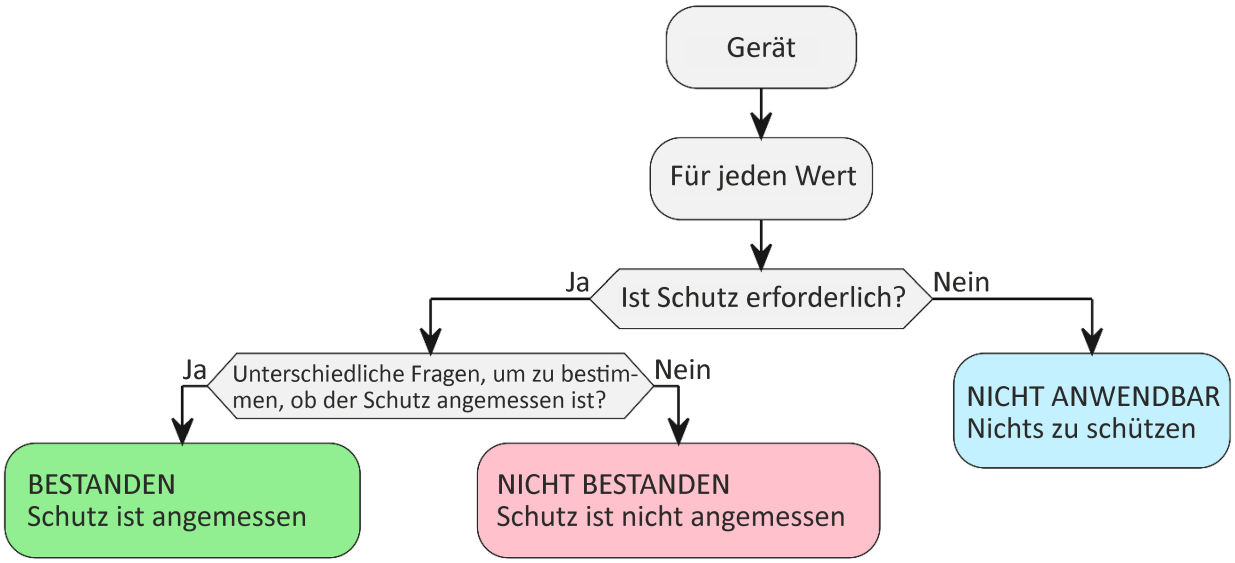

Bild A.1 — Beispiel für einen Entscheidungsbaum

Am Anfang der meisten Entscheidungsbäume steht das Gerät, gefolgt von einem Element, über das iteriert wird (z. B. die oben erwähnten Werte). Für jedes dieser Elemente müssen Fragen zu den Geräteeigenschaften oder den entsprechenden Umgebungsfaktoren beantwortet werden. Jeder Entscheidungsbaum hat mindestens jeweils einen Pfad, der in BESTANDEN und NICHT BESTANDEN endet, und er kann optional einen oder mehrere Pfade haben, der/die in NICHT ANWENDBAR enden. Für jeden gewählten Pfad muss die Begründung dokumentiert werden.

A.2.5.2 Technische Dokumentation

Die Beurteilungen sind von den Informationen abhängig, die als Teil der technischen Dokumentation vom Hersteller bereitzustellen sind. Die spezifischen Informationselemente, die für die Beurteilung in der technischen Dokumentation des Herstellers enthalten sein müssen, werden als [E.Doc.xxxxx] bezeichnet, wobei xxxxx für den spezifischen geforderten Informationssatz steht; beispielsweise enthält [E.Doc.OperationalEnvironment] die Beschreibung der für die Nutzung des Geräts vorgesehenen Betriebsumgebung, und [E.Doc.ACM] enthält einige Informationen, die für die Beurteilung von Zugangssteuerungsmechanismen erforderlich sind.

Zu den erwarteten allgemeinen Informationen gehören:

— Informationen über die bestimmungsgemäße Verwendung des Geräts;

— Informationen über die für die Nutzung des Geräts vorgesehene Betriebsumgebung;

— technische Informationen über das Gerät;

— Festlegung des Standes der Technik und der bewährten Verfahrensweisen;

— spezifische Einzelheiten, wie beispielsweise eine Liste externer Schnittstellen;

— Risikobeurteilung.

Pfade durch den Entscheidungsbaum, die als Eingänge für die Beurteilung dienen, werden mit [E.Doc.DT.xxxxxx] bezeichnet, und die Begründung wird mit [E.Just.DT.xxxxxx] bezeichnet. Die folgende Tabelle ist nur ein Beispiel, wie dies bei der konzeptuellen Beurteilung umgesetzt werden könnte.

Tabelle A.2 —

Nr.	Frage	Antwort		Begründung/Nachweis
1	Bestimmungsgemäße Verwendung der Schnittstelle: Ermöglicht die Schnittstelle den Zugang zu Netzwerkwerten oder Sicherheitswerten von Geräten?	Ja (x)	Nein	Netzwerkwert: IP-basierte Kommunikation mit dem Internet Sicherheitswerte des Geräts Zugangsdaten zum Cloud-Konto Gemeinsames Geheimnis
2	Für die Nutzung vorgesehene Betriebsumgebung: Kommuniziert die Schnittstelle nur innerhalb von vertrauenswürdigen Netzwerken	Ja	Nein (x)	Sie kommuniziert über das Internet
3	Technische Eigenschaften der Schnittstelle: Erfordert die Schnittstelle zur Erfüllung ihrer bestimmungsgemäßen Funktion, dass keine Authentisierung erfolgt?	Ja	Nein (x)	Keine Begründung für das Nichtvorhandensein

Tabelle A.2 (*fortgesetzt*)

Nr.	Frage	Antwort		Begründung/Nachweis
4	Technische Eigenschaften der Schnittstelle: Nutzt die Schnittstelle einen Authentisierungsmechanismus?	Ja (x)	Nein	Passwortbasierter Authentisierungsmechanismus zwischen Smartphone und Cloud und gemeinsames Geheimnis auf Basis eines Vertrauensverhältnisses zwischen Babyüberwachungsgerät und Cloud
Entscheidung über den Beurteilungsfall: BESTANDEN				

A.2.5.3 Sicherheitsprüfung

Die Angemessenheit der meisten Sicherheitsprüfungen ist nicht quantitativ messbar, da es keine zu einem Thermometer oder einem Frequenzmessgerät äquivalenten Geräte gibt, um die Stellung der Ausrüstung in Bezug auf Sicherheit zu messen, und keine stringente Definition, wann „gut“ gut genug ist.

Das Ergebnis ist daher vom Wissen des Beurteilers und seiner Wahrnehmung der Bedrohungslandschaft abhängig sowie davon, was für eine spezifische Ausrüstung in einer spezifischen Umgebung angemessen ist; dies trägt zusätzlich zu der Schwierigkeit bei, verifizierbare, objektive und reproduzierbare Prüfkriterien zu definieren, weil selbst zwei Beurteiler erheblich abweichende Ansichten und/oder Meinungen haben können.

Tools für Sicherheitsprüfungen weisen oft anhand von Negativprüfungen nach, dass bestimmte Schwachstellen nicht vorhanden sind; weil aber Sicherheitstools ständig aktualisiert werden, können aufgrund aktualisierter Informationen oder bei der Ausführung über längere Zeiträume neue Probleme erkannt werden - so führt auch dies nicht zu reproduzierbaren Prüfungsergebnissen.

Daher verbessert der in diesem Dokument gewählte Ansatz zwar das Ergebnis der Beurteilung, aber er kann das Problem nicht lösen. Die meisten Beurteilungen beruhen darauf, dass ausreichende Informationen zur Verfügung stehen.

A.2.6 Sicherheitsparameter

Ein Sicherheitsparameter ist eine in Sicherheitsfunktionen zum Schutz von Werten verwendete Information:

— Per Definition handelt es sich bei einem vertraulichen Sicherheitsparameter (CSP) um eine geheime sicherheitsrelevante Information, deren Änderung oder Offenlegung die Sicherheit eines Werts kompromittieren kann. Übliche Beispiele sind PINs und Passwörter, symmetrische kryptographische Schlüssel oder private asymmetrische kryptographische Schlüssel.

— Ein öffentlicher Sicherheitsparameter (PSP) ist eine sicherheitsbezogene öffentliche Information, deren Änderung die Sicherheit eines Werts kompromittieren kann. Dies bedeutet, dass zwar die Integrität von PSPs entscheidend wichtig ist, nicht aber deren Vertraulichkeit. Übliche Beispiele sind öffentliche kryptographische Schlüssel oder kryptographische Zertifikate.

— Ein sensibler Sicherheitsparameter (SSP) ist entweder ein CSP oder ein PSP.

Anhang ZA
(informativ)

Zusammenhang zwischen dieser Europäischen Norm und der Delegierten Verordnung (EU) 2022/30 zur Ergänzung der Verordnung 2014/53/EU des Europäischen Parlaments und des Rates im Hinblick auf die Anwendung der grundlegenden Anforderungen, wie in Artikel 3(3), Punkt (d), Punkt (e) und Punkt (f) dieser abzudeckenden Verordnung in Bezug genommen

Diese Europäische Norm wurde im Rahmen eines von der Europäischen Kommission erteilten Normungsauftrages [C(2022) 5637 final] erarbeitet, um ein freiwilliges Mittel zur Erfüllung der grundlegenden Anforderungen der Verordnung 2014/53/EU [Amtsblatt L 153] des Europäischen Parlaments und des Rates zur Anwendung der in Artikel 3(3) in Bezug genommenen grundlegenden Anforderungen bereitzustellen.

Im Falle von Unterschieden zwischen in dieser Europäischen Norm definierten Begriffen und in der genannten Verordnung definierten Begriffen ist die Verordnung maßgebend.

Sobald diese Norm im Amtsblatt der Europäischen Union im Sinne dieser Delegierten Verordnung (EU) 2022/30 in Bezug genommen worden ist, berechtigt die Übereinstimmung mit den in Tabelle ZA.1 aufgeführten normativen Abschnitten dieser Norm innerhalb der Grenzen des Anwendungsbereiches dieser Norm zur Vermutung der Konformität mit den entsprechenden grundlegenden Anforderungen der Richtlinie 2014/53/EU und der zugehörigen EFTA-Vorschriften.

Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und der Richtlinie 2014/53/EU [Amtsblatt L 153]

Grundlegende Anforderungen der Richtlinie 2014/53/EU	Abschnitt(e)/Unterabschnitt(e) dieser EN	Erläuterungen/Anmerkungen
3.3.(d)	5.1 bis 5.11	Abgedeckt
3.3.(e)		
3.3.(f)		

WARNHINWEIS 1 — Die Konformitätsvermutung bleibt nur bestehen, solange die Fundstelle dieser Europäischen Norm in der im Amtsblatt der Europäischen Union veröffentlichten Liste erhalten bleibt. Anwender dieser Norm sollten regelmäßig die im Amtsblatt der Europäischen Union zuletzt veröffentlichte Liste einsehen.

WARNHINWEIS 2 — Für Produkte, die in den Anwendungsbereich dieser Norm fallen, können weitere Rechtsvorschriften der EU anwendbar sein.

Literaturhinweise

[1] EN IEC 62443-4-1, *IT-Sicherheit für industrielle Automatisierungssysteme — Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung*

[2] EN IEC 62443-4-2, *IT-Sicherheit für industrielle Automatisierungssysteme — Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)*

[3] EN ISO/IEC 27002:2022, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmaßnahmen*

[4] EN ISO/IEC 24760 (Reihe), *IT-Sicherheit und Datenschutz — Rahmenwerk für Identitätsmanagement*

[5] ETSI EN 303 645, *Cyber Security for Consumer Internet of Things — Baseline Requirements*

[6] ETSI TS 103 701, *Cyber Security for Consumer Internet of Things — Conformance Assessment of Baseline Requirements*

[7] NIST SP 800-63 series, *Digital Identity Guidelines*

[8] NIST SP 800-63B, *Digital Identity Guidelines — Authentication and Lifecycle Management*

[9] NIST SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

[10] NIST SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*

[11] NIST SP 800-90C, *Recommendation for Random Bit Generator (RBG) Constructions*

[12] NIST SP 800-108r1, *Recommendation for Key Derivation Using Pseudorandom Functions*

[13] NIST SP 800-132, *Recommendation for Password-Based Key Derivation: Part 1: Storage Applications*

[14] NIST SP 800-160, *Engineering Trustworthy Secure Systems*

[15] NIST SP 800-218, *Secure Software Development Framework (SSDF) — Recommendations for Mitigating the Risk of Software Vulnerabilities*

[16] BSI AIS 31, *A Proposal for Functionality Classes for Random Number Generators*

[17] FIPS 140-2, *Security Requirements for Cryptographic Modules*

[18] FIPS 140-3, *Security Requirements for Cryptographic Modules*

– Entwurf –

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 18031-1

August 2023

ICS

English version

Common security requirements for radio equipment - Part 1: Internet connected radio equipment

Exigences de sécurité communes applicables aux équipements radioélectriques connectés à l¿internet

Gemeinsame Sicherheitsanforderungen für mit dem Internet verbundene Funkanlagen

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

Ref. No. prEN 18031-1:2023 E

Contents

Page

European foreword

This document (prEN 18031-1:2023) has been prepared by Technical Committee CEN/CENELEC JTC 13/WG 8 “Special Working Group RED Standardization Request”, the secretariat of which is held by NEN.

This document is currently submitted to the CEN Enquiry.

This document has been prepared under a mandate given to CEN/CENELEC by the European Commission and the European Free Trade Association and supports essential requirements of EU Directive(s) / Regulation(s).

For relationship with EU Directive(s) / Regulation(s), see informative Annex ZA, which is an integral part of this document.

Introduction

It is important to note that in order to achieve the overall cybersecurity of radio equipment, defence in depth best practices will be needed. In particular, no one single measure will suffice to achieve the given objectives, indeed achieving even a single security objective will usually require a suite of mechanisms and measures. Throughout this document, the guidance material includes lists of examples. These lists must be read only as indicative possibilities: there are other possibilities that are not listed, and even using the examples given will not be sufficient unless the mechanisms and measures chosen are implemented in a coordinated fashion.

1 Scope

This document specifies common security requirements for internet-connected radio equipment. This document provides technical specifications for radio equipment, which concerns electrical or electronic products that are capable to communicate over the internet, regardless of whether these products communicate directly or via any other equipment.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp/

3.1
access control mechanism
equipment functionality to grant, restrict or deny access to specific *equipment's* resources

Note 1 to entry: Access to specific equipment's resources can amongst others be:

- reading specific data; or
- writing specific data to equipment's persistent storage; or
- performing a specific equipment functionality such as recording audio.

3.2
authentication
provision of assurance that an *entity* is who or what it claims to be

3.3
authentication mechanism
equipment functionality to verify that an *entity* is who or what it claims to be

Note 1 to entry: An entity can amongst others claim to be:

- a specific human, owner of a user account, device, or service; or
- a member of specific groups such as an authorized group to access a specific equipment's resource; or
- authorized by another entity to access a specific equipment's resource.

Note 2 to entry: Typically, the verification is based on examining evidence from one or more elements of the categories:

- knowledge; and
- possession; and
- inherence.

3.4
authenticator
means used to validate the claim of an *entity*

EXAMPLE: A password or token may be used as an authenticator.

3.5
best practice
measures that have been shown to provide appropriate security for the corresponding use case

3.6
brute force attack
method based on trial-and-error to guess the right *authenticator*

3.7
communication mechanism
equipment functionality that allows communication via a device *interface*

3.8
confidential security parameters
secret security related information whose modification or disclosure can compromise the security of an asset

3.9
denial of service (DoS)
prevention or interruption of authorized access to an equipment resource or the delaying of equipment operations and functions

[SOURCE : IEC 62443-1-1 :2019, 3.2.42] modified

3.10
entity
user, device or service

3.11
equipment
radio equipment
electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radio determination, or an electrical or electronic product which must be completed with an accessory, such as an antenna, to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radio determination

[SOURCE: Directive 2014/53/EU, article 2.1(1)]

3.12
external interface
interface on the *equipment* that is accessible from outside the *equipment*

3.13
factory default state
defined state where the configuration settings and configuration of the equipment is set to initial values typically set when it leaves the manufacturing factory

Note 1 to entry: a factory default state may include security updates, installed after the equipment being placed on the market.

3.14
initialization
process that configures the network connectivity of the *equipment* for operation

Note 1 to entry: Initialization may provide the possibility to configure authentication features for a user or for network access

3.15
interface
shared boundary across which *entities* exchange information

3.16
legacy
equipment, software/hardware component, cryptography or communication protocol that cannot be protected against current cybersecurity threats without mitigating measures

3.17
machine interface
external interface between the *equipment* and a service or device

3.18
network equipment
equipment that exchanges data between different networks

3.19
network asset
network functions, or *network functions configuration* stored at the *equipment,* or *sensitive security parameter* stored at the *equipment* for access to network resources

3.20
network function
equipment's functionality to access network resources

3.21
network functions configuration
data that defines the behaviour of the *equipment's network functions*

3.22
network interface
external interface enabling the *equipment* to have or provide access to a network

Note 1 to entry: Examples for network interfaces are a LAN port (wired) or a wireless network interface enabling WLAN or Bluetooth communication, e.g., using a 2.4 GHz antenna.

3.23
operational state
state in which the *equipment* is functioning normally providing its intended use and within its intended operational environment of use

3.24
optional services
services which are not necessary to setup the *equipment*, and which are not part of the basic functionality but are still relevant for the intended use of the *equipment* and are delivered as part of the factory default.

Example: an SSH service on the equipment is not required for basic functionality of the equipment, but it may be used to allow a remote access to the equipment

3.25
password
sequence of characters (letters, numbers, or other symbols) used to authenticate an *entity*
Note: personal identification numbers (PINs) are also considered a form of password

3.26
public security parameters
security related public information whose modification can compromise the security of an asset

3.27
resilient
able to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

[SOURCE: NIST Glossary: https://csrc.nist.gov/glossary/term/cyber_resiliency]

3.28
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:2014]

3.29
security asset
equipment's security functionality that can directly affect the *equipment's* integrity, or *security relevant configuration* used by the *equipment* or, *sensitive security parameter* for *equipment's* integrity used by the *equipment*

3.30
security relevant configuration
data that affects the behaviour of the *equipment's* security functionality

3.31
sensitive security parameters
confidential security parameter for an asset or *public security parameter* for an asset

3.32
security update
software update that addresses security vulnerabilities through code patches or other mitigations

3.33
storage mechanism
equipment functionality that allows to store information

3.34
update mechanism
equipment functionality that allows to change *equipment's* software

3.35
user interface
external interface between the *equipment* and a user

3.36
vulnerability
weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the *equipment*, network, application, or protocol involved.

[SOURCE: (ITSEC) (definition given by ENISA, "computer system" has been replaced by "equipment")]

4 Application of this standard

This standard uses the concept of mechanism to instruct the user of this standard when to apply certain security measures. Mechanisms address the applicability and appropriateness through a set of requirements including assessment criteria. The pass/fail decision is made for each of the items specified, for example when checking the applicability of a requirement on external interfaces, then the decision whether the requirement and all further requirements need to be fulfilled is determined for each external interface independently.

The mechanisms are documented using the following structure and how to apply them:

Table 1

Clause #	Title	Description on how to apply the standard
5.x	XXX Mechanism	Mechanism for each specific item (e.g., external interface or security asset)
5.x.1	XXX-1 Applicability of mechanisms	Applicability of the mechanism
5.x.1.1	Requirement	For each specific item determine and assess if the mechanism is required. Note: A mechanism might combine applicability and appropriateness in a single requirement.
5.x.1.2	Rationale	
5.x.1.3	Guidance	
5.x.1.4	Assessment criteria	
5.x.1.4.1	Assessment objective	
5.x.1.4.2	Required information	
5.x.1.4.3	Conceptual assessment	
5.x.1.4.4	Functional completeness assessment	
5.x.1.4.5	Functional sufficiency assessment	
5.x.2	XXX-2 Appropriate mechanisms	Appropriateness of the mechanism
5.x.2.1	Requirement	

Clause #	Title	Description on how to apply the standard
5.x.2.2	Rationale	For each specific item for which the mechanism is required as determined by XXX-1, determine and assess if the mechanism is implemented sufficiently. Note: A mechanism might have multiple appropriateness sub-clauses to focus on specific properties.
5.x.2.3	Guidance	
5.x.2.4	Assessment criteria	
5.x.2.4.1	Assessment objective	
5.x.2.4.2	Required information	
5.x.2.4.3	Conceptual assessment	
5.x.2.4.4	Functional completeness assessment	
5.x.2.4.5	Functional sufficiency assessment	
5.x.y	XXX-# Supporting Requirements	Applicability and appropriateness of supporting requirements for the mechanism
5.x.y.1	Requirement	For each specific item for which the mechanism is required as determined by XXX-1, determine and assess if the supporting requirement needs to be implemented (there might be specific conditions, for instance if the equipment is a toy) and if it needs to be implemented, whether it is implemented sufficiently.
5.x.y.2	Rationale	
5.x.y.3	Guidance	
5.x.y.4	Assessment criteria	
5.x.y.4.1	Assessment objective	
5.x.y.4.2	Required information	
5.x.y.4.3	Conceptual assessment	
5.x.y.4.4	Functional completeness assessment	
5.x.y.4.5	Functional sufficiency assessment	

The assessments are conducted by examining the documented assessment cases, not all assessment cases might be provided for every mechanism:

— Conceptual assessment

  Examine if the provided documentation and rationale adequately provides the required evidence (for example the rationale why a mechanism is not applicable for a specific network interface).

— Functional completeness assessment

  Examine and test if the provided documentation is complete (for example use network scanners to verify that all external interfaces are properly identified, documented and assessed)

— Functional sufficiency assessment

  Examine and test if the implementation is adequate (for example run fuzzing tools on a network interface to check if it is resilient to attacks with malformed data)

Each of the assessments is further divided into the following sub-clauses which might use a decision tree to guide the assessment:

— Assessment purpose

— Preconditions

— Assessment units

— Assignment of verdict

Required information lists the information that is to be provided through technical documentation. The standard does not require each required information element to be provided as a separate document.

5 Requirements

5.1 [ACM] Access control mechanism

5.1.1 [ACM-1] Applicability of access control mechanisms

5.1.1.1 Requirement

The equipment shall use access control mechanisms to manage entities access to security assets and network assets, unless for security or network assets where:

— Its full public accessibility is the “equipment’s reasonably foreseeable and intended use”; or

— the “foreseeable and intended operational environment of use” ensures that its accessibility is limited to authorized entities.

5.1.1.2 Rationale

Security and network assets are exposed to unauthorized access attempts. Access control mechanisms limit the ability of any unauthorized entity to access these assets.

5.1.1.3 Guidance

The requirement does not demand access control mechanisms on assets that it does not cover (for example, the dispense button on a coffee machine). Further it does not demand access control mechanisms for assets that are in principle covered, but where the reasonably foreseeable and intended use is to be generally accessible by the public or where the foreseeable and intended operational environment of use ensures that only authorized access is possible.

Note that radio interfaces might be accessible even if the equipment is in a trusted environment, for instance a wireless network is often accessible from outside a user’s home.

For example, depending on the equipment’s technical properties, foreseeable and intended use and foreseeable and intended operational environment of use access control mechanisms might not be necessary for relevant assets where:

— all entities with access to the equipment (the equipment is intended to be operated in an area which has physical access control) are authorized to access these assets (for example, the WPS button on a home router);

— the equipment’s functionality only provides information (on assets) that is intended to be publicly accessible (for instance broadcasting Bluetooth advertising beacons).

Access control mechanisms need properties to tie access rights to. Such properties can amongst others be:

— verified claims of entities (for instance being owner of a user account, member of specific group, authorized by another entity);

— certain states of the equipment or the equipment’s environment (for instance an electronic flight bag might have different access rights for a local user when it is operated in the air, then when it is stored at the ground);

— the interface an access is performed from (for instance a local access, where physical access control is obviously in place might have different access rights than a remote access);

— various combinations of these or other properties.

5.1.1.4 Assessment criteria

5.1.1.4.1 Assessment objective

The assessment addresses the requirement ACM-1.

5.1.1.4.2 Required information

[E.Doc.DT.ACM-1] Description of the selected path through the decision tree in Figure 1 for each security and network asset.

[E.Just.DT.ACM-1] Justification for the path through the decision tree in Figure 1 for each security and network asset.

[E.Doc.SecurityAsset] Documentation of each security asset.

[E.Doc.NetworkAsset] Documentation of each network asset.

[E.Doc.ACM] Documentation of all access control mechanisms that manage entities access for each security asset documented in [E.Doc.SecurityAsset] and each network asset documented in [E.Doc.NetworkAsset].

5.1.1.4.3 Conceptual assessment

5.1.1.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether access control mechanisms are implemented when it is required.

5.1.1.4.3.2 Preconditions

None

5.1.1.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each security and network asset;
if (Is the full public accessibility of the asset the\n"equipment’s reasonably foreseeable
and\nintended use?) then (Yes)
   #application :NOT APPLICABLE\nIntended use is fully\npublic;
   detach;
else (No)
   if (Does the "foreseeable and intended\noperational environment of use" ensure\nthat
accessibility to the asset is limited\nto authorized entities? ) then (Yes)
      #application :NOT APPLICABLE\nIntended environment\nprotects the asset;
      detach;
   else (No)
         if (<b>access control mechanism property:</b>\nAre there access control
mechanisms that\nmanage entities access to the security\nand network asset? ) then (Yes)
            #lightgreen :PASS\nAccess control\nmechanism needed\nand present;
            detach;
         else (No)
```

```
            #pink :FAIL\nAccess control\nmechanism needed\nbut not present;
            detach;
         endif
      endif
endif
@enduml
```

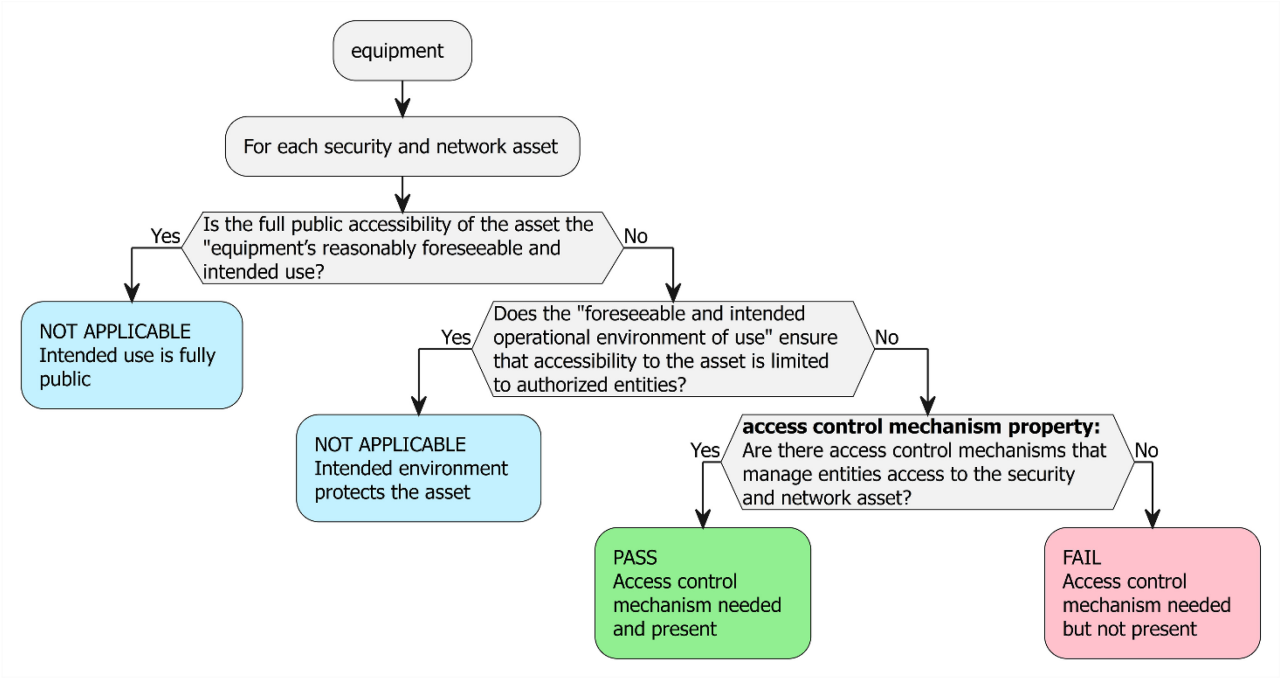

Figure 1 — Decision Tree for requirement ACM-1.

For each security asset documented in [E.Doc.SecurityAsset] and each network asset documented in [E.Doc.NetworkAsset], check whether the path through the decision tree documented in [E.Doc.DT.ACM-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.ACM-1], examine its justification documented in [E.Just.DT.ACM-1].

5.1.1.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.1.1.4.4 Functional completeness assessment

5.1.1.4.4.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of security and network assets is complete.

5.1.1.4.4.2 Preconditions

The equipment is in an operational state.

5.1.1.4.4.3 Assessment units

Functional assess whether there exist security assets, which are not documented in [E.Doc.SecurityAsset] and whether there exist network assets, which are not documented in [E.Doc.NetworkAsset].

5.1.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all security assets found are documented in [E.Doc.SecurityAsset] and all network assets found are documented in [E.Doc.NetworkAsset].

The verdict FAIL for the assessment case is assigned if a security asset is found which is not documented in [E.Doc.SecurityAsset] or a network asset is found which is not documented in [E.Doc.NetworkAsset].

5.1.1.4.5 Functional sufficiency assessment

5.1.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the access control mechanisms are implemented when they are required.

5.1.1.4.5.2 Preconditions

The equipment is in an operational state.

5.1.1.4.5.3 Assessment units

For each security asset documented in [E.Doc.SecurityAsset] and each network asset documented in [E.Doc.NetworkAsset], functionally confirm the existence of access control mechanisms according to [E.Doc.ACM].

5.1.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that access control mechanisms have not been implemented as described.

The verdict FAIL for the assessment case is assigned if there is evidence that access control mechanisms have not been implemented as described.

5.1.2 [ACM-2] Appropriate access control mechanisms

5.1.2.1 Requirement

For each security and network asset that is managed by access control mechanisms, the access control mechanisms shall ensure that only authorized entities have access to the managed security and network assets.

5.1.2.2 Rationale

Security and network assets may be exposed by unauthorized access attempts. Appropriate access control mechanisms ensure these assets are protected from unauthorized access.

5.1.2.3 Guidance

This requirement is intended to ensure that the access control mechanisms used to protect the relevant assets are chosen and configured such that unauthorized access is denied. With a variety of asset access methods and control mechanisms (for instance display on a wearable's screen), equipment use cases and operational environments, it is difficult to specify a generic model for entities and associated access rights.

Whether an access control mechanism can deny unauthorized access, always depends on external assumptions that need to be fulfilled. For example, that the sharing of passwords or unauthorized physical access are not permitted.

Depending on the equipment's technical properties, foreseeable and intended operational environment of use, the access control mechanisms use appropriate properties to tie access rights to and that these access rights are suitably distributed.

When access control mechanisms rely on authentication mechanisms, see AUM, for example

— an authorized entity, e.g., specific human, owner of a user account, device or service, can after authentication access their asset, such as changing security configuration,

— a member of specific authorized groups can after authentication access an asset or

— an entity, authorized by another entity authorized to so, can access a specific asset.

For the determination of access control mechanisms on assets the following aspects are important:

— the risk associated with an entity's access to an asset,

— the form of access an equipment's functionality allows to an asset,

— the interface the asset is accessed through and

— the impact of access control provided by the reasonably foreseeable and intended environment of use.

For the determination of entities' access rights on assets (authorized entities for certain access on assets), the following aspects are important:

— the risk associated with an entity's access to an asset,

— the "need-to-know principle": Does an entity need to get some information to an asset,

— the "need-to-use principle": Does an entity have a clear need to use a functionality based to an asset,

— the "least privileges principle": everything is forbidden unless permitted

— the equipment's clearly advertised functionality e.g., concerning accessibility of assets or interoperability with components of an existing infrastructure.

5.1.2.4 Assessment criteria

5.1.2.4.1 Assessment objective

The assessment addresses the requirement ACM-2.

5.1.2.4.2 Required information

[E.Doc.DT.ACM-2] Description of the selected path through the decision tree in Figure 2 for each security and network asset that is managed by access control mechanisms.

[E.Just.DT.ACM-2] Justification for the path through the decision tree in Figure 2 for each security and network asset that is managed by access control mechanisms.

NOTE A Justification includes a description of the entities, their access rights on the respective asset and means how the access control mechanisms ensures that only authorised access to the respective asset is granted.

[E.Doc.SecurityAsset] Documentation of each security asset.

[E.Doc.NetworkAsset] Documentation of each network asset.

[E.Doc.ACM] Documentation of all access control mechanisms that manage entities access for each security asset documented in [E.Doc.SecurityAsset] and each network asset documented in [E.Doc.NetworkAsset].

5.1.2.4.3 Conceptual assessment

5.1.2.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the access control mechanisms have the required properties.

5.1.2.4.3.2 Preconditions

None.

5.1.2.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each security and network asset that\nis managed by access control mechanisms;
    if (<b>access control mechanism property:</b>\nDo the access control mechanisms
ensure\nthat only authorized entities have access\nto the managed security and network
asset? ) then (Yes)
      #lightgreen :PASS\nAccess control mechanisms\nare appropriate;
      detach;
    else (No)
      #pink :FAIL\nAccess control mechanisms\nare not appropriate;
      detach;
    endif
@enduml
```

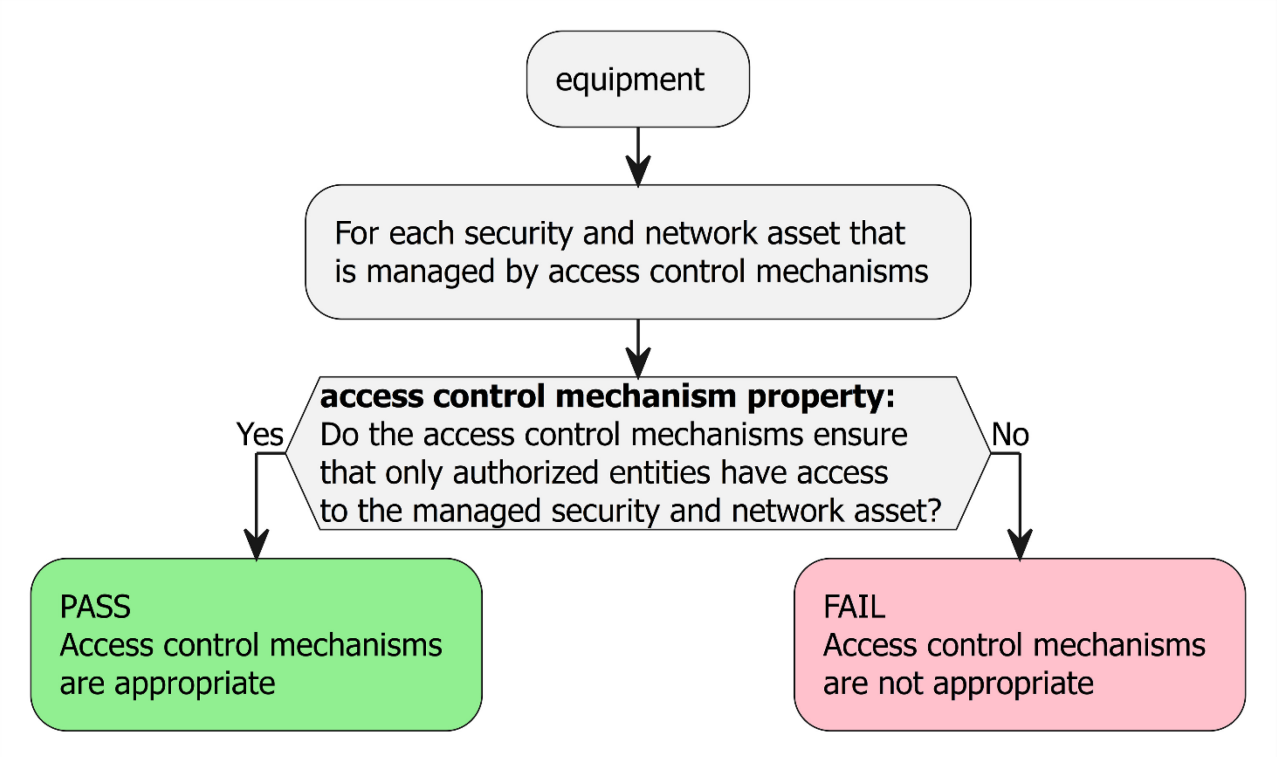

Figure 1 — Decision Tree for requirement ACM-2.

For each security asset documented in [E.Doc.SecurityAsset] and each network asset documented in [E.Doc.NetworkAsset] that is managed by access control mechanisms according to [E.Doc.ACM], check whether the path through the decision tree documented in [E.Doc.DT.ACM-2] ends with “PASS”.

For each path through the decision tree documented in [E.Doc.DT.ACM-2], examine its justification documented in [E.Just.DT.ACM-2].

5.1.2.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— all path through the decision tree ends with “PASS”; and

— all justifications are valid.

The verdict FAIL for the assessment case which is assigned otherwise.

5.1.2.4.4 Functional completeness assessment

None

5.1.2.4.5 Functional sufficiency assessment

5.1.2.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the access control mechanisms have the required properties.

5.1.2.4.5.2 Preconditions

The equipment is in an operational state.

5.1.2.4.5.3 Assessment units

For each security asset documented in [E.Doc.SecurityAsset] and each network asset documented in [E.Doc.NetworkAsset] that is managed by access control mechanisms according to [E.Doc.ACM], functionally confirm the access control mechanism properties in the justification provided in [E.Just.DT.ACM-2].

5.1.2.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that access control mechanism properties are not as described.

The verdict FAIL for the assessment case is assigned if there is evidence that access control mechanism properties are not as described.

5.2 [AUM] Authentication mechanism

In the context of the requirements in this section the formulation “provide access to” means that an interface is implemented to facilitate the usage of specific assets that are part of the equipment.

5.2.1 [AUM-1] Applicability of authentication mechanisms for external interfaces

5.2.1.1 [AUM-1-1] Requirement network interface

The equipment shall use at least one authentication mechanisms on each interface which is accessible via a network and its intended use is to provide access to network assets or equipment security assets, unless

— the interface requires the absence of authentication to be able to fulfil the interface’s intended function; or

— the equipment can only be operated in a trusted network which is logically or physically separated from untrusted networks.

5.2.1.2 [AUM-1-2] Requirement user interface

The equipment shall use at least one authentication mechanisms on each user interface that provides access to network assets or equipment security assets, unless the intended operational environment of use provides confidence in the correctness of an entity’s claim.

5.2.1.3 Rationale

The equipment needs to provide an authentication mechanism in combination with an access control mechanism to prevent successful attacks regarding the assets of the equipment and the misuse of the network resource. The authentication mechanism verifies that an entity is who or what it claims to be.

5.2.1.4 Guidance

In the context of the present clause the addressed interfaces provide paths to the assets covered by the requirement. Authentication mechanisms verify the validity of entities’ claims somewhere (e.g., application or network) along the path. The management of associated access rights for entities are part of the access control mechanism.

There are different kinds of entities that can interact with the equipment for example:

— a specific human, owner of a user account, device or service; or

— a member of specific groups such as an authorized group to access a specific equipment's resource; or

— authorised by another entity to access a specific equipment's resource.

Typically, the verification of an entity is based on examining evidence from one or more elements of the categories:

— knowledge (something you know); and

— possession (something you have); and

— inherence (something you are).

A trust relation to a network (e.g., an entity disposes a shared secret like Wi-Fi credentials) could be used to authenticate an entity.

Authentication might not be needed on all external interfaces, for instance interfaces that provide protocols which are intended to be accessible without authentication such as but not limited to DHCP and ICMP messages.

5.2.1.5 Assessment criteria network interface

5.2.1.5.1 Assessment objective

The assessment addresses the requirement AUM-1-1.

5.2.1.5.2 Required information

[E.Doc.DT.AUM-1-1] Description of the selected path through the decision tree in Figure 3 for each security and network asset.

[E.Just.DT.AUM-1-1] Justification for the path through the decision tree in Figure 3 for each security and network asset.

[E.Doc.NetworkInterfaces.AUM-1-1] Description of each interface that is accessible via network including the description of:

— The intended use of the interface

— Description of the functionality of the interface

(If given) [E.Doc.SecurityAsset.AUM-1-1] Documentation of each security asset that is accessible via network interfaces documented in [E.Doc.NetworkInterfaces.AUM-1-1].

(If given) [E.Doc.NetworkAsset.AUM-1-1] Documentation of each network asset that is accessible via network interfaces documented in [E.Doc.NetworkInterfaces.AUM-1-1].

[E.Doc.AUM-1-1] Documentation of the implemented authentication mechanisms on all network interfaces documented in [E.Doc.NetworkInterfaces.AUM-1-1].

[E.Doc.OperationalEnvironment] Description of the intended operational environment of use for the equipment.

5.2.1.5.3 Conceptual Assessment

5.2.1.5.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether an authentication mechanism is implemented when it is required to protect network assets or security assets.

5.2.1.5.3.2 Preconditions

None

5.2.1.5.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each network interface;
if (<b>Intended interface use</b>:\nDoes the interface provide \naccess to network assets
\nor security assets? ) then (Yes )
  if (<b>Intended environment</b>:\nIs the equipment logically \nor physically separated
\nfrom untrusted networks?) then (Yes )
  #application :NOT APPLICABLE \nUsed in a \nprotected \nenvironment;
  detach
  else (No)
          if (<b>Interface property</b>:\nDoes the interface require\n the absence of
authentication \nin order to fullfill its indended use? ) then (Yes )
           #application :NOT APPLICABLE \nAbsence of \nauthentication \nrequired;
           detach
    else (No)
      if (<b>Interface property</b>:\nDoes the interface use an \nauthentication
mechanism? ) then (Yes )
        #lightgreen :PASS;
        detach
      else (No)
        #pink :FAIL \nApplicable but not met;
        detach
      endif
    endif
  endif
else (No)
  #application :NOT APPLICABLE \nOut of scope;
  detach
endif
@enduml
```

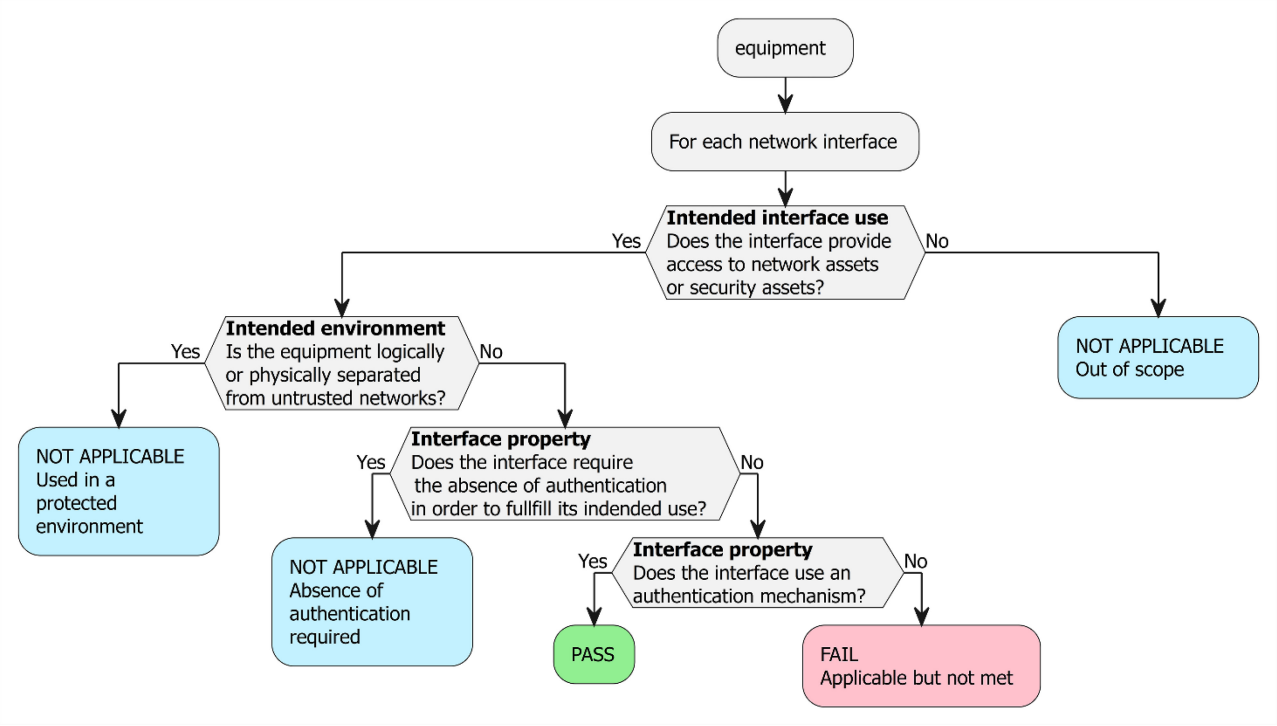

Figure 2 — Decision Tree for requirement AUM-1-1

For each network interface documented in [E.Doc.NetworkInterfaces.AUM-1-1] for the access of security assets documented in [E.Doc.SecurityAsset.AUM-1-1] and/or network assets documented in [E.Doc.NetworkAsset.AUM-1-1], the operational environment of use documented in [E.Doc.OperationalEnvironment] and the authentication mechanisms documented in [E.Doc.AUM-1-1], check whether the path through the decision tree documented in [E.Doc.DT.AUM-1-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.AUM-1-1], examine its justification documented in [E.Just.DT.AUM-1-1].

5.2.1.5.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.2.1.5.4 Functional completeness assessment

None.

5.2.1.5.5 Functional sufficiency assessment

None.

5.2.1.6 Assessment criteria user interface

5.2.1.6.1.1 Assessment objective

The assessment addresses the requirement AUM-1-2.

5.2.1.6.2 Required information

[E.Doc.DT.AUM-1-2] Description of the selected path through the decision tree shown Figure 4 for each security and network asset.

[E.Just.DT.AUM-1-2] Justification for the path through the decision tree shown Figure 4 for each security and network asset.

[E.Doc.UserInterfaces.AUM-1-2] Description of each interface that is accessible via network including the description of:

— The intended use of the interface

— Description of the functionality of the interface

(If given) [E.Doc.SecurityAsset.AUM-1-2] Documentation of each security asset that is accessible via user interfaces documented in [E.Doc.UserInterfaces.AUM-1-2].

(If given) [E.Doc.NetworkAsset.AUM-1-2] Documentation of each network asset that is accessible via user interfaces documented in [E.Doc.UserInterfaces.AUM-1-2].

[E.Doc.AUM-1-2] Documentation of the implemented authentication mechanisms on all user interfaces documented in [E.Doc.UserInterfaces.AUM-1-2].

[E.Doc.OperationalEnvironment] Description of the intended operational environment of use for the equipment.

5.2.1.6.3 Conceptual assessment

5.2.1.6.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms are implemented when they are required to protect network assets or security assets.

5.2.1.6.3.2 Preconditions

None.

5.2.1.6.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each user interface;
if (<b>Intended interface usage</b>:\nDoes the interface provide \naccess to network
assets \nand/or security assets? ) then (Yes )
  if (<b>Intended environment</b>:\nDoes the intended operational \nenvironment of use
provides \nconfidence in the correctness \nof an entity's claim? ) then (Yes )
```

```
  #application :NOT APPLICABLE \nUsed in a secure \noperational \nenvironment;
  detach
    else (No)
      if (<b>Interface property</b>:\nDoes the human \ninterface use an \nauthentication
\nmechanism? ) then (Yes )
        #lightgreen :PASS;
        detach
      else (No)
        #pink :FAIL \nApplicable but not met;
        detach
      endif
  endif
else (No)
  #application :NOT APPLICABLE \nOut of scope;
  detach
endif
@enduml
```

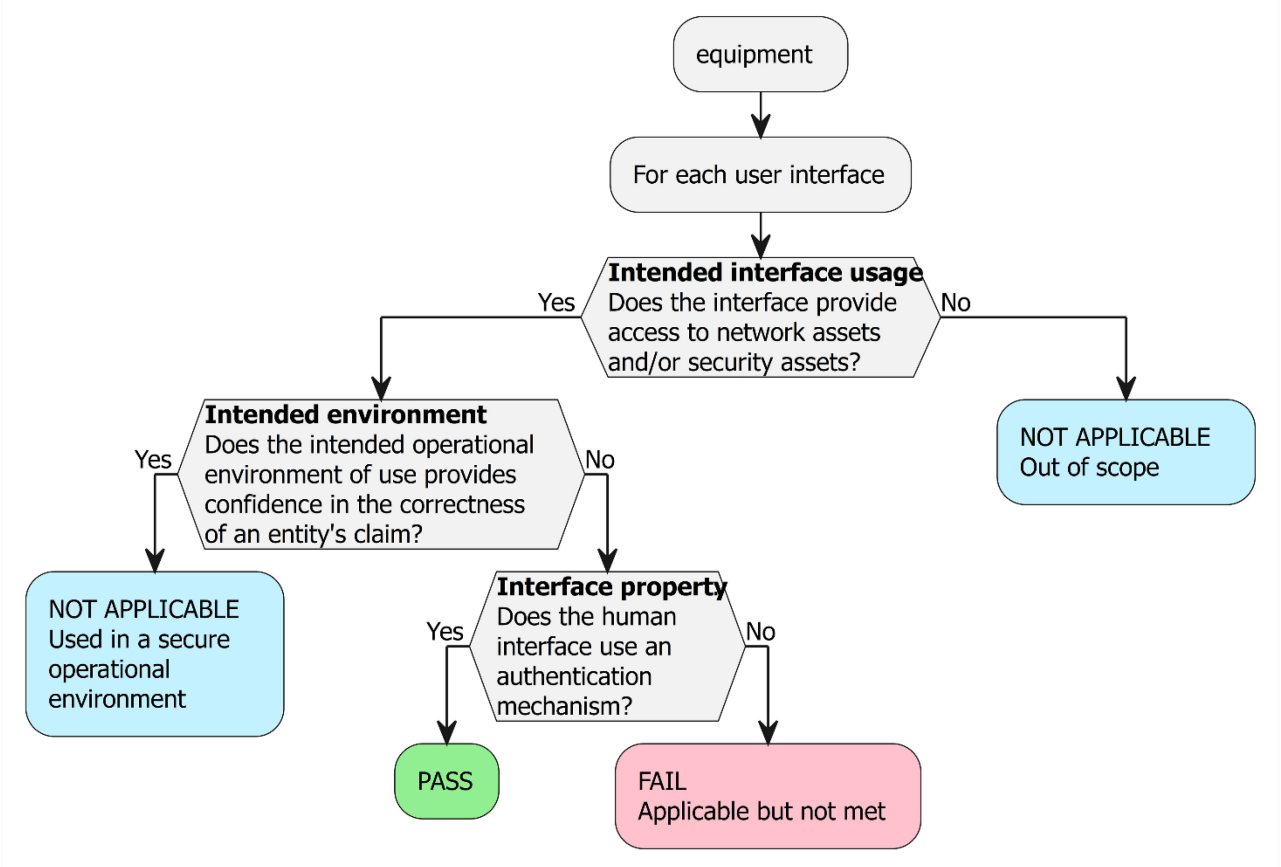

Figure 3 — Decision Tree for requirement AUM-1-2.

For each user interface documented in [E.Doc.UserInterfaces.AUM-1-2] for the access of security assets documented in [E.Doc.SecurityAsset.AUM-1-2] and/or network assets documented in [E.Doc.NetworkAsset.AUM-1-2], the operational environment of use documented in [E.Doc.OperationalEnvironment] and the authentication mechanisms documented in [E.Doc.AUM-1-2], check whether the path through the decision tree documented in [E.Doc.DT.AUM-1-2] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.AUM-1-2], examine its justification documented in [E.Just.DT.AUM-1-2].

5.2.1.6.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.2.1.6.4 Functional completeness assessment

None.

5.2.1.6.5 Functional sufficiency assessment

None.

5.2.2 [AUM-2] Appropriate authentication mechanisms for external interfaces

5.2.2.1 Requirement

For each access to security and/or network assets where an authentication mechanism is required due AUM-1-1 (network interface) or AUM-1-2 (user interface) at least one authentication mechanism shall verify an entity’s claim based on examining evidence from at least one element of the categories, knowledge, possession and inherence (one factor authentication).

5.2.2.2 Rationale

One factor authentication is suitable to protect the network resources of an equipment against misuse, e.g., as part of a DoS attack. Further, personal data on the equipment need to be protected with at least one factor authentication in particular against manipulation and theft.

When the primary use of the equipment is to specifically process sensitive data a higher need of protection is given because the disclosure could have serious consequences. In this case at least two factor authentication is required. Equipment which general purpose is to proceed any data which only could possibly include sensitive personal data such as desktop pcs, smartphones, cameras or printers needs only foresee protection for personal data. Generally, when designing equipment to store personal data, it is reasonable to consider providing multifactor authentication.

5.2.2.3 Guidance

Examples for a verification of an entity’s claim based on examining evidence from one element of the categories, knowledge, possession and inherence, are:

— PIN-Code used for user interface

— 1-Factor (e.g., password based) of each incoming connection on an interface

Trust relation to a network (e.g., based on a common secret) established at on-boarding

Examples for a verification of an entity's claim based on examining evidence from at least two different elements of the categories, knowledge, possession and inherence, are:

— Password + OTP

— PIN + Smartcard

— Password + Token

Considering possible constraints of human users with disabilities is an important aspect for implementing appropriate authentication mechanisms.

Currently long passwords like "Weihnachtsmarkt2023@Bonn" are considered better passwords than short passwords like "P@ssw0rd!".

More guidance on best practice on passwords can be found in NIST Special Publication 800-63B [8], ISO/IEC EN 27002:2022 [3], ISO/IEC EN 24760 [4], IEC EN 62443-4-2 [2] and ETSI EN 303 645 [5]

5.2.2.4 Assessment criteria

5.2.2.4.1 Assessment objective

The assessment addresses the requirement AUM-2.

5.2.2.4.2 Required information

[E.Doc.DT.AUM-2] Description of the selected the path through the decision tree in Figure 5 for each authentication mechanism affecting security and/or network assets.

[E.Just.DT.AUM-2] Justification for the selected path through the decision tree in Figure 5 for each authentication mechanism protecting security and/or network assets.

[E.Doc.SecurityAsset.AUM-2] Documentation of each security asset that is accessible via network interfaces and/or user interfaces.

[E.Doc.NetworkAsset.AUM-2] Documentation of each network asset that is accessible via network interfaces and/or user interfaces.

[E.Doc.AUM] Description of all authentication mechanisms for each path to access security assets documented in [E.Doc.SecurityAsset.AUM-2] and/or network assets documented in [E.Doc.NetworkAsset.AUM-2], including all network interfaces and/or user interfaces.

5.2.2.4.3 Conceptual assessment

5.2.2.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether all authentication mechanism on each path to security and/or network assets have the required properties.

5.2.2.4.3.2 Preconditions

None.

5.2.2.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  : For each access to security and/or network assets;
    if (<b>authentication mechanism property:</b>\nDoes at least one authentication
mechanism on the path use \nat least one factor authentication to verify an entities'
claim?) then (Yes)
      #lightgreen :PASS\nAuthentication mechanisms\nare appropriate;
      detach;
    else (No)
      #pink :FAIL\nAuthentication mechanisms\nare not appropriate;
      detach;
    endif
@enduml
```

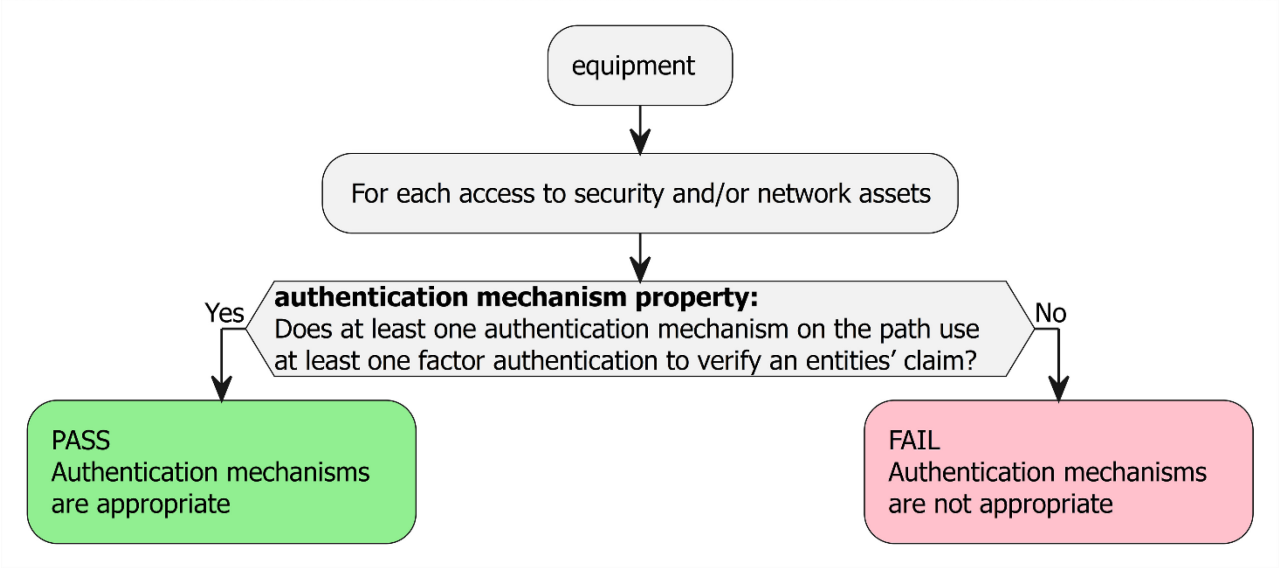

Figure 4 — Decision Tree for requirement AUM-2

For each authentication mechanism documented in [E.Doc.AUM], check whether the path through the decision tree documented in [E.Doc.DT.AUM-2] ends with "PASS".

For each path through the decision tree documented in [E.Doc.DT.AUM-2], examine its justification documented in [E.Just.DT.AUM-2].

5.2.2.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— all paths through the decision tree end with "PASS"; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— no authentication mechanisms for protection of security and/or network assets is required.

The verdict FAIL for the assessment case is assigned otherwise.

5.2.2.4.4 Functional completeness assessment

5.2.2.4.4.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of authentication mechanisms is complete.

5.2.2.4.4.2 Preconditions

The equipment is in an operational state.

5.2.2.4.4.3 Assessment units

Functional assess whether there exist authentication mechanisms, which are not listed in [E.Doc.AUM].

5.2.2.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all authentication mechanisms found are documented in [E.Doc.AUM].

The verdict FAIL for the assessment case is assigned if one authentication mechanism found is not documented in [E.Doc.AUM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.2.2.4.5 Functional sufficiency assessment

5.2.2.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether at least one authentication on each path to network or security assets has the required properties.

5.2.2.4.5.2 Preconditions

The equipment is in an operational state.

5.2.2.4.5.3 Assessment units

For each authentication mechanism documented in [E.Doc.AUM], functionally confirm the operation of the authentication mechanism as documented in [E.Doc.AUM].

5.2.2.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that the authentication mechanisms deviate from [E.Doc.AUM].

The verdict FAIL for the assessment case is assigned if there is evidence that the authentication mechanisms deviate from [E.Doc.AUM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.2.3 [AUM-3] Authenticator validation

5.2.3.1 Requirement

Each authentication mechanism subject to AUM-1 shall validate all relevant properties of the used authenticators, dependent on the information available in the operational environment of use.

5.2.3.2 Rationale

Even when the equipment provides an authentication mechanism, the risk is given that an attacker uses typical design weakness to overcome it. The usage of forged or partially forged authenticators builds a typical attack against such a mechanism. Therefore, the security design of the mechanisms needs techniques to resist forged authenticators, for example manipulated PKI certificates.

5.2.3.3 Guidance

The authenticator and its attributes may vary depending on the authentication mechanism. For the validation of the authenticator, best practice ought to be applied which is typically described in a standard for the corresponding authentication protocol. This is necessary in order to detect and prevent the use of an authenticator that has been forged. For example if the equipment only text matches the common name of a PKI certificate without further validation of the complete certificate information, then a correspondingly forged authenticator would be accepted. In this example, the relevant property would be the signatures and public keys of the trust chain, and in many cases also the validity of the certificate. The set of relevant properties may differ depending on whether the equipment is actually internet connected or not. For example, offline equipment may not have access to a reliable time source or to certificate revocation information.

Another example is if passwords are only partially validated. This would weaken the strength of the password, facilitating brute force attacks on the corresponding authentication mechanism.

5.2.3.4 Assessment criteria

5.2.3.4.1 Assessment objective

The assessment addresses the requirement AUM-3.

5.2.3.4.2 Required information

[E.Doc.DT.AUM-3] Description of the selected the path through the decision tree in Figure 6 for each authentication mechanism.

[E.Just.DT.AUM-3] Justification for the selected path through the decision tree in Figure 6 for each authentication mechanism.

[E.Doc.AUM] Description of all authentication mechanisms for each path to access security and network assets including user interface and network interfaces.

[E.Doc.AuthVal] Description for all authentication mechanisms how the validation of the authenticator is performed considering the available information about the authenticator in the operational environment of use.

5.2.3.4.3 Conceptual assessment

5.2.3.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms on each path to security and/or network assets have the required properties.

5.2.3.4.3.2 Preconditions

None.

5.2.3.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each path to security and network assets;
    if (<b>authentication mechanism property</b>:\nDoes the authentication mechanism
validate all relevant properties \nconsidering the available information about the
authenticator in \nthe operational environments of use?) then (Yes)
      #lightgreen :PASS\nAuthenticator validation \nis appropriate;
      detach;
    else (No)
      #pink :FAIL\nAuthenticator validation \nis inappropriate;
      detach;
    endif
@enduml
```

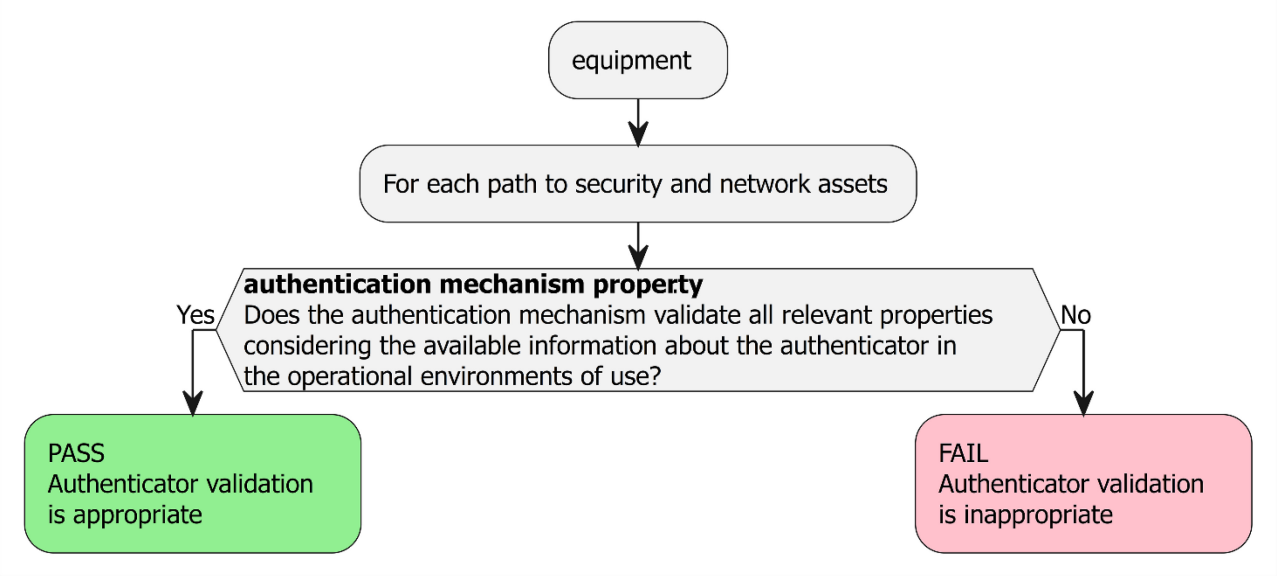

Figure 5 — Decision Tree for requirement AUM-3.

For each authentication mechanism documented in [E.Doc.AUM], check whether the path through the decision tree documented in [E.Doc.DT.AUM-3] ends with “PASS”.

For each path through the decision tree documented in [E.Doc.DT.AUM-3], examine its justification documented in [E.Just.DT.AUM-3].

5.2.3.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— all paths through the decision tree end with “PASS”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— no authentication mechanisms for protection of network and/or security assets is required (see 5.2.1).

The verdict FAIL for the assessment case is assigned otherwise.

5.2.3.4.4 Functional completeness assessment

5.2.3.4.4.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of authentication mechanisms is complete.

5.2.3.4.4.2 Preconditions

The equipment is in an operational state.

5.2.3.4.4.3 Assessment units

Functional assess whether there exist authentication mechanisms, which are not listed in [E.Doc.AUM].

5.2.3.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all authentication mechanisms found are documented in [E.Doc.AUM].

The verdict FAIL for the assessment case is assigned if one authentication mechanism found is not documented in [E.Doc.AUM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.2.3.4.5 Functional sufficiency assessment

5.2.3.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether at the authentication mechanism on each path to network and/or security assets have the required properties.

5.2.3.4.5.2 Preconditions

The equipment is in an operational state.

5.2.3.4.5.3 Assessment units

For each authentication mechanism documented in [E.Doc.AUM], functionally confirm the operation of the authenticator validation as documented in [E.Doc.AuthVal].

5.2.3.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that the validation of the authenticator deviates from [E.Doc.AuthVal].

The verdict FAIL for the assessment case is assigned if there is evidence that the validation of the authenticator deviates from [E.Doc.AuthVal].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.2.4 [AUM-4] Changing authenticators

5.2.4.1 Requirement

Each authentication mechanism which is subject to AUM-1 shall allow for changing the authenticator unless conflicting security goals do not allow for a change.

5.2.4.2 Rationale

Unchangeable authenticators build a risk for the secure operation of the equipment, e.g. increases the vulnerability to brute force and eavesdropping attacks. Therefore, the support for changing authenticators on the equipment is needed as a countermeasure.

5.2.4.3 Guidance

An authorised entity needs the possibility to change the authenticator. The procedure may vary depending on the authentication mechanism used.

— The equipment provides a functionality to the authorised entity, e.g. user, to change the authenticator on the equipment.

— The authenticator, e.g. token, is renewed or changed by the manufacturer and the equipment accepts the changed authenticator because the trust chain is still valid.

— The authenticator is updated using a secure update mechanism.

For machine interfaces, for example, a new pairing may be required. For user interfaces whether for example a fingerprint, password or other token is used, the integration of the functionality into the normal workflow facilitates the simple implementation.

There may be exceptions where an authenticator is static for example a root of trust where the confidentiality of the corresponding cryptographic key is ensured by the manufacturer. In such an example the manufacturer typically provides tokens to authorized entities that are all linked to the same root of trust.

There may be exceptions, where the overall risk of changing an authenticator, e.g. due to complexity, is higher than the risk associated to the assets while using static authenticators. In such a case “best practice security design principles” ought to be taken into account to minimize the risk associated with the static authenticator, e.g., by not using global authenticators.

Depending on the intended use of the equipment it might be needed to ensure the availability of the equipment functionality due a deferral option, e.g., not forcing the update of a password whilst driving a car.

5.2.4.4 Assessment criteria

5.2.4.4.1 Assessment objective

The assessment addresses the requirement AUM-4.

5.2.4.4.2 Required information

[E.Doc.DT.AUM-4] Description of the selected path through the decision tree in Figure 7 for each authenticator change functionality.

[E.Just.DT.AUM-4] Justification for the selected path through the decision tree in Figure 7 for each authenticator change functionality.

[E.Doc.AUM] Description of all authentication mechanisms for each path to access security and network assets including user interface and network interfaces.

[E.Doc.AuthChange] Description for all authentication mechanisms how the change of the authenticator is performed under consideration of the security concept of the equipment.

5.2.4.4.3 Conceptual assessment

5.2.4.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms on each path to security and/or network assets have the required properties.

5.2.4.4.3.2 Preconditions

None

5.2.4.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each path to security and/or network assets;
    if (<b>Equipment security concept:</b>\nDoes the change of the authenticatior
\nconflict security goals?) then (Yes)
    #application:NOT APPLICABLE\nStatic for security reasons;
    detach;
    else(No)
    if (<b>Authentication mechanism property:</b>\nDoes the authentication mechanism allow
\nthe change of the authenticator?) then (Yes)
      #lightgreen :PASS\nAuthenticator changeable;
      detach;
    else (No)
      #pink :FAIL\nAuthenticator not changeable;
      detach;
    endif
@enduml
```

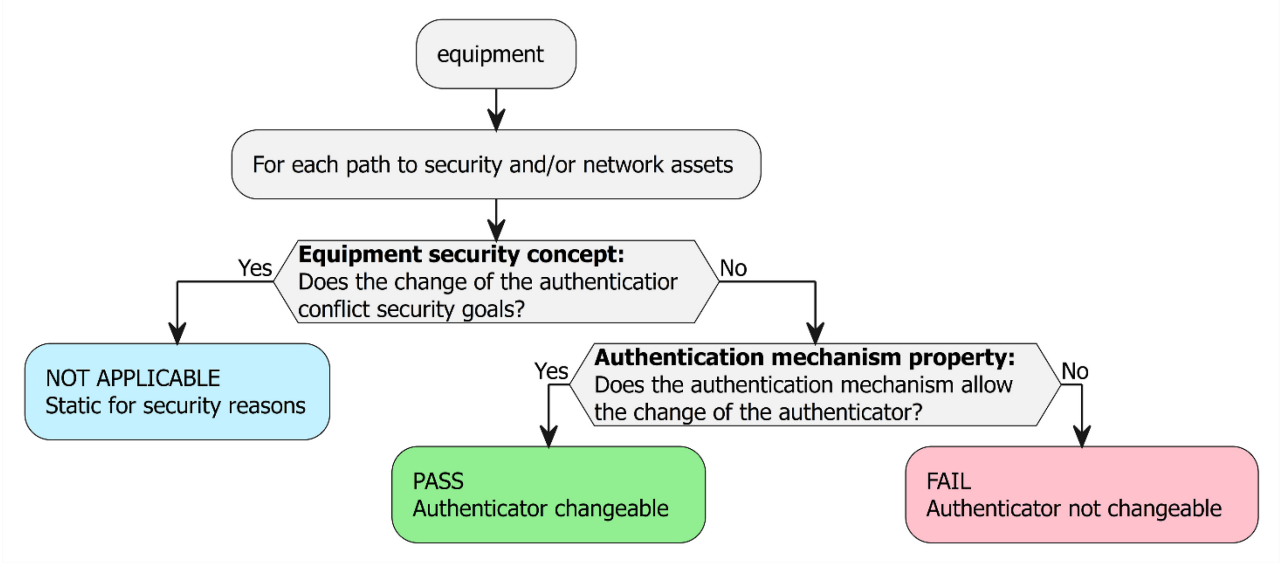

Figure 6 — Decision Tree for requirement AUM-4.

For each authenticator change functionality documented in [E.Doc.AUM], check whether the path through the decision tree documented in [E.Doc.DT.AUM-4] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.AUM-4], examine its justification documented in [E.Just.DT.AUM-4].

5.2.4.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— all paths through the decision tree end with “PASS”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— no authentication mechanisms for protection of network and/or security assets is required (see 5.2.1).

The verdict FAIL for the assessment case is assigned otherwise.

5.2.4.4.4 Functional completeness assessment

5.2.4.4.4.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of authentication mechanisms is complete.

5.2.4.4.4.2 Preconditions

The equipment is in an operational state.

5.2.4.4.4.3 Assessment units

Functional assess whether there exist authentication mechanisms, which are not listed in [E.Doc.AUM].

5.2.4.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all authentication mechanisms found are documented in [E.Doc.AUM].

The verdict FAIL for the assessment case is assigned if one authentication mechanism found is not documented in [E.Doc.AUM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.2.4.4.5 Functional sufficiency assessment

5.2.4.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether at the authentication mechanism on each path to network and/or security assets have the required properties.

5.2.4.4.5.2 Preconditions

The equipment is in an operational state.

5.2.4.4.5.3 Assessment units

For each authentication mechanism documented in [E.Doc.AUM], functionally confirm the change of authenticator as documented in [E.Doc.AuthChange].

5.2.4.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that the change of the authenticator deviates from [E.Doc.AuthChange].

The verdict FAIL for the assessment case is assigned if there is evidence that the change of the authenticator deviates from [E.Doc.AuthChange].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.2.5 [AUM-5] Preventing static and default values

5.2.5.1 Requirement

If passwords are used by an authentication mechanism subject to AUM-1-2 they shall:

— Be practically unique per equipment in case of factory default or

— if the equipment is logically or physically separated from untrusted networks be enforced to be set by the user on first use and

— in any case follow best practice concerning strength.

NOTE Passwords include pin codes.

5.2.5.2 Rationale

Universal passwords represent one of the most exploited attack vectors for equipment. A wide range of malware exists that uses such passwords to automatically compromise equipment. Therefore, the usage of equipment individual passwords is essential on first use.

5.2.5.3 Guidance

There exists a variety of techniques to avoid universal passwords, examples are:

— The equipment password for the factory default state is printed on a sticker under the equipment casing. The password is created by using a hardware random generator or another cryptographically secure pseudorandom number generator (CSPRNG) implementation.

— The equipment prompts a user to create a password on the first use

Guidance on best practice on passwords can be found in NIST Special Publication 800-63B [8],

ISO/IEC EN 27002:2022 [3], ISO/IEC EN 24760 [4], IEC EN 62443-4-2 [2] and ETSI EN 303 645 [5]

Unique relates to not systematically reused or deducible for another equipment of the same product type and cannot be easily derived from equipment properties (e.g. manufacturer name, model name or Media Access Control (MAC) address). Established random generator can be used to generate practically unique passwords.

When forcing a password to be changed, also safety aspects are relevant. e.g., don't force changing a password while driving a car.

5.2.5.4 Assessment criteria

5.2.5.4.1 Assessment objective

The assessment addresses the requirement AUM-5.

5.2.5.4.2 Required information

[E.Doc.DT.AUM-5] Description of the selected the path through the decision tree in Figure 8 for each authentication mechanism.

[E.Just.DT.AUM-5] Justification for the selected path through the decision tree in Figure 8 for each authentication mechanism.

[E.Doc.AUM] Description of all authentication mechanisms for each path to access security and network assets including user interface and network interfaces.

[E.Doc.PwdProperty] Description for all authentication mechanisms which uses passwords how practically uniqueness is implemented for the password or the change of the password is enforced on first use. The documentation also contains the parameter of the followed password strength.

5.2.5.4.3 Conceptual assessment

5.2.5.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms on each path to security and/or network assets have the required properties.

5.2.5.4.3.2 Preconditions

None

5.2.5.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
    if (<b>Equipment property:</b>\nAre passwords used?) then (Yes)
     :For each path to security and network assets;
     if (<b>Password property:</b>\nIs the password practically \nunique per equipment
\nin factory default) then (Yes)
      #lightgreen :PASS\nPassword is \npractically unique;
      detach;
     else(No)
      if(<b>Operational environment:</b>\nEquipment is logically \nor physically separated
\nfrom untrusted networks?) then (No)
       #pink :FAIL\nInappropriate \nenvoirnment;
       detach;
      else(Yes)
       if(<b>AuthMech property:</b>\nIs setting a new \npassword enforced \non first use?)
then (Yes)
        #lightgreen :PASS\nSetting of a \nnew password is \nenforced on first use;
        detach;
       else(No)
        #pink :FAIL\nSetting of a \nnew password is \nenforced on first use;
        detach;
       endif
      endif
     endif
     detach;
    else(No)
    #application:NOT APPLICABLE\nNo passwords used;
    detach;
    endif
@enduml
```

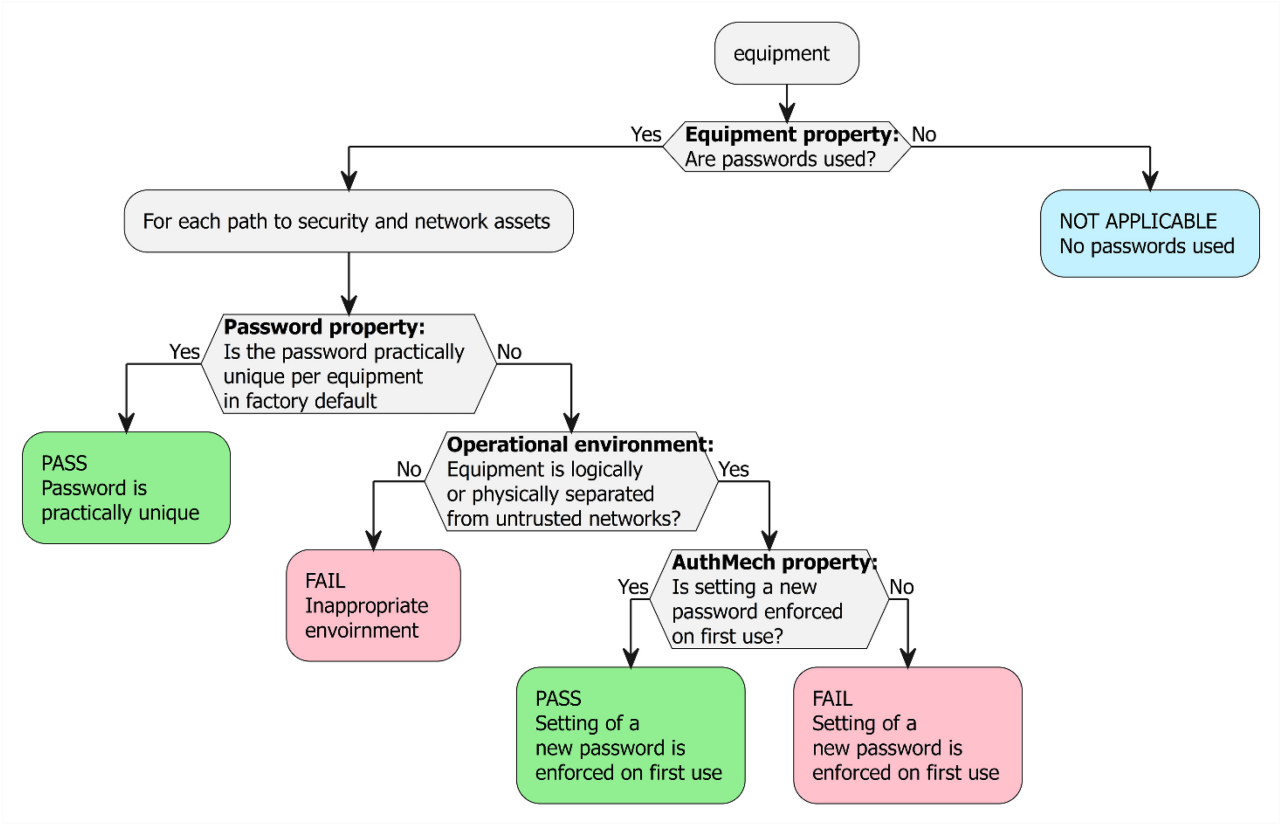

Figure 7 — Decision Tree for requirement AUM-5.

For each authentication mechanism documented in [E.Doc.AUM], check whether the path through the decision tree documented in [E.Doc.DT.AUM-5] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.AUM-5], examine its justification documented in [E.Just.DT.AUM-5].

5.2.5.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— all paths through the decision tree end with “PASS”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— no authentication mechanisms for protection of network and/or security assets is required (see AUM-1).

The verdict FAIL for the assessment case is assigned otherwise.

5.2.5.4.4 Functional completeness assessment

5.2.5.4.4.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of authentication mechanisms is complete.

5.2.5.4.4.2 Preconditions

The equipment is in an operational state.

5.2.5.4.4.3 Assessment units

Functional assess whether there exist authentication mechanisms, which are not listed in [E.Doc.AUM].

5.2.5.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all authentication mechanisms found are documented in [E.Doc.AUM].

The verdict FAIL for the assessment case is assigned if one authentication mechanism found is not documented in [E.Doc.AUM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.2.5.4.5 Functional sufficiency assessment

5.2.5.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether at the authentication mechanism on each path to network and/or security assets have the required properties.

5.2.5.4.5.2 Preconditions

The equipment is in an operational state.

5.2.5.4.5.3 Assessment units

For each authentication mechanism that uses passwords documented in [E.Doc.AUM], functionally confirm the password properties and associated functionalities are as documented in [E.Doc.PwdProperty].

5.2.5.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that the validation of the authenticator deviates from [E.Doc. PwdProperty].

The verdict FAIL for the assessment case is assigned if there is evidence that the validation of the authenticator deviates from [E.Doc. PwdProperty].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.2.6 [AUM-6] Brute force protection

5.2.6.1 Requirement

The equipment shall be resilient against brute force attacks to the authentication mechanisms subject to AUM-1.

5.2.6.2 Rationale

An attacker can try to use mass authentication attempts to overcome an authentication mechanism or to impact equipment availability. Therefore, techniques are required to mitigate such an attack.

5.2.6.3 Guidance

There exists a variety of techniques which aim to make successful brute force attacks impracticable.

Example techniques used to reduce the likelihood of a successful brute force attack include:

— Time delays between consecutive failed attempts to authenticate.

— A limited number of failed authentication attempts, followed by a suspension period where no login is allowed.

— Multi-factor authentication.

— Appropriate entropy for authentication values based on best practice cryptography.

NOTE An appropriate entropy is represented by the length and content of the value under consideration of the possible character set and the number of attempts before brute force prevention is activated.

— Depending on the implemented techniques related risks concerning "resource exhaustion" and “denial of service” need to be considered.

Consideration is to be given to defending against repeated attempts to gain illegitimate authentication and defending against blocking of legitimate access by triggering the preceding defence mechanism.

See NIST 800-63 series [7].

5.2.6.4 Assessment criteria

5.2.6.4.1 Assessment objective

The assessment addresses the requirement AUM-6.

5.2.6.4.2 Required information

[E.Doc.DT.AUM-6] Description of the selected the path through the decision tree in Figure 9 for each authentication mechanism.

[E.Just.DT.AUM-6] Justification for the selected path through the decision tree in Figure 9 for each authentication mechanism.

[E.Doc.AUM] Description of all authentication mechanisms for each path to access security and network assets including user interface and network interfaces.

[E.Doc.BFProtection] Description for all authentication mechanisms how the resilience against brute force attacks is ensured.

5.2.6.4.3 Conceptual assessment

5.2.6.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms on each path to security and/or network assets have the required properties.

5.2.6.4.3.2 Preconditions

None.

5.2.6.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each path to security and/or network assets;
    if (<b>Authentication mechanism property:</b>\nIs the authentication mechanism
\nresilient against brute force attacks?) then (Yes)
      #lightgreen :PASS\nIs resilient ;
      detach;
    else (No)
      #pink :FAIL\nIs not resilient;
      detach;
    endif
@enduml
```

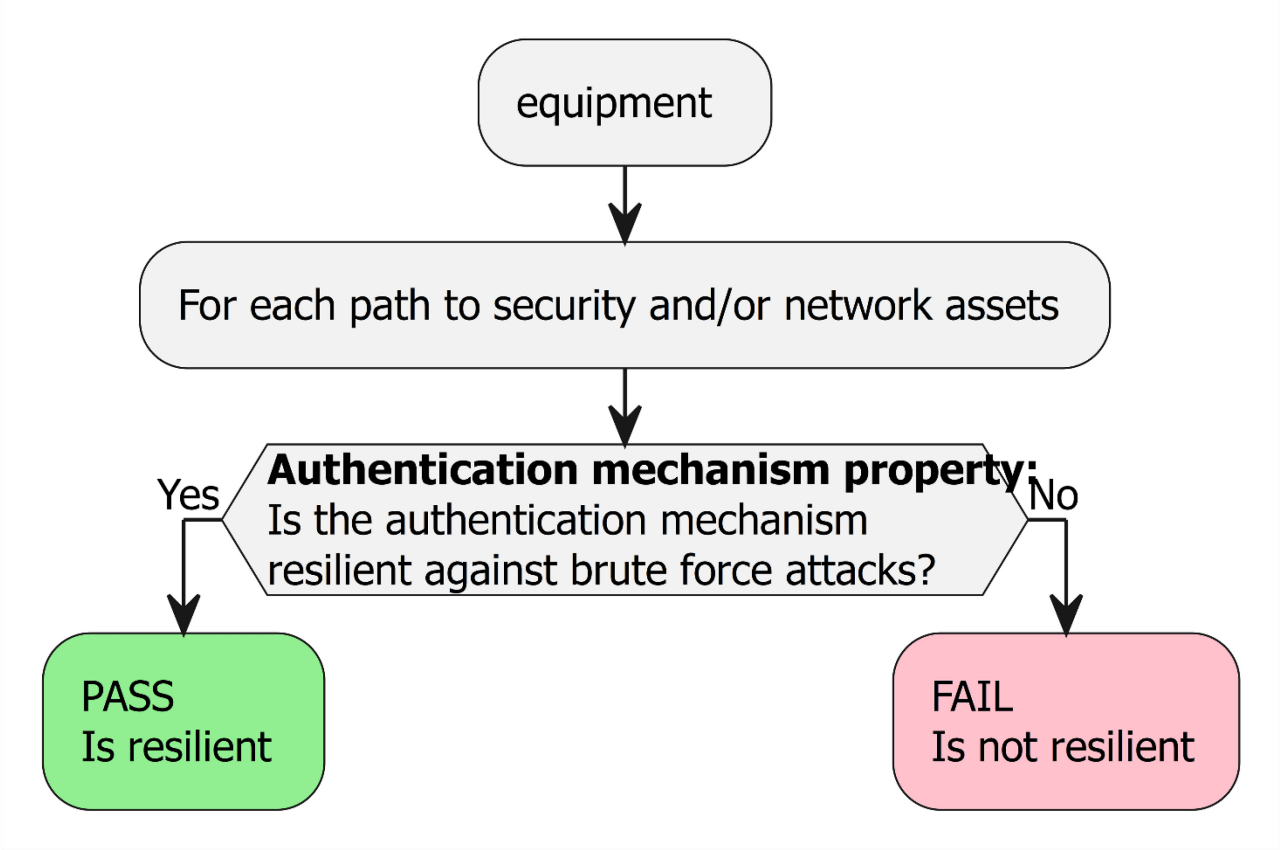

Figure 8 — Decision Tree for requirement AUM-6.

For each authentication mechanism documented in [E.Doc.AUM], check whether the path through the decision tree documented in [E.Doc.DT.AUM-6] ends with “PASS”.

For each path through the decision tree documented in [E.Doc.DT.AUM-6], examine its justification documented in [E.Just.DT.AUM-6].

5.2.6.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— all paths through the decision tree end with “PASS”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— no authentication mechanisms for protection of network and/or security assets is required (see 5.2.1).

The verdict FAIL for the assessment case is assigned otherwise.

5.2.6.4.4 Functional completeness assessment

5.2.6.4.4.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of authentication mechanisms is complete.

5.2.6.4.4.2 Preconditions

The equipment is in an operational state.

5.2.6.4.4.3 Assessment units

Functional assess whether there exist authentication mechanisms, which are not listed in [E.Doc.AUM].

5.2.6.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all authentication mechanisms found are documented in [E.Doc.AUM].

The verdict FAIL for the assessment case is assigned if one authentication mechanism found is not documented in [E.Doc.AUM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.2.6.4.5 Functional sufficiency assessment

5.2.6.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether at the authentication mechanism on each path to network and/or security assets have the required properties.

5.2.6.4.5.2 Preconditions

The equipment is in an operational state.

5.2.6.4.5.3 Assessment units

For each authentication mechanism documented in [E.Doc.AUM], functionally confirm the resilience against brute force attacks (compare section 5.2.6.3) [E.Doc.BFProtection].

5.2.6.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no indication that the brute force protection deviates from [E.Doc.BFProtection].

The verdict FAIL for the assessment case is assigned if there is evidence that the brute force protection deviates from [E.Doc.BFProtection].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.3 [SUM] Secure update mechanism

5.3.1 [SUM-1] Applicability of update mechanisms

5.3.1.1 Requirement

The equipment shall provide at least one update mechanism for updating each part of its software affecting security and/or network assets, unless:

— functional safety implications do not allow updatability; or

— the software is immutable for security reasons; or

— alternative measures exist that protect security assets and/or network assets during the entire lifecycle of the equipment.

If the above exceptions affect all the equipment's software, no update mechanism is required.

5.3.1.2 Rationale

Being able to provide and deploy software updates via update mechanism is an essential capability to keep the equipment well maintained and mitigate security vulnerabilities that, if exploited, may be used to compromise the equipment and thus may harm the network or its functioning or misusing network resources, thereby causing an unacceptable degradation of service.

However, some parts of software might be immutable and therefore not updatable for security reasons or functional safety implications do not allow their updatability. Vulnerabilities might also be mitigated by alternative measures, such as exchanging vulnerable equipment throughout the entire life cycle or being securely mitigated by other equipment that ensures the protection of the asset.

5.3.1.3 Guidance

There might be more than one update mechanism for different parts of the equipment’s software.

Not all software on the equipment may be updatable. This may include software in read only memory for security reasons or in order to satisfy functional safety requirements.

There are cases where alternative measures exist to prevent harm from potential publicly known exploitable vulnerabilities in parts of the equipment’s software or where an exploitable vulnerability in its software might not endanger the equipment’s integrity or the assets to be protected. For instance:

— Equipment having a replacement strategy, e.g., for equipment with limited resources such as sensors that would have to work on battery for many years; or

— Equipment or parts of software, which can and are foreseen to be securely isolated within the equipment’s intended use; or

— parts of software running with restricted privileges which do not endanger the assets being protected; or

— (parts of) software where the equipment’s intended use and intended operational environment of use, mitigate the exploit of any vulnerability.

Where it is possible, it is good practice to implement a software update mechanism that allows for separate security related software updates and application software updates.

5.3.1.4 Assessment criteria

5.3.1.4.1 Assessment objective

The assessment addresses the requirement SUM-1.

5.3.1.4.2 Required information

[E.Doc.DT.SUM-1] Description of the selected path through the decision tree in Figure 10 for each part of the software.

[E.Just.DT.SUM-1] Justification for the selected path through the decision tree in Figure 10 for each part of the software.

[E.Doc.PartOfSoftw] Documentation of each of the equipment's part of the software.

NOTE: The present document does not determine the granularity of the separation of the equipment's software into parts. A suitable separation with respect to efforts in documentation considers the coverage of the parts of the software by certain update mechanisms.

If the equipment provides an update mechanism for updating parts of its software affecting security and/or network assets: [E.Doc.SUM] Complete Documentation of update mechanisms for updating parts of the equipment's software affecting security and/or network assets.

5.3.1.4.3 Conceptual assessment

5.3.1.4.3.1 Assessment purpose

The purpose of this assessment case is to determine whether an update mechanism is implemented when it is required.

5.3.1.4.3.2 Preconditions

The equipment must be in operational state.

5.3.1.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each part of the equipment's software;
if (<b>software part property:</b>\nDoes the part of the software affect security and/or
network assets? ) then (Yes)
    if (Do functional safety implications prohibit updatability?) then (Yes)
        #application :NOT APPLICABLE\nFunctional safety implications;
        detach;
    else (No)
       if (Is the software is immutable for security reasons?) then (Yes)
           #application :NOT APPLICABLE\nImmutable for security;
           detach;
       else (No)
          if (Do alternative measures exist that protect security\nassets and/or network
assets during the entire lifecycle?) then (Yes)
             #application :NOT APPLICABLE\nAlternative measures;
             detach;
          else (No)
      if (<b>software part property:</b>\nDoes the equipment provide at least\none update
mechanism for updating\nthe part of the software? ) then (No)
        #pink :FAIL\nSoftware is not updatable;
```

```
        detach;
      else (Yes)
        #lightgreen :PASS\nSoftware is updatable;
        detach;
      endif
          endif
       endif
    endif
else
     #application :NOT APPLICABLE\nSoftware does not \naffect asset;
     detach;
endif
@enduml
```

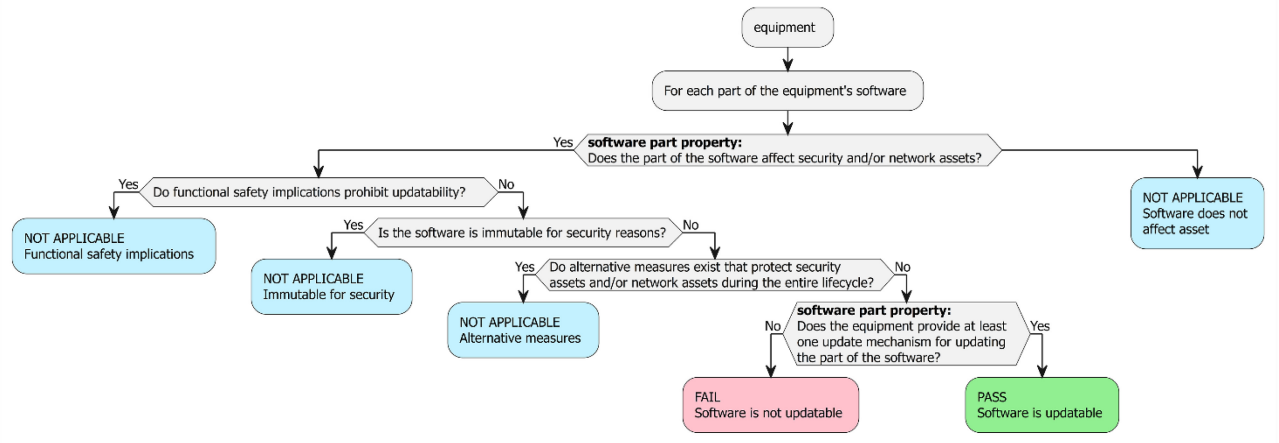

Figure 9 — Decision Tree for requirement SUM-1.

For each part of the software documented in [E.Doc.PartOfSoftw], check whether the path through the decision tree documented in [E.Doc.DT.SUM-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.SUM-1], examine its justification documented in [E.Just.DT.SUM-1].

5.3.1.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree documented ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications documented in are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through decision the tree documented in end with “NOT APPLICABLE”; and

— all justifications documented in are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.3.1.4.4 Functional completeness assessment

None.

5.3.1.4.5 Functional sufficiency assessment

None.

5.3.2 [SUM-2] Secure updates

5.3.2.1 Requirement

Each update mechanism that allows updating software affecting security and/or network assets shall only install software whose integrity and authenticity is valid at the time of the installation.

5.3.2.2 Rationale

A secure software update mechanism ensures that the software that controls the equipment is not tampered with through the update mechanism.

5.3.2.3 Guidance

A common approach for confirming that an update is valid cryptographically is to verify its integrity and authenticity based on a trust anchor. This can be done on the equipment or by another equipment that is trusted to perform this verification. For the latter the verified update is typically sent over a secure channel to the equipment.

NOTE "Secure channel" typically preserve the security properties of the communicated information and can also include authorized and authenticated personnel providing the validated software update locally (example of technical or organisational measures).

Manufacturer may provide a secure method to install alternative software not provided by the manufacturer themselves, for example allowing a user to install alternative software on a home router.

It is a security best practice to prevent downgrading the software to an older version.

5.3.2.4 Assessment criteria

5.3.2.4.1 Assessment objective

The assessment addresses the requirement SUM-2.

5.3.2.4.2 Required information

[E.Doc.DT.SUM-2] Description of the selected path through the decision tree in Figure 11 for each update mechanism for parts of the software affecting security and/or network assets.

[E.Just.DT.SUM-2] Justification for the selected path through the decision tree in Figure 11 for each update mechanism for parts of the software affecting security and/or network assets.

If the equipment provides an update mechanism for updating parts of its software affecting security and/or network assets: [E.Doc.SUM] Documentation of each update mechanisms for updating parts of the equipment's software affecting security and/or network assets.

If the equipment provides an update mechanism for updating parts of its software affecting security and/or network assets: [E.Doc.SUM.AuthIntVal] A description of the methods to ensure the validity of the software's integrity and authenticity before installation for each update mechanism for updating parts of its software affecting security and/or network assets.

5.3.2.4.3 Conceptual assessment

5.3.2.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether update mechanism for updating parts of its software affecting security and/or network assets have the required properties.

5.3.2.4.3.2 Preconditions

None.

5.3.2.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each update mechanism for\nparts of the software affecting\nsecurity and/or network
assets;
    if (<b>update mechanism property:</b>\nDoes the update mechanism\nonly install
software whose\nintegrity and authenticity\nis validated? ) then (Yes)
      #lightgreen :PASS\nUpdate secure;
      detach;
    else (No)
       #pink :FAIL\nUpdate not secure;
       detach;
    endif
@enduml
```

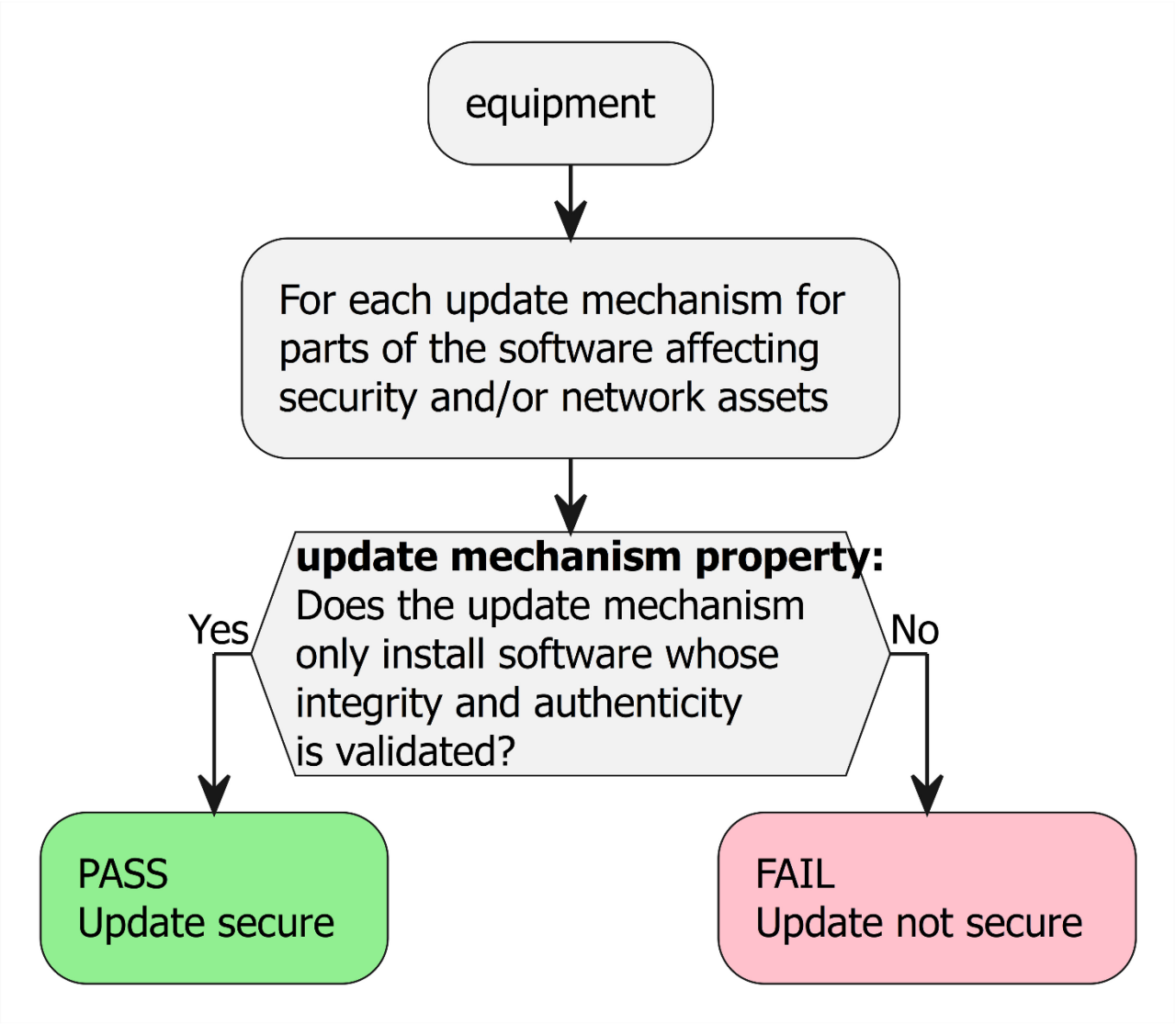

Figure 10 — Decision Tree for requirement SUM-2.

For each update mechanism documented in [E.Doc.SUM], check whether the path through the decision tree documented in [E.Just.DT.SUM-2] ends with “PASS”.

For each path through the decision tree documented in [E.Doc.DT.SUM-2], examine its justification documented in [E.Just.DT.SUM-2].

5.3.2.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— all paths through the decision tree end with “PASS”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— no update mechanisms for updating parts of the equipment’s software affecting security and/or network assets is required.

The verdict FAIL for the assessment case is assigned otherwise.

5.3.2.4.4 Functional completeness assessment

5.3.2.4.4.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of update mechanism for parts of the software affecting security and/or network assets is complete.

5.3.2.4.4.2 Preconditions

The equipment is in an operational state.

5.3.2.4.4.3 Assessment units

Functionally assess whether there exist update mechanisms for parts of the software affecting security and/or network assets, which are not listed in [E.Doc.SUM].

5.3.2.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all update mechanisms found are documented in [E.Doc.SUM].

The verdict FAIL for the assessment case is assigned if one <subject of requirement> found is not documented in [E.Doc.SUM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.3.2.4.5 Functional sufficiency assessment

5.3.2.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the update mechanisms for parts of the software affecting security and/or network assets have the required properties.

5.3.2.4.5.2 Preconditions

The equipment is in an operational state.

5.3.2.4.5.3 Assessment units

For each update mechanism documented in [E.Doc.SUM], functionally confirm the methods to ensure the validity of the software's integrity and authenticity before installation documented in [E.Doc.SUM.AuthIntVal] and used in the justification [E.Just.DT.SUM-2].

5.3.2.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that the methods to ensure the validity of the software's integrity and authenticity before installation are not as documented.

The verdict FAIL for the assessment case is assigned if there is evidence that a method to ensure the validity of the software's integrity and authenticity before installation is not as documented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.3.3 [SUM-3] Automated updates

5.3.3.1 Requirement

If the equipment has a network interface that allows transferring a software update, at least one update mechanism for each updatable part of the software affecting security or network assets shall be capable of updating the software:

— without human intervention at the equipment; or

— via scheduling or triggering the installation of an update under human approval

unless functional safety implications do not allow the automation of updating this part of the software.

5.3.3.2 Rationale

In case of an existing publically exploitable vulnerability in the equipment, that can compromise security and network assets, an automated update mechanism can ensure that an available security update that addresses this vulnerability is automatically applied preventing the vulnerability exploitation.

5.3.3.3 Guidance

In certain cases, automatic updates can result in harm (e.g. safety critical systems). A means to prevent such harm is to provide the updates in a non-automated manner.

In specific cases involving safety or time-critical aspects, the update may require some precautions and/or on-site verifications before it is initiated and therefore cannot be performed in an automatic way so that the operation of the application is not affected.

It is advised to install new software in a free memory location prior to activation of the new software.

NOTE 1 “Activation” of the software means making the software the default version to be executed on the equipment.

In case the installation of the new software fails, e.g. validation of the software image(s) is un-successful, a roll-back policy can be applied to re-activate the previous software.

Simple updatability from a user’s perspective supports the distribution of security updates.

NOTE 2 “Simple from a user’s perspective” may include:

- simple configuration of notifications related to the secure update mechanism,
- simple configuration of the update mechanism and
- simple providing a consent to fully automated updates

Where fully automatic update mechanisms are possible, asking for user’s consent to activate it when putting the equipment into service, supports the distribution of security updates.

Checking the availability of new security updates after initialization and at regular can supports the distribution of security updates

5.3.3.4 Assessment criteria

5.3.3.4.1 Assessment objective

The assessment addresses the requirement SUM-3.

5.3.3.4.2 Required information

[E.Doc.PartOfUpdableSoftw] Documentation of each updatable part of the equipment's software affecting security and/or network assets.

[E.Doc.DT.SUM-3] Description of the selected path through the decision tree in Figure 12 for each part of the updatable software affecting security or network assets.

[E.Just.DT.SUM-3] Justification for the selected path through the decision tree in Figure 12 for each part of the updatable software affecting security or network assets.

[E.Doc.SUM-3] Documentation of the means to automate update mechanism(s) for updating parts of the equipment's software affecting security and/or network assets.

5.3.3.4.3 Conceptual assessment

5.3.3.4.3.1 Assessment purpose

The purpose of this assessment case is to determine whether each updatable part of the software affecting security or network assets is automated updatable as required.

5.3.3.4.3.2 Preconditions

None.

5.3.3.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  if (<b>Equipment property:</b>\nDoes the equipment have a network interface \nthat
allows transferring an update?) then (Yes)
    :For each updatable part of the software \naffecting security and/or network assets;
      if (<b>Functional safety implications:</b>\nAre there functional safety
implications, that do not allow the \nautomation of updating this part of the software?)
then (Yes)
            #application :NOT APPLICABLE\nFunctional safety implications \nprohibit
automation;
            detach;
      else (No)
        switch (<b>update mechanism property:</b>\nIs there at least one update mechanism
for the software \nthat is capable of updating the part of software:\n - without human
intervention at the equipment;or\n - via scheduling or triggering the installation of an
update under user approval? )
        case ( \n Yes,\n without intervention)
          #lightgreen :PASS\nUpdateable without intervention;
          detach;
        case ( \n  Yes,\n  via notification promt)
          #lightgreen :PASS\nUpdateable via notification;
          detach;
        case ( \n No)
          #pink :FAIL\nNot updateable as required;
          detach;
      endswitch
    endif
  else (No)
    #application :NOT APPLICABLE\nTechnical capabilities for \nautomated updates not
present;
    detach;
  endif
@enduml
```

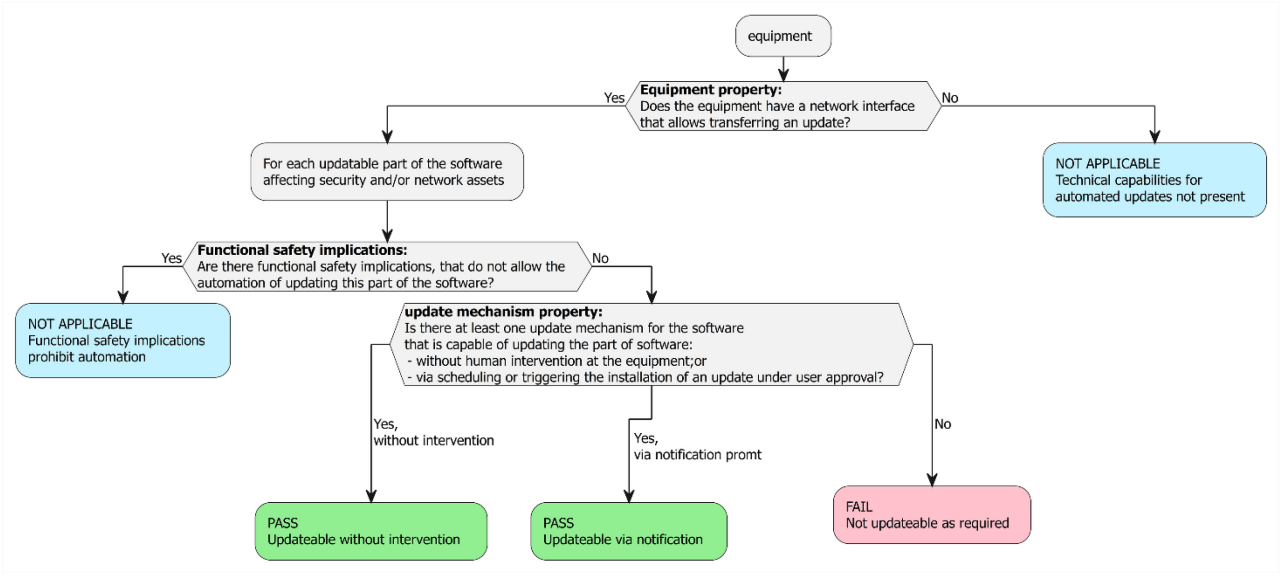

Figure 11 — Decision Tree for requirement SUM-3.

For each updatable part of the software affecting security and/or network assets documented in [E.Doc.PartOfUpdableSoftw], (optionally) automatically updatable as documented in [E.Doc.SUM-3], check whether the path through the decision tree documented in [E.Doc.DT.SUM-3] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.SUM-3], examine its justification documented in [E.Just.DT.SUM-3].

5.3.3.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through the decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.3.3.4.4 Functional completeness assessment

None.

5.3.3.4.5 Functional sufficiency assessment

None.

5.4 [SSM] Secure storage Mechanism

5.4.1 [SSM-1] Applicability of secure storage mechanisms

5.4.1.1 Requirement

The equipment shall use secure storage mechanisms for protecting the security assets and network assets persistently stored on the equipment, unless

— the security assets and network assets in storage are protected by the intended operational environment of use, providing physical or logical protection.

5.4.1.2 Rationale

Secure storage mechanisms protect assets from unauthorized access. If security assets or network assets are not appropriately secured, an attacker can access, tamper, or delete the assets and compromise the equipment, which might lead to the misuse of network resources.

5.4.1.3 Guidance

The assets can be protected by e.g.:

— cryptographic measures like encryption to ensure confidentiality,

— cryptographic measures like digital signatures to ensure integrity and authenticity,

— access control using authentication or authorisation,

— hardware protection measures

— physical protection measures

Physical protection measures can include but are not limited to those provided by sealed enclosure using tamper evident seals.

The appropriate protection mechanism depends on the risks associated with the assets to be stored and this might depend on:

— the criticality of the assets;

— the amount of assets;

— the duration for which the assets needs to be stored;

— the intended operational environment of use.

5.4.1.4 Assessment criteria

5.4.1.4.1 Assessment objective

The assessment addresses the requirement SSM-1.

5.4.1.4.2 Required information

[E.Doc.DT.SSM-1] Description of the selected path through the decision tree in Figure 13.

[E.Just.DT.SSM-1] Justification for the selected path through the decision tree in Figure 13.

[E.Doc.SecurityAsset] Complete documentation of the security assets stored on the equipment.

[E.Doc.NetworkAsset] Complete documentation of the network assets stored on the equipment.

[E.Doc.SSM] Documentation of the secure storage mechanisms that describes the set of the mechanisms used to store security assets as documented in [E.Doc.SecurityAsset] and network assets as documented in [E.Doc.NetworkAsset].

5.4.1.4.3 Conceptual assessment

5.4.1.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether secure storage mechanisms are implemented when it is required to protect the security assets and network assets stored on the equipment.

5.4.1.4.3.2 Preconditions

None.

5.4.1.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:Equipment;
if (Are network assets or security\nassets stored on the equipment? ) then ( Yes )
  :For each network asset and security \nasset stored on the equipment;
  if ( Is the asset secured while\n stored on the equipment? ) then ( Yes )
  #lightgreen :PASS\nAsset is protected;
  detach
  else (No)
        if (Is the asset stored on an equipment\nprotected by intended operational
environment of use \nproviding physical or logical protection? ) then ( Yes )
        #application :NOT APPLICABLE\nAsset protected\nby the intended environment of use;
        detach
      else ( No )
        #pink :FAIL\nAsset not protected;
        detach
      endif
  endif
else (No)
  #application :NOT APPLICABLE\nNo assets stored;
  detach
endif
@enduml
```

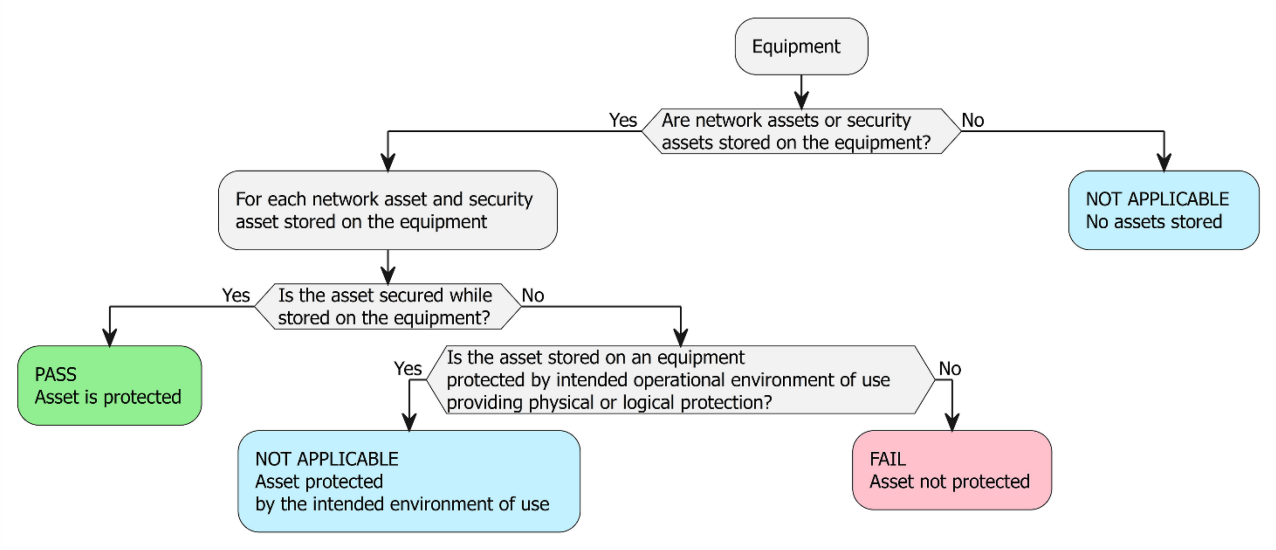

Figure 12 — Decision tree for requirement SSM-1.

For each security asset documented in [E.Doc.SecurityAsset] and for each network asset documented in [E.Doc.NetworkAsset], check whether the path through the decision tree documented in [E.Doc.DT.SSM-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.SSM-1], examine its justification documented in [E.Just.DT.SSM-1].

5.4.1.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.4.1.4.4 Functional completeness assessment

5.4.1.4.4.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation is complete.

5.4.1.4.4.2 Preconditions

— The equipment must be in normal operational state.

5.4.1.4.4.3 Assessment units

Functionally assess whether there are security assets stored on the equipment, which are not listed in [E.Doc.SecurityAssets].

Functionally assess whether there are network assets stored on the equipment, which are not listed in [E.Doc.NetworkAsset].

Functionally assess whether there are secure storage mechanisms used to store security assets or network assets, which are not listed in [E.Doc.SSM].

5.4.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— all security assets are documented in [E.Doc.SecurityAsset], and

— all network assets are documented in [E.Doc.NetworkAsset], and

— no evidence is found that secure storage mechanisms used to store security assets or network assets are not documented in [E.Doc.SSM]

The verdict FAIL for the assessment case is assigned otherwise.

5.4.1.4.5 Functional sufficiency assessment

5.4.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether secure storage mechanisms are implemented when it is required.

5.4.1.4.5.2 Preconditions

— The equipment must be in normal operational state

5.4.1.4.5.3 Assessment units

Functionally confirm that secure storage mechanisms are implemented as documented in [E.Doc.SSM].

5.4.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that the secure storage mechanisms are not existing as documented.

The verdict FAIL for the assessment case is assigned if there is an indication that the secure storage mechanisms are not existing as documented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms

5.4.2.1 Requirement

Each secure storage mechanism which is subject to SSM-1 shall protect the integrity of security assets and network assets persistently stored.

5.4.2.2 Rationale

When stored, security assets and network assets require protection against tampering. If the integrity of the assets stored is not appropriately secured, an attacker can manipulate those assets, which might endanger network resources.

The integrity applies for encrypted as well as for unencrypted storage.

5.4.2.3 Guidance

Data can be protected from tampering by for instance:

— cryptographic measures like digital signatures,

— access control

— hardware protection measures.

5.4.2.4 Assessment criteria

5.4.2.4.1 Assessment objective

The assessment addresses the requirement SSM-2.

5.4.2.4.2 Required information

[E.Doc.DT.SSM-2] Description of the selected path through the decision tree in Figure 14 for each secure storage mechanism in each operational state.

[E.Just.DT.SSM-2] Justification for the selected path through the decision tree in Figure 14 for each secure storage mechanism in each operational state. This is a documented analysis (based on e.g., threat models and security risk assessment), rationale and verdict regarding the appropriateness of mechanisms and modes used to ensure the integrity of the assets stored.

[E.Doc.SSM-2] Documented list of security mechanisms or cryptographic modes that are used to protect the integrity of security assets and network assets when stored on the equipment.

[E.Doc.OperationalStates] Description of the equipment's operational states, how such states will differ from the normal operation state, and under which secure conditions the operational states can be entered.

5.4.2.4.3 Conceptual assessment

5.4.2.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each secure storage mechanism of the equipment is protecting the integrity of security assets and network assets.

5.4.2.4.3.2 Preconditions

None.

5.4.2.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each secure storage mechanism;
:For each operational state;
if (Is the integrity of the assets sufficiently \nprotected to ensure that attacks on
secure \nstorage do not lead to their manipulation?) then (Yes)
  #lightgreen :PASS\nIntegrity protected;
  detach;
else (No)
  #pink :FAIL\nIntegrity not protected;
  detach;
endif
@enduml
```

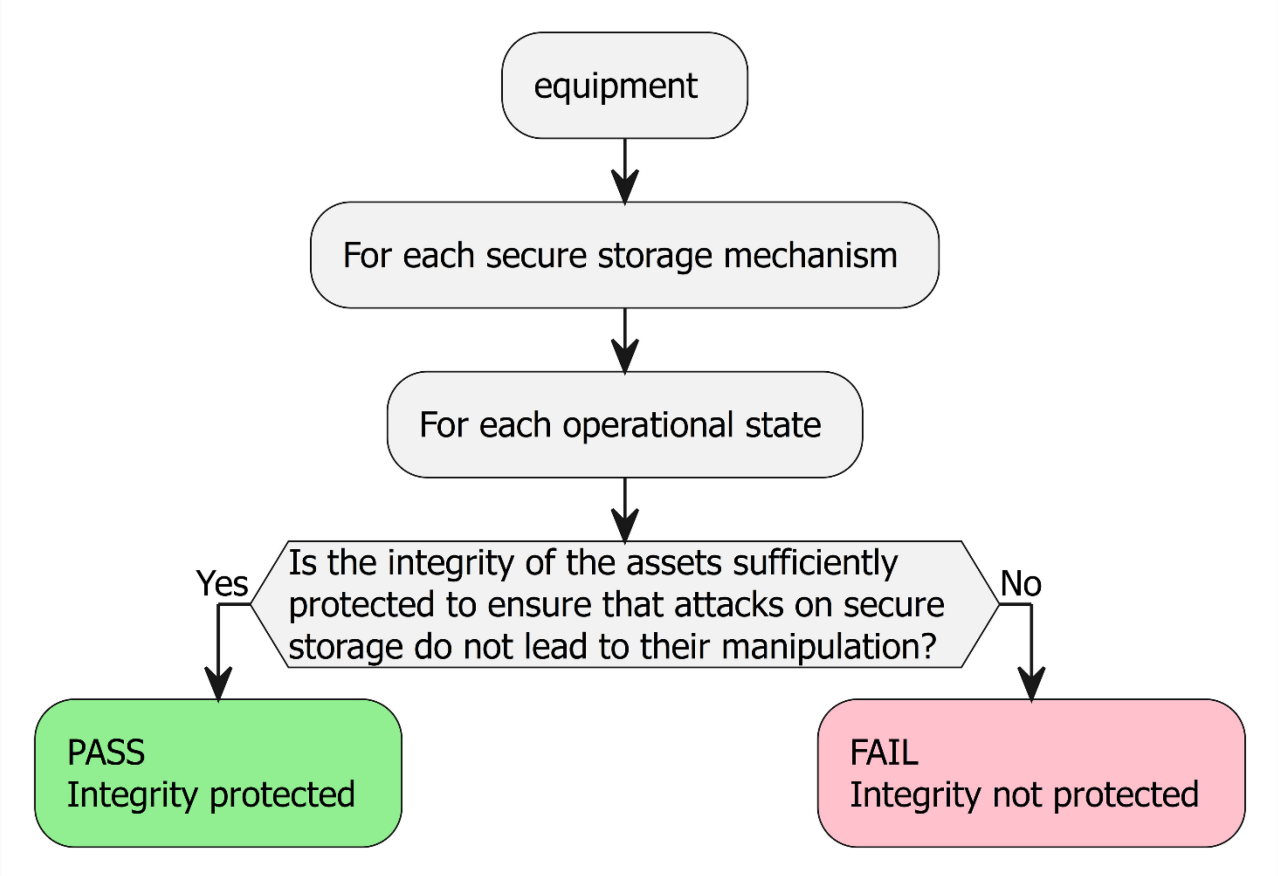

Figure 13 — Decision tree for requirement SSM-2.

For each secure storage mechanism in [E.Doc.SSM-2], and for each operational state described in [E.Doc.OperationalStates], check whether the path through the decision tree documented in [E.Doc.DT.SSM-2] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.SSM-2], examine its justification documented in [E.Just.DT.SSM-2].

5.4.2.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.4.2.4.4 Functional completeness assessment

None.

5.4.2.4.5 Functional sufficiency assessment

5.4.2.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the secure storage mechanism provides the required integrity protection.

5.4.2.4.5.2 Preconditions

— The equipment must be in normal operational state.

5.4.2.4.5.3 Assessment units

Functionally assess whether security assets or network assets stored on the equipment can be tampered by an unauthorized entity.

5.4.2.4.5.4 Assignment of verdict

The verdict PASS is assigned if:

— there is no evidence that integrity protection is not implemented as documented.

— no tamper attack was successful.

The verdict FAIL is assigned otherwise.

5.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms

5.4.3.1 Requirement

Each secure storage mechanism which is subject to SSM-1 shall protect the secrecy of confidential security parameter for an asset persistently stored.

5.4.3.2 Rationale

When stored, confidential security parameters for an asset require protection from exposure. If confidential security parameter for an asset is not appropriately secured, an attacker can access and misuse the equipment and stored data, which might lead to the misuse of network resources.

5.4.3.3 Guidance

Data can be protected from exposure by e.g.:

— cryptographic measures like encryption,

— access control

— hardware protection measures

5.4.3.4 Assessment criteria

5.4.3.4.1 Assessment objective

The assessment addresses the requirement SSM-3.

5.4.3.4.2 Required information

[E.Doc.DT.SSM-3] Description of the selected path through the decision tree in Figure 15 for each secure storage mechanism in each operational state.

[E.Just.DT.SSM-3] Justification for the selected path through the decision tree in Figure 15 for each secure storage mechanism in each operational state. This is a documented analysis (based on e.g., threat models and security risk assessment), rationale and verdict regarding the appropriateness of mechanisms and modes used to ensure the confidentiality of the asset stored

[E.Doc.SSM-3] Documented list of security mechanisms or cryptographic modes that are used to protect the confidentiality of sensitive security parameters when stored on the equipment.

[E.Doc.OperationalStates] Description of the equipment's operational states, how such states will differ from the normal operation state, and under which secure conditions the operational states can be entered.

5.4.3.4.3 Conceptual assessment

5.4.3.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each secure storage mechanism of the equipment is protecting the confidentiality of sensitive security parameters.

5.4.3.4.3.2 Preconditions

None.

5.4.3.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each secure storage mechanism;
:For each operational state;
if (Is the confidentiality of the assets sufficiently \nprotected to ensure that attacks
on secure \nstorage do not lead to their disclosure?) then (Yes)
  #lightgreen :PASS\nConfidentiality protected;
  detach;
else (No)
```

```
  #pink :FAIL\nConfidentiality not protected;
  detach;
endif
@enduml
```

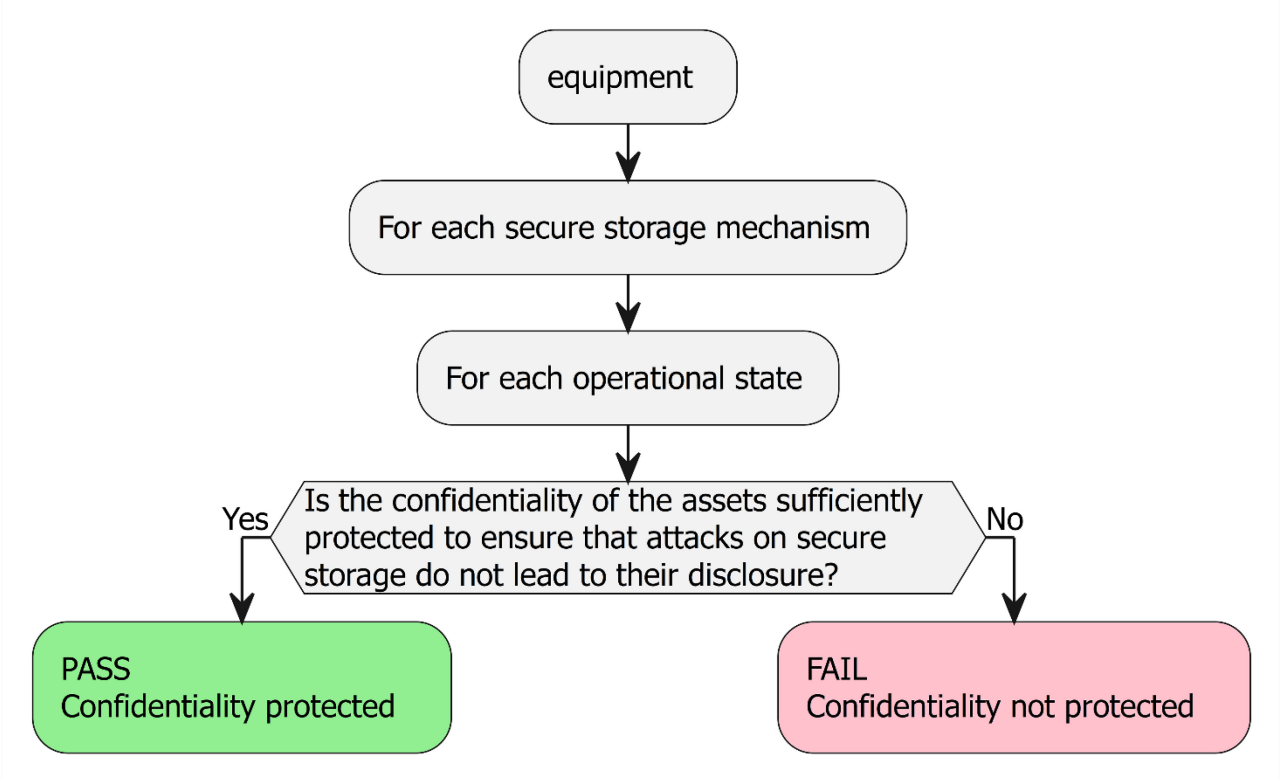

Figure 14 — Decision tree for requirement SSM-3.

For each secure storage mechanism in [E.Doc.SSM-3], and for each operational state described in [E.Doc.OperationalStates], check whether the path through the decision tree documented in [E.Doc.DT.SSM-3] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.SSM-3], examine its justification documented in [E.Just.DT.SSM-3].

5.4.3.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.4.3.4.4 Functional completeness assessment

None.

5.4.3.4.5 Functional sufficiency assessment

5.4.3.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the secure storage mechanism provides the required confidentiality protection.

5.4.3.4.5.2 Preconditions

— The equipment must be in normal operational state.

5.4.3.4.5.3 Assessment units

Functionally assess whether security assets or network assets stored on the equipment can be disclosed to an unauthorized entity.

5.4.3.4.5.4 Assignment of verdict

The verdict PASS is assigned if:

— there is no evidence that confidentiality protection is not implemented as documented.

— no security assets or network assets are disclosed to unauthorized entities.

The verdict FAIL is assigned otherwise.

5.5 [SCM] Secure communication mechanism

5.5.1 [SCM-1] Applicability of secure communication mechanisms

5.5.1.1 Requirement

The equipment shall use appropriate secure communication mechanisms for exchanging security assets and network assets, unless

— the communication mechanism is required for interoperability with legacy networks or other devices, or

— the security assets and network assets in transfer are protected by the environment providing physical or logical protection.

5.5.1.2 Rationale

The assets of the equipment may be communicated to other communication partners for example when using web services. Communication, in case of wireless with less effort, enables an attacker having access to the communication to eavesdrop, manipulate or replay the communication. The equipment needs to ensure that the communication is protected against those attacks using secure communication mechanisms.

5.5.1.3 Guidance

Various security mechanisms exist that can be applied to secure the communication (compare also [CRY] cryptography) of the equipment. Best practice configuration ought to be applied to prevent the communication from eavesdropping, manipulation, and replay. Typical measures are a combination of authentication, integrity protection, encryption and replay protection. The measures can for example be

applied to the communication channel or used for end-to-end protection. The equipment needs to provide best practice to other communication partners by default. If the necessity exits for "legacy support" the resulting risks towards "best practice security" ought to be assessed. Appropriate measures may differ between the underlying use cases of the communication.

5.5.1.4 Assessment criteria

5.5.1.4.1 Assessment objective

The assessment addresses the requirement SCM-1.

5.5.1.4.2 Required information

[E.Doc.DT.SCM-1] Description of the selected path through the decision tree in Figure 16 for each of the network interfaces.

[E.Just.DT.SCM-1] Justification for the selected path through the decision tree in Figure 16 for each network interface.

[E.Doc.NetworkInterfaces] Complete documentation of all network interfaces.

[E.Doc.SecurityAsset.SCM] Complete documentation of the security assets communicated over the network interfaces.

[E.Doc.NetworkAsset.SCM] Complete documentation of the network assets communicated over the network interfaces.

[E.Doc.SCM] Documentation of the secure communication mechanisms that describes the set of the mechanisms used to communicate security assets documented in [E.Doc.SecurityAsset.SCM] or network assets documented in [E.Doc.NetworkAsset.SCM] over the network interfaces.

5.5.1.4.3 Conceptual assessment

5.5.1.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether secure communication mechanisms are implemented when it is required to protect the security parameters communicated over network interfaces.

5.5.1.4.3.2 Preconditions

None.

5.5.1.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:Equipment ;
if (Are security assets or network assets\ncommunicated over any network interface?) then
( Yes )
  :For every network interface communicating assets;
  if (Are the assets secured while \ncommunicated over the interface?) then ( Yes )
    #lightgreen :PASS\nApplicable and met;
    detach
  else (No)
    if (Is the communication mechanism required \nto communicate with legacy networks or
devices) then ( Yes )
      #application :NOT APPLICABLE\nRequired for legacy;
```

```
      detach
    else ( No )
      if (Is the communication of assets protected \nby the environment providing physical
or \nlogical protection? ) then ( Yes )
        #application :NOT APPLICABLE\nProtected by the environment;
        detach
      else ( No )
        #pink :FAIL\nApplicable but not met;
        detach
      endif
    endif
  endif
else (No)
  #application :NOT APPLICABLE\nNothing to protect;
  detach
endif
@enduml
```

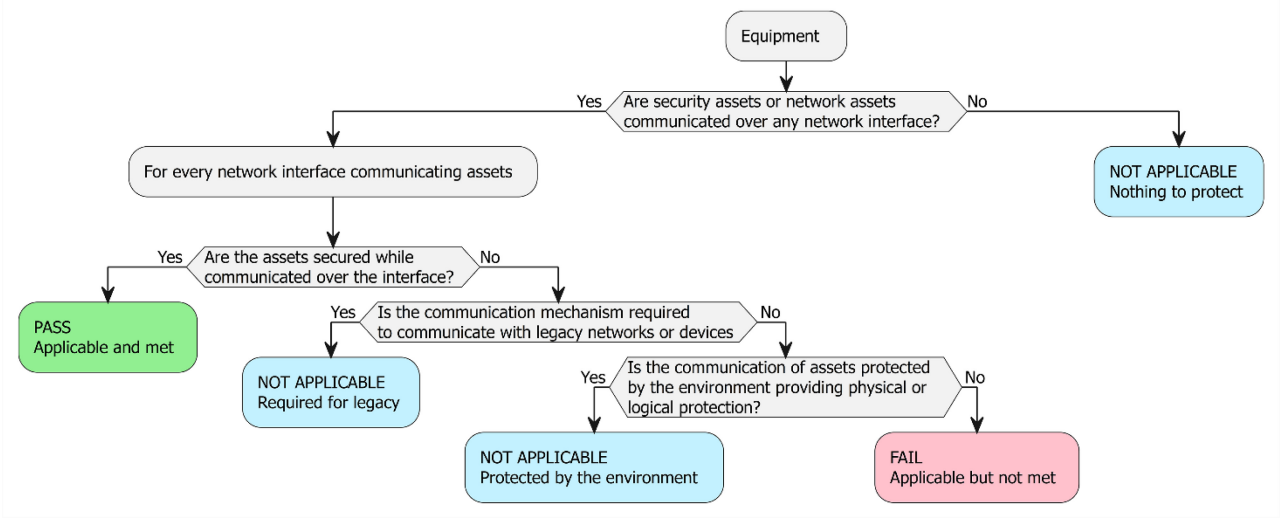

Figure 15 — Decision Tree for requirement SCM-1.

For each network interface documented in [E.Doc.NetworkInterfaces], check whether the path through the decision tree documented in [E.Doc.DT.SCM-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.SCM-1], examine its justification documented in [E.Just.DT.SCM-1].

5.5.1.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.5.1.4.4 Functional completeness assessment

5.5.1.4.4.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation is complete.

5.5.1.4.4.2 Preconditions

— The equipment must be in normal operational state and all [E.Doc.NetworkInterfaces], are either enabled or are configured so that each network interface can be tested.

— Where [E.Doc.SCM] is implemented the necessary security parameters are provided or configured to be able to test each network interface.

5.5.1.4.4.3 Assessment units

Functionally assess whether there are network interfaces, which are not listed in [E.Doc.NetworkInterfaces].

Functionally assess whether there are security assets communicated, which are not listed in [E.Doc.SecurityAssets.SCM].

Functionally assess whether there are network assets communicated, which are not listed in [E.Doc.NetworkAsset.SCM].

Functionally assess whether there are secure communication mechanisms, which are not listed in [E.Doc.SCM].

5.5.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— all network interfaces are documented in [E.Doc.NetworkInterfaces], and

— all security assets communicated are documented in [E.Doc.SecurityAsset.SCM], and

— all network assets communicated are documented in [E.Doc.NetworkAsset.SCM], and

— all secure communication mechanisms are documented in [E.Doc.SCM]

The verdict FAIL for the assessment case is assigned otherwise.

5.5.1.4.5 Functional sufficiency assessment

5.5.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the secure communication mechanisms are implemented when they are required.

5.5.1.4.5.2 Preconditions

— The equipment must be in normal operational state and all [E.Doc.NetworkInterfaces], are either enabled or are configured so that each network interface can be tested.

— Where [E.Doc.SCM] is implemented the necessary security parameters are provided or configured to be able to test each network interface.

5.5.1.4.5.3 Assessment units

For each security and network asset documented in [E.Doc.SecNetAsset], functionally confirm the existence of secure communication mechanisms according to [E.Doc.SCM].

5.5.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that secure communication mechanisms have not been implemented as described.

The verdict FAIL for the assessment case is assigned if there is evidence that secure communication mechanisms have not been implemented as described.

5.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms

5.5.2.1 Requirement

Each secure communication mechanism which is subject to SCM-1 shall protect the integrity and authenticity of the security assets and network assets communicated.

5.5.2.2 Rationale

During communication security assets and network assets require protection against manipulation. An attacker having gained access to the network might intercept and tamper the communication (man-in-the-middle attack). The equipment needs to ensure that the communication is protected against those attacks by using integrity and authenticity protection measures.

The integrity and authenticity protection applies for encrypted as well as for unencrypted communications.

5.5.2.3 Guidance

Various security mechanisms exist that can be applied to secure the communication (see CRY-1) of the equipment. Best practice configuration ought to be applied to prevent the communication from manipulation. Typical measures are a combination of authentication and integrity protection. The measures can for example be applied to the communication channel or used for “end-to- end” protection. The equipment needs to provide best practice to other communication partners by default. If the necessity exits for “legacy support” the resulting risks towards “best practice security” ought to be assessed. Appropriate measures may differ between the underlying use cases of the communication.

The cryptographic mode used to protect the integrity and authenticity of the assets communicated is determined in the requirement [CRY-1] Cryptography.

5.5.2.4 Assessment criteria

5.5.2.4.1 Assessment objective

The assessment addresses the requirement SCM-2.

5.5.2.4.2 Required information

[E.Doc.DT.SCM-2] Description of the selected path through the decision tree in Figure 17 for each communication mechanism in each operational state.

[E.Just.DT.SCM-2] Justification for the selected path through the decision tree in Figure 17 for each communication mechanism in each operational state. This is a documented analysis (based on e.g., threat models and security risk assessment), rationale and verdict regarding the appropriateness of mechanisms and modes used to protect the integrity and authenticity of the asset communicated.

[E.Doc.SecurityAsset.SCM] Complete documentation of the security assets communicated over the network interfaces.

[E.Doc.NetworkAsset.SCM] Complete documentation of the network assets communicated over the network interfaces.

[E.Doc.SCM-2] Documented list of security mechanisms and cryptographic modes that are used to protect the integrity and authenticity of communicate security assets documented in [E.Doc.SecurityAsset.SCM] or network assets documented in [E.Doc.NetworkAsset.SCM] communicated over network interfaces that are described in [E.Doc.NetworkInterfaces].

[E.Doc.CommunicationProtocol] Description of the communication protocol which is used for communication on the network interfaces and how [E.Doc.SCM-2] is applied in the protocol.

[E.Doc.OperationalStates] Description of the equipment's operational states, how such states will differ from the normal operation state, and under which secure conditions the operational states can be entered.

5.5.2.4.3 Conceptual assessment

5.5.2.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each secure communication mechanism of the equipment is protecting the integrity and authenticity of security assets and network assets.

5.5.2.4.3.2 Preconditions

None.

5.5.2.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each secure communication mechanism;
:For each operational state;
if (Is the integrity and authenticity of the assets \nsufficiently protected to ensure
that attacks \non secure communication sessions do not \nlead to their manipulation?) then
(Yes)
  #lightgreen :PASS;
  detach;
else (No)
  #pink :FAIL;
  detach;
endif
@enduml
```

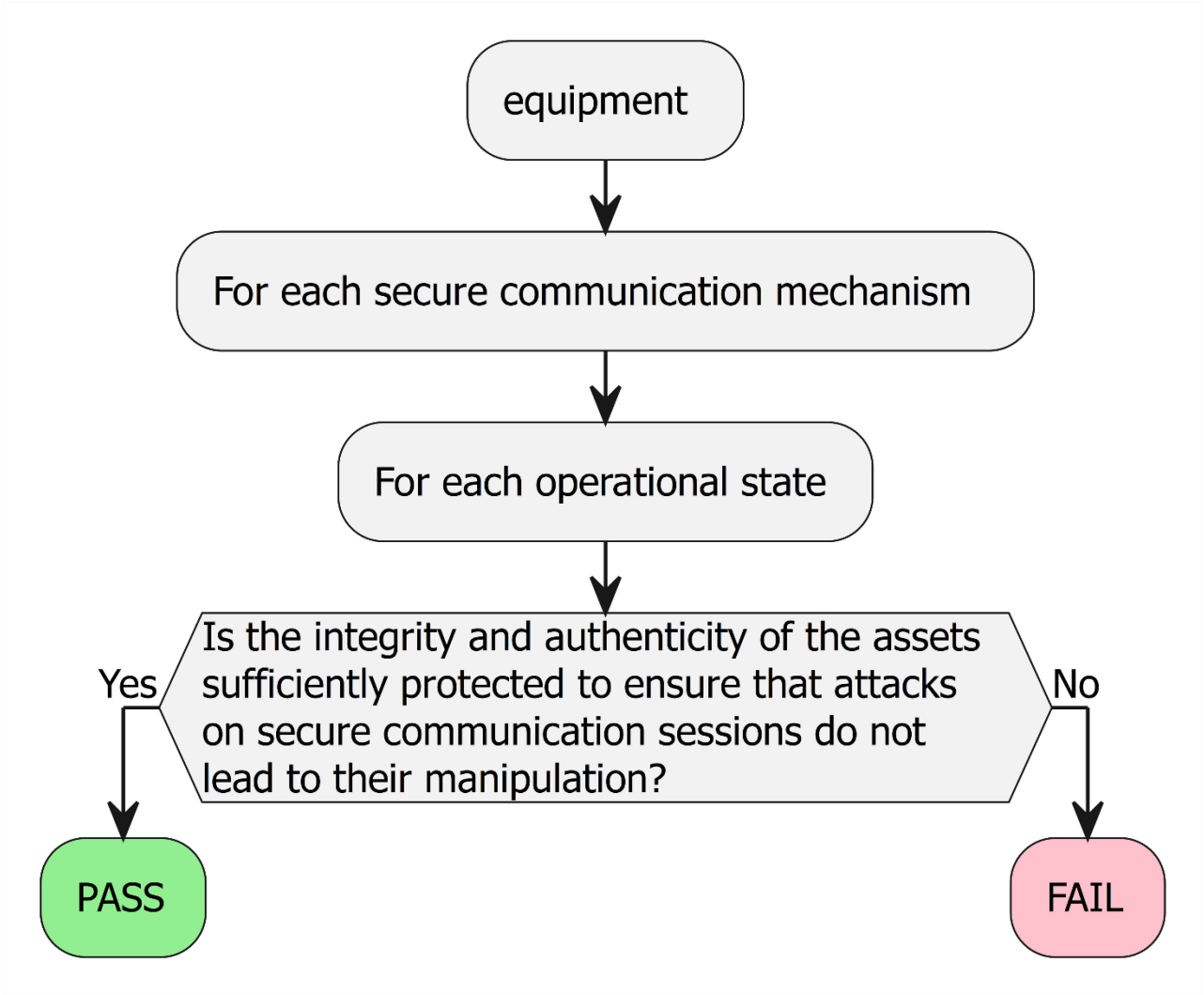

Figure 16 — Decision Tree for requirement SCM-2.

For each secure communication mechanism in [E.Doc.SCM-2], and for each state described in [E.Doc.OperationalStates], check whether the path through the decision tree documented in [E.Doc.DT.SCM-2] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.SCM-2], examine its justification documented in [E.Just.DT.SCM-2].

NOTE 1: Methods to mitigate the risks of attacks on ongoing communication sessions are, among others:

Integrity and authentication protection of communicated data using Cipher-based Message Authentication Code (MAC) techniques.

5.5.2.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.5.2.4.4 Functional completeness assessment

None.

5.5.2.4.5 Functional sufficiency assessment

5.5.2.4.5.1 Assessment purpose

The purpose of this test case is the functional assessment whether the assets communicated are protected against unnoticed tampering.

5.5.2.4.5.2 Preconditions

— The equipment must be in normal operational state and all [E.Doc.NetworkInterfaces], which are part of the intended use, are either enabled or configured, so that each network interface can be tested.

— On interfaces where [E.Doc.SCM-2] are implemented the necessary CSP's are provided or configured to be able to test each secured communication interface [E.Doc.NetworkInterfaces].

— Test tools such as but not limited to protocol analysers for [E.Doc.CommunicationProtocol].

5.5.2.4.5.3 Assessment units

A legitimate communication session on the [E.Doc.NetworkInterfaces] using [E.Doc.CommunicationProtocol] is setup between the equipment and a legitimate communication endpoint. An attempt to tamper with the communication of sensitive security parameters communicated is made.

5.5.2.4.5.4 Assignment of verdict

The verdict PASS is assigned if:

— all secure communication mechanisms are implemented correctly and as documented.

— all attempts to inject malicious data frames during communication sessions do not break the secure communication mechanisms.

— No manipulation due to man-in-the-middle attack is successful.

The verdict FAIL is assigned otherwise.

5.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms

5.5.3.1 Requirement

Each secure communication mechanism which is subject to SCM-1 shall protect the secrecy of confidential security parameter for an asset communicated.

5.5.3.2 Rationale

During communication confidential security parameters for an asset require protection against eavesdropping. An attacker having gained access to the network might monitor the communication. The

equipment needs to ensure that the communication is protected against those attacks by providing confidentiality using encryption measures.

5.5.3.3 Guidance

Various security mechanisms exist that can be applied to secure the confidentiality of the communication (see 4.15 cryptography). Best practice configuration ought to be applied to prevent the communication from eavesdropping. This is typically achieved by symmetric encryption schemes. Those schemes can be applied to the communication channel or used for "end-to-end" protection. It is recommended to provide confidentiality by default between the communicating entities and using best practice cryptography. If the necessity exits for "legacy support" the resulting risks towards "best practice security" ought to be assessed. Appropriate measures may differ between the underlying use cases of the communication.

The cryptographic schemes used to protect the confidentiality of the data communicated is determined in the requirement 4.15 Cryptography.

NOTE: Authenticated encryption (AE) can be used to assure data confidentiality and authenticity in one cryptographic scheme. Those schemes may be used to address the requirement in 5.5.2 as well.

5.5.3.4 Assessment criteria

5.5.3.4.1 Assessment objective

The assessment addresses the requirement SCM-3.

5.5.3.4.2 Required information

[E.Doc.DT.SCM-3] Description of the selected path through the decision tree in Figure 18 for each communication mechanism in each operational state.

[E.Just.DT.SCM-3] Justification for the selected path through the decision tree in Figure 18 for each communication mechanism in each operational state. This is a documented analysis (based on e.g., threat models and security risk assessment), rationale and verdict regarding the appropriateness of mechanisms and schemes used to protect the confidentiality of the asset communicated.

[E.Doc.SecurityAsset.SCM-3] Complete documentation of the confidential security parameters communicated over the network interfaces.

[E.Doc.SCM-3] Documented list of security mechanisms and cryptographic schemes that are used to protect the confidentiality of confidential security parameters documented in [E.Doc.SecurityAsset.SCM-3] communicated over network interfaces that are described in [E.Doc.NetworkInterfaces].

[E.Doc.CommunicationProtocol] Description of the communication protocol which is used for communication on the network interfaces and how [E.Doc.SCM-3] is applied in the protocol.

[E.Doc.OperationalStates] Description of the equipment's operational states, how such states will differ from the normal operation state, and under which secure conditions the operational states can be entered.

5.5.3.4.3 Conceptual assessment

5.5.3.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each secure communication mechanism of the equipment is protecting the confidentiality of confidential security parameters.

5.5.3.4.3.2 Preconditions

None.

5.5.3.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each secure communication mechanism;
:For each operational state;
if (Is the confidentiality of the assets sufficiently \nprotected to ensure that attacks
on secure \ncommunication sessions do not lead to their \ndisclosure?) then (Yes)
  #lightgreen :PASS;
  detach;
else (No)
  #pink :FAIL;
  detach;
endif
@enduml
```

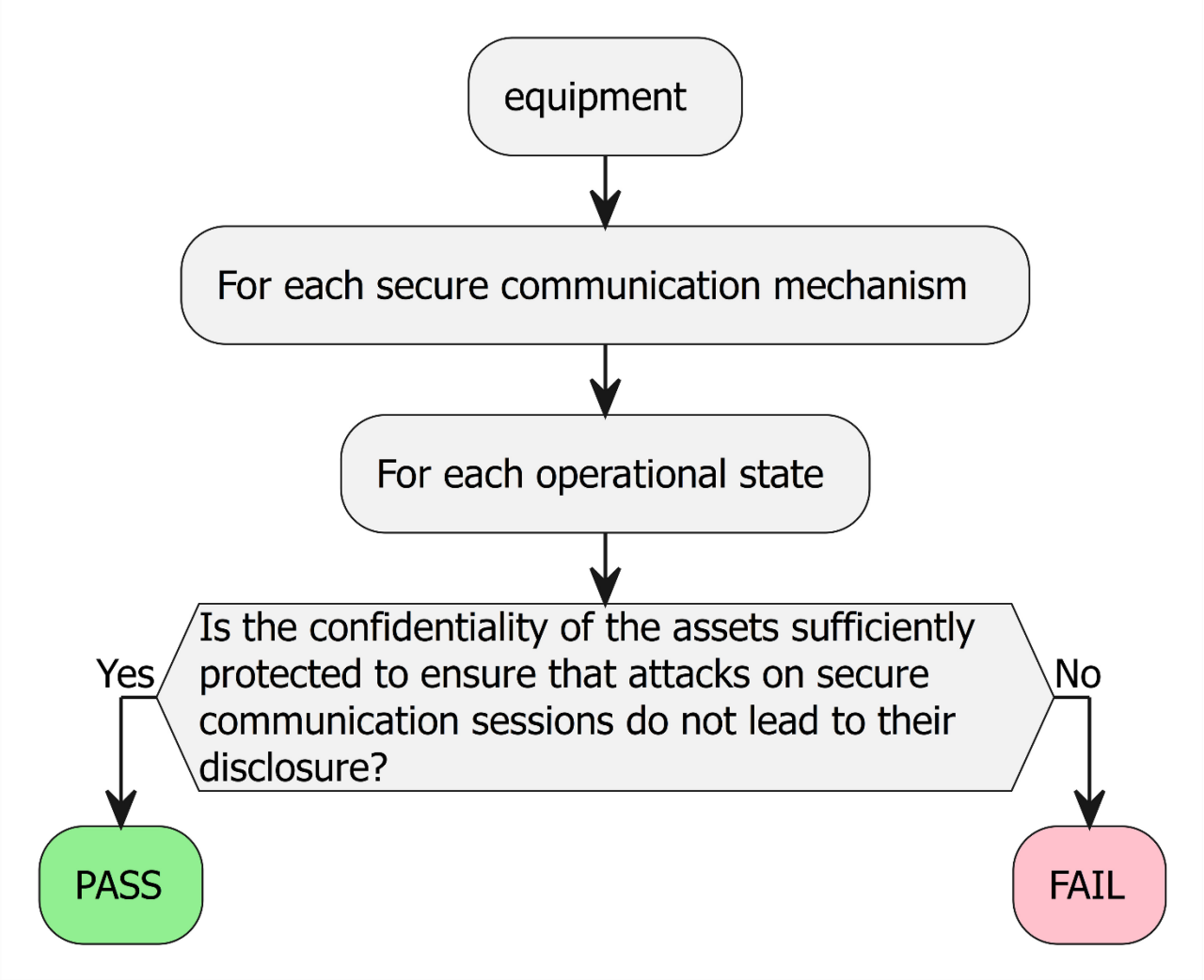

Figure 17 — Decision tree for requirement SCM-3.

For each secure communication mechanism in [E.Doc.SCM-3], and for each state described in [E.Doc.OperationalStates], check whether the path through the decision tree documented in [E.Doc.DT.SCM-3] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.SCM-3], examine its justification documented in [E.Just.DT.SCM-3].

5.5.3.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree ends with “PASS”; and
- no path through the decision tree ends with “FAIL”; and
- all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.5.3.4.4 Functional completeness assessment

None.

5.5.3.4.5 Functional sufficiency assessment

5.5.3.4.5.1 Assessment purpose

The purpose of this test case is the functional assessment whether the assets communicated are protected against eavesdropping.

5.5.3.4.5.2 Preconditions

— The equipment must be in normal operational state and all [E.Doc.NetworkInterfaces], which are part of the intended use, are either enabled or configured, so that each network interface can be tested.

— On interfaces where [E.Doc.SCM-3] are implemented the credentials necessary to establish the communication to a counterpart are provided necessary CSP's are provided or configured to be able to test each secured communication interface [E.Doc.NetworkInterfaces].

— Test tools such as but not limited to protocol analysers for [E.Doc.CommunicationProtocol].

5.5.3.4.5.3 Assessment units

A legitimate communication session on the [E.Doc.NetworkInterfaces] using [E.Doc.CommunicationProtocol] is setup between the equipment and a legitimate communication endpoint. The test case covers eavesdrop attacks regarding the communication of confidential security parameters communicated.

5.5.3.4.5.4 Assignment of verdict

The verdict PASS is assigned if:

— all secure communication mechanisms are implemented correctly and as documented.

— no eavesdrop attack is successful.

The verdict FAIL is assigned otherwise.

5.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms

5.5.4.1 Requirement

Each secure communication mechanism which is subject to SCM-1 shall protect the security assets and the network assets communicated against replay attacks, unless:

— a duplicate transfer of security assets and network assets does not impose a threat of a replay attack.

5.5.4.2 Rationale

A replay attack is a form of network attack in which valid data transmission is maliciously repeated. An attacker having gained access to the network might record the communication and replay it unchanged, causing undesired effects at the receiving entity.

For example, if, during a login process of a user the password is communicated encrypted, but without replay protection, an attacker may be able to replay the encrypted login part of the communication, and thus gain maliciously authorized access to the system.

The equipment needs to protect the communication against that class of attacks.

Based on a risk assessment use cases might be identified for which a replay protection might not be needed, e.g., when the data communicated does not lead to a state change at the receiving entity. For example, the request to retrieve an X.509 certificate from a server might not pose a risk for a replay attack.

5.5.4.3 Guidance

Replay attacks can typically be prevented by tagging each datagram of a communication session with a session ID and a counter. The session ID prevents replay attacks of the complete communication, while the counter prevents the replay of a specific datagram within a communication session.

5.5.4.4 Assessment criteria

5.5.4.4.1 Assessment objective

The assessment addresses the requirement SCM-4.

5.5.4.4.2 Required information

[E.Doc.DT.SCM-4] Description of the selected path through the decision tree in Figure 19 for each communication mechanism in each operational state.

[E.Just.DT.SCM-4] Justification for the selected path through the decision tree in Figure 19 for each communication mechanism in each operational state. This is a documented analysis (based on e.g., threat models and security risk assessment), rationale and verdict regarding the appropriateness of mechanisms and schemes used to protect the asset communicated form replay attacks.

[E.Doc.SecurityAsset.SCM] Complete documentation of the security assets communicated over the network interfaces.

[E.Doc.NetworkAsset.SCM] Complete documentation of the network assets communicated over the network interfaces.

[E.Doc.SCM-4] Documented list of security mechanisms and cryptographic schemes that are used to protect security assets documented in [E.Doc.SecurityAsset.SCM] and network assets communicated documented in [E.Doc.NetworkAsset.SCM] from replay attacks over network interfaces that are described in [E.Doc.NetworkInterfaces].

[E.Doc.CommunicationProtocol] Description of the communication protocol which is used for communication on the network interfaces and how [E.Doc.SCM-4] is applied in the protocol.

[E.Doc.OperationalStates] Description of the equipment's operational states, how such states will differ from the normal operation state, and under which secure conditions the operational states can be entered.

5.5.4.4.3 Conceptual assessment

5.5.4.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each secure communication mechanism of the equipment is protecting the communication of security assets and network assets communicated against replay attacks.

5.5.4.4.3.2 Preconditions

None.

5.5.4.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each secure communication mechanism;
:For each operational state;
if (Does the duplicate transfer of an asset \npose a threat of a replay attack?) then
(Yes)
  if (Is the transfer of the asset information\nprotected against replay attacks?) then
(Yes)
    #lightgreen :PASS\nProtected;
    detach;
  else (No)
    #pink :FAIL\nNot protected;
    detach;
  endif
else (No)
  #application :NOT APPLICABLE \nRisk does not exist;
  detach;
@enduml
```

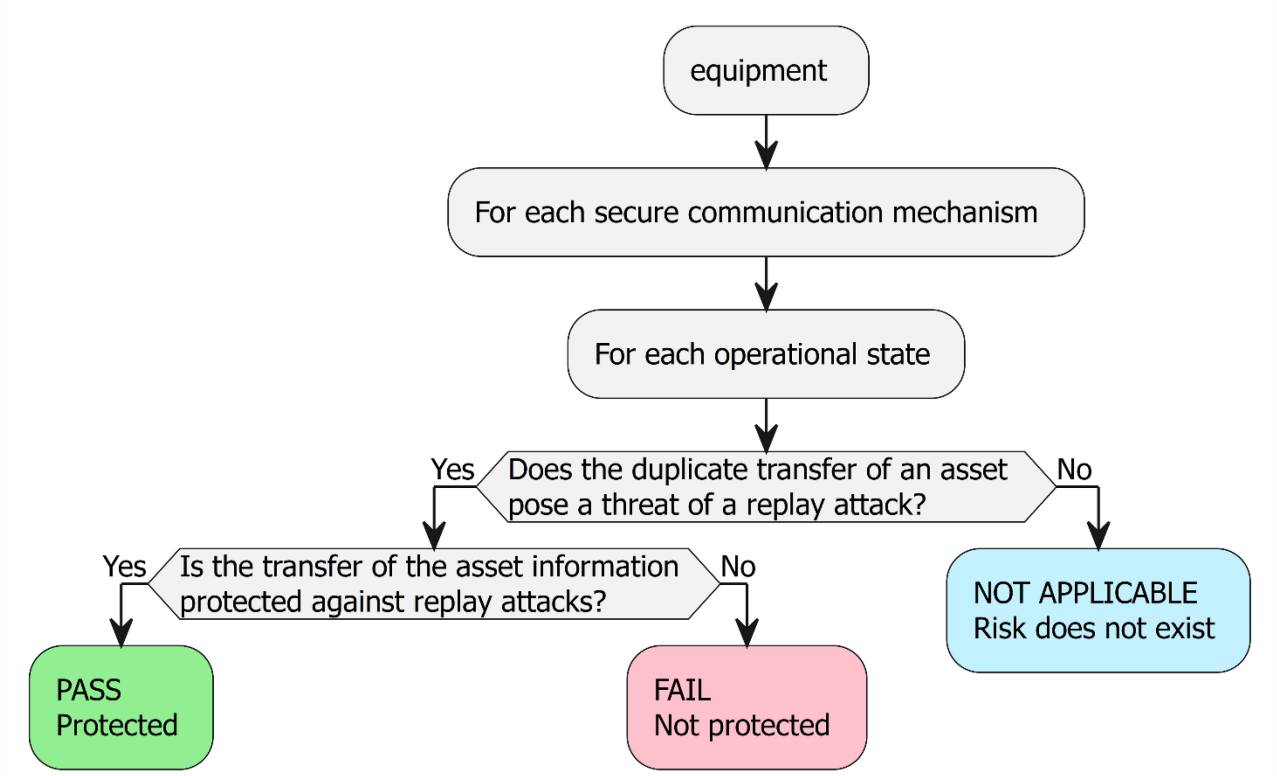

Figure 18 — Decision tree for requirement SCM-4.

For each secure communication mechanism in [E.Doc.SCM-4], and for each state described in [E.Doc.OperationalStates], check whether the path through the decision tree documented in [E.Doc.DT.SCM-4] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.SCM-4], examine its justification documented in [E.Just.DT.SCM-4].

5.5.4.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision ends with “FAIL”; and

— all justifications documented are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through the decision tree end with “NOT APPLICABLE”; and

— all justifications documented are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.5.4.4.4 Functional completeness assessment

None.

5.5.4.4.5 Functional sufficiency assessment

5.5.4.4.5.1 Assessment purpose

The purpose of this test case is the functional assessment whether the assets communicated are protected against replay attacks.

5.5.4.4.5.2 Preconditions

— The equipment must be in normal operational state and all [E.Doc.NetworkInterfaces], which are part of the intended use, are either enabled or configured, so that each network interface can be tested.

— On interfaces where [E.Doc.SCM-4] are implemented the necessary CSP’s are provided or configured to be able to test each secured communication interface [E.Doc.NetworkInterfaces].

— Test tools such as but not limited to protocol analysers for [E.Doc.CommunicationProtocol].

5.5.4.4.5.3 Assessment units

a) Setup a legitimate communication session on the [E.Doc.NetworkInterfaces] using [E.Doc.CommunicationProtocol] between the equipment and a legitimate communication endpoint. The communication of security assets and network assets are recorded.

b) An attempt is made to replay parts of the communication, or the complete communication recording.

5.5.4.4.5.4 Assignment of verdict

The verdict PASS is assigned if:

— all secure communication mechanisms are implemented correctly and as documented.

— No replay attack is successful.

The verdict FAIL is assigned otherwise.

5.6 [RLM] Resilience mechanism

5.6.1 [RLM-1] Applicability of resilience mechanisms

5.6.1.1 Requirement

The equipment shall use resilience mechanisms to mitigate the effects of DoS Attacks on the network interfaces and return to a defined state after the attack unless:

— the equipment's network interface is used in a local network only that does not interoperate with other networks

— Equipment in the network provides sufficient protection against DoS attacks and loss of essential function of equipment for network operations.

5.6.1.2 Rationale

Denial of Service attacks are disruptive to the availability of network resources and may cause permanent disruption in network operation if the attacked equipment is not recovering from a Denial of Service attack properly.

5.6.1.3 Guidance

To reduce the effect of such attacks on the network interfaces, equipment ought to be designed in such a manner that it can employ functions that reduce the effect of such attacks on the network services and resources.

This means that when the equipment's network interfaces are subjected to Denial of Service attacks the equipment is designed so that it can recover to a defined state following the attack. The defined state is specified by the manufacturer of the equipment for its intended use and may include resilience mechanisms enabling the equipment to maintain essential functions while being subjected to the effects of a Denial of Service attacks on one or more of its networking interfaces.

The equipment enters a defined state during the attack and recovers to defined operational state when the attack is finished. The aim is to ensure that the equipment continues to work during an ongoing attack on the network interfaces. Examples of resilience mechanisms that may be applicable depending on the intended use of the equipment are

— Network storm protection

— Network packet filtering mechanisms

— Network traffic rate limiting techniques

— Strategies involving reservation of equipment internal resources (to limit use of resources and protect against exhaustion)

5.6.1.4 Assessment criteria

5.6.1.4.1 Assessment objective

The assessment addresses the requirement RLM-1.

5.6.1.4.2 Required information

[E.Doc.DT.RLM-1] Description of the selected the path through the decision tree in Figure 20 for each network interface.

[E.Just.DT.RLM-1] Justification for the selected path through the decision tree in Figure 20 for each network interface.

(If the equipment communicates over network interfaces to the network) [E.Doc.NetworkInterfaces] Complete Documentation of the network interfaces.

(If the equipment provides a resilience mechanism for mitigating the effects of DoS Attacks on the network interfaces) [E.Doc.RLM] Complete Documentation of the set of resilience mechanisms used for mitigating the effect of DoS Attacks on the network interfaces and returning the equipment to a defined state following the attack.

5.6.1.4.3 Conceptual assessment

5.6.1.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether a resilience mechanism is implemented when it is required.

5.6.1.4.3.2 Preconditions

None.

5.6.1.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:Equipment;
:For each network interface;
if (Is the network interface intended to be \nused to communicate with other \nequipment
in a local network only? ) then (Yes, local \nnetwork only )
              #application :NOT APPLICABLE \ncondition for the network \ninterface;
              detach
    else (No)
      if (Does equipment in the network provide \nsufficient protection against loss of \n
function of the equipment? ) then (Yes, resources in \nthe network )
              #application :NOT APPLICABLE \ncondition for the network \ninterface;
              detach
      else (No)
        if (Does the equipment use resilience \nmechanisms to mitigate the effects \nof
DoS Attacks on the network \ninterfaces and return to a defined \nstate after attack? )
then (Yes )
              #lightgreen :PASS for network interface: \napplicable and met;
              detach
        else (No)
          #pink :FAIL for network interface: \nApplicable but not met;
          detach
        endif
      endif
    endif
@enduml
```

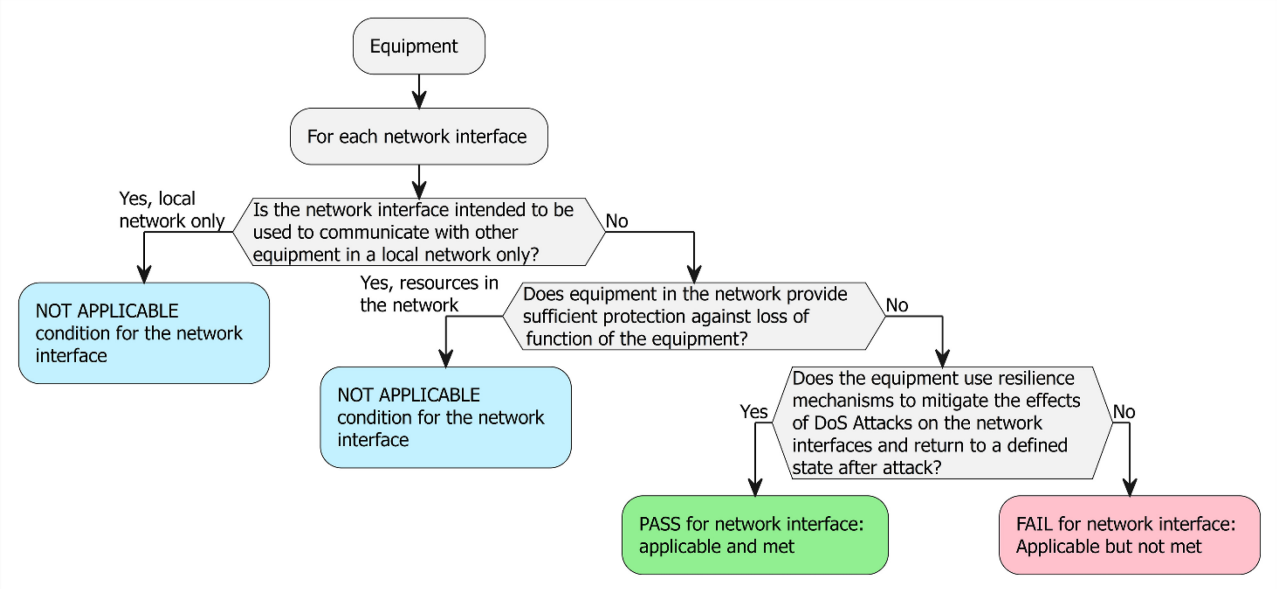

Figure 19 — Decision Tree for requirement RLM-1.

For each network interface documented in [E.Doc.NetworkInterfaces], check whether the path through the decision tree documented in [E.Doc.DT.RLM-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.RLM-1], examine its justification documented in [E.Just.DT.RLM-1].

5.6.1.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.6.1.4.4 Functional completeness assessment

5.6.1.4.4.1 Assessment purpose

The purpose of this assessment case is the functional validation whether the resilience mechanisms implemented mitigate the effects of DoS Attacks on the network interfaces and that the equipment returns to a defined state after an attack with regard to completeness of documentation of network interfaces and the correctness of implementation.

5.6.1.4.4.2 Preconditions

— The equipment is in an operational state and each [E.Doc.NetworkInterfaces] needs to either be enabled or configured so that each network interface can be tested.

— Where [E.Doc.RLM] are used the information on what to configure to be able to test the implemented mechanisms is provided.

5.6.1.4.4.3 Assessment units

— Functionally assess whether there are network interfaces, which are not listed in [E.Doc.NetworkInterfaces].

— Functionally assess if resilience mechanisms are configured as documented in [E.Doc.RLM].

5.6.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if

— all network interfaces identified are documented in [E.Doc.NetworkInterfaces], and

— all resilience mechanisms configured are documented in [E.Doc.RLM].

The verdict FAIL for the assessment case is assigned if at least one network interfaces found is not documented in [E.Doc.NetworkInterfaces] or if resilience mechanisms are not configured as documented in [E.Doc.RLM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.6.1.4.5 Functional sufficiency assessment

5.6.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the resilience mechanisms are implemented when required.

5.6.1.4.5.2 Preconditions

— The equipment is in an operational state and each [E.Doc.NetworkInterfaces] is either be enabled or configured.

— Where [E.Doc.RLM] are used the information on what to configure to be able to test the implemented mechanisms is provided.

— Test tools. The purpose of the test tools is to identify if the equipment when subjected to simulated DoS attacks on the network interfaces is capable of returning to a defined state following the simulated attack scenarios. Examples of tools are:

  - network scanning tools
  - Flooding test tools
  - application scanning tools to discover accessible services, and where applicable fuzzing tools such as:
    - protocol fuzzing tools

- application fuzzing tools

5.6.1.4.5.3 Assessment units

Functionally confirm the [existence/usage] of resilience mechanisms documented in [E.Doc.RLM] and used in the justification [E.Just.DT.RLM-1].

Functionally assess whether the resilience mechanisms mitigate the effects of DoS attacks on the network interfaces and that the equipment returns to a defined state following an attack, considering the intended use of the equipment and its intended operational environment of use.

5.6.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that the resilience mechanisms are not [existing/used] as documented.

The verdict FAIL for the assessment case is assigned if there is evidence that the resilience mechanisms are not [existing/used] as documented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.7 [NMM] Network monitoring mechanism

5.7.1 [NMM-1] Applicability of and appropriate network monitoring mechanisms

5.7.1.1 Requirement

Network equipment shall provide network monitoring mechanisms to detect for evidence of DoS attacks, which is received by the equipment unless:

— The network equipment is not intended to connect other devices to public networks.

5.7.1.2 Rationale

To increase cyber resilience of a system as a whole against unusual network traffic related to the intended use of the equipment which could lead to a Denial-of-Service (DoS), each network equipment as a component of such a system needs to be able to detect implications for such DoS events. This requires the equipment to be able to detect unusual traffic and patterns which could be related to a DoS Attack.

5.7.1.3 Guidance

Unusual traffic which ought to be taken into account are network datagrams which can result in a partial or full Denial-of-Service of the network.

The origin of a DoS event can be an unintentional malfunction of an arbitrary network resource as well as an intentional attack.

To be able to detect implications of DoS event, the equipment must be able to perform an analysis of datagrams with regard to frequency and impact on availability of services of the equipment. Detection of DoS events can be behaviour or signature based, which ever method may be appropriate for the equipment, the intended use and intended operational environment of use

A general measure against DoS events is disabling of via network interface exposed services which are not needed for the intended use of the equipment.

Examples of measures which could be implemented to monitor the network traffic with regard to possible DoS attacks are:

— Monitoring of the number of datagrams in a defined timeframe

— Monitoring if there are datagrams which are originating from an unknown network or have a destination network which is outside of configured network of the network equipment

— Monitoring if there is an unusual number of datagrams which have an unusual round-trip time or are getting a timeout

5.7.1.4 Assessment criteria

5.7.1.4.1 Assessment objective

The Assessment addresses the requirement NMM-1.

5.7.1.4.2 Required information

— [E.Doc.DT.NMM-1] Description of the selected the path through the decision tree in Figure 21 for network monitoring mechanism.

— [E.Just.DT.NMM-1] Justification for the selected path through the decision tree in Figure 21 for network monitoring mechanism.

If the equipment is a network equipment which connects other equipment to public networks:

— [E.Doc.NMM] Documentation of the implemented monitoring mechanisms to monitor and analyse the traffic between networks which is processed via the network interfaces of the network equipment.

— [E.Just.network.Risk] Documented analysis, rationale and verdict regarding the risks for the security and network assets which are processed, controlled or served by the network equipment between networks, in the context of the intended use and intended operational environment of use.

5.7.1.4.3 Conceptual assessment

5.7.1.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether a network monitoring mechanism is implemented when it is required.

5.7.1.4.3.2 Preconditions

None.

5.7.1.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
if (Is the equipment a \nNetwork Equipment? ) then (Yes)
      if (Is the Network Equipment intended to \nconnect other equipment to a public
network?) then (No)
      #application :NOT APPLICABLE\ncondition for\nnon-applicability met;
      detach;
    else (Yes)
      if (Does the Network Equipment provide a network monitoring mechanism ) then (No)
          #pink :FAIL\napplicable but not met;
          detach;
        else (Yes)
          #lightgreen :PASS\napplicable and met;
          detach;
        endif
    endif
else (No)
  #application :NOT APPLICAPLE\ncondition for requirement's\napplicability not met;
  detach;
endif
@enduml
```

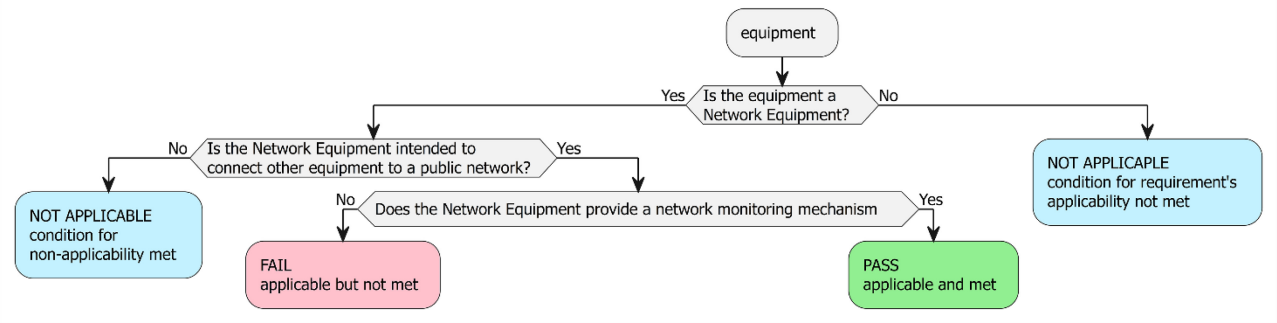

Figure 20 — Decision Tree for requirement NMM-1.

For each path through the decision tree documented in [E.Doc.DT.NMM-1] examine its justification documented in [E.Just.DT.NMM-1].

Check whether the path through the decision tree documented in [E.Doc.DT.NMM-1] ends with “NOT APPLICABLE” or “PASS”.

5.7.1.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.7.1.4.4 Functional completeness assessment

5.7.1.4.4.1 Assessment purpose

The purpose of this assessment case is the functional validation whether the traffic between networks which is controlled or processed by the network equipment is monitored and analysed to mitigate the risk related to security and network assets in the networks which are controlled or served by the equipment concerning to completeness of the documentation and the correctness of the implementation.

5.7.1.4.4.2 Preconditions

The equipment must be in operational state and if available setup or configuration did take place which is related to the traffic between networks.

Physical network connection to communicate between networks is established.

5.7.1.4.4.3 Assessment units

— Functionally assessment whether the traffic between networks which is controlled or processed by the network equipment is monitored and analysed as described in [E.Doc.NMM]

— Attempting to reveal any via the equipment controlled or processed traffic between networks even if the related traffic is not described or documented in [E.Just.network.Risk].

5.7.1.4.4.4 Assignment of verdict

The verdict PASS is assigned if:

— every type of traffic between networks is documented in [E.Just.networkRisk] and

— for all monitoring mechanisms described in [E.Doc.NMM] there is evidence provided that they are working as intended. There is no evidence that the implementation of network monitoring mechanisms differs from its documentation.

The verdict NOT APPLICABLE is assigned if:

— The network equipment is not intended to connect other equipment to public networks

The verdict FAIL is assigned otherwise.

5.7.1.4.5 Functional sufficiency assessment

None.

5.8 [TCM] Traffic control mechanism

5.8.1 [TCM-1] Applicability of and appropriate traffic control mechanisms

5.8.1.1 Requirement

If the equipment is a Network Equipment used to connect other devices to a public network, then the equipment shall provide at least one network traffic control mechanisms.

5.8.1.2 Rationale

Malicious data traffic may be generated by a compromised equipment. While operators of public networks may implement measures to mitigate the effects of malicious traffic based on a datagram's networking information, their knowledge of the network's properties might hinder an effective treatment. Network Equipment that is intended to be used to equipment to public networks can have sufficient information to detect malicious traffic and a traffic control mechanism allows to prevent the public network from corresponding harm.

5.8.1.3 Guidance

Typical equipment categories, whose intended purpose includes forwarding datagrams to a public network are for example home routers that connect private IP networks to the internet or mobile network access points (i.e., base stations), which enable public mobile network access for other equipment.

Controlling data traffic on network layer based on network addresses includes the Network Equipment's ability to block or redirect certain datagrams based on their source or destination address.

5.8.1.4 Assessment criteria

5.8.1.4.1 Assessment objective

The assessment addresses the requirement TCM-1.

5.8.1.4.2 Required information

[E.Doc.DT.TCM-1] Description of the selected the path through the decision tree in Figure 22 for traffic control mechanism.

[E.Just.DT.TCM-1] Justification for the selected path through the decision tree in Figure 22 for traffic control mechanism.

[E.Doc.TCM] the document describes the traffic control mechanism implemented by the network equipment documented in [E.Doc.NetworkEquipment].

5.8.1.4.3 Conceptual assessment

5.8.1.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether a traffic control mechanism is implemented when it is required.

5.8.1.4.3.2 Preconditions

None.

5.8.1.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
if (Is the equipment a \nNetwork Equipment? ) then (Yes)
      if (Is the Network Equipment intended to \nconnect other devices to a public
network?) then (No)
      #application :NOT APPLICABLE\ncondition for\nnon-applicability met;
      detach;
```

```
    else (Yes)
      if (Does the Network Equipment \nprovide a traffic control mechanism? ) then (No)
         #pink :FAIL\napplicable but not met;
         detach;
       else (Yes)
         #lightgreen :PASS\napplicable and met;
         detach;
       endif
    endif
else (No)
  #application :NOT APPLICAPLE\ncondition for requirement's\napplicability not met;
  detach;
endif
@enduml
```

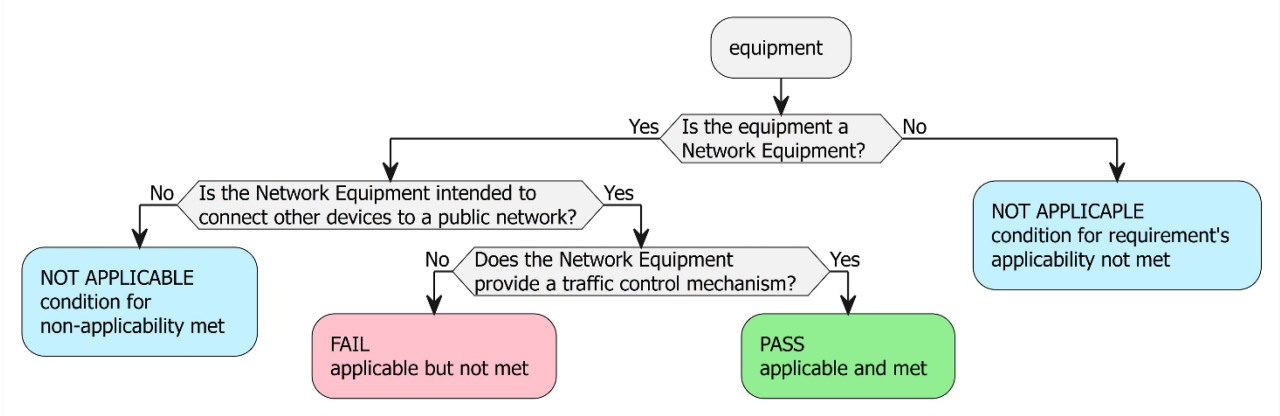

Figure 21 — Decision Tree for requirement TCM-1.

For each path through the decision tree documented in [E.Doc.DT.TCM-1] examine its justification documented in [E.Just.DT.TCM-1].

Check whether the path through the decision tree documented in [E.Doc.DT.TCM-1] ends with “NOT APPLICABLE” or “PASS”.

5.8.1.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.8.1.4.4 Functional completeness assessment

5.8.1.4.4.1 Assessment purpose

The purpose of this assessment case is the functional validation whether the traffic forwarded by the network equipment to a public network is controlled to avoid compromising or harm the security and network assets in the networks which are controlled or served by the network equipment concerning to completeness of the documentation and the correctness of the implementation.

5.8.1.4.4.2 Preconditions

The equipment must be in operational state and if available setup or configuration did take place which is related to the traffic between networks.

5.8.1.4.4.3 Assessment units

- Functionally assessment whether of the traffic forwarded by the network equipment to a public network is controlled as described in [E.Doc.TCM]

5.8.1.4.4.4 Assignment of verdict

The verdict PASS is assigned if:

— every control mechanism is documented in [E.Doc.TMC] and

— for all control mechanisms described in [E.Doc.TCM] there is evidence provided that they are working as intended.

The verdict NOT APPLICABLE is assigned if:

— The network equipment is not intended to control the traffic forwarded by the network equipment to a public network.

The verdict FAIL is assigned otherwise.

5.8.1.4.5 Functional sufficiency assessment

None.

5.9 [CCK] Confidential cryptographic keys

5.9.1 [CCK-1] Appropriate Confidential cryptographic keys (CCKs)

5.9.1.1 Requirement

Confidential cryptographic keys for protecting access to network and/or security assets shall adhere to best practice cryptography unless the equipment enforces their generation on first use.

5.9.1.2 Rationale

Equipment can use cryptography and therefore CCKs for many and different purposes like for authentication to enforce access control to assets, for the protecting the confidentiality or integrity of assets at rest or when communicated to another entity or for the derivation of other CCKs. If the confidentiality or the integrity of a CCK is compromised the assets protected by the CCK may get compromised too. A CCK of an equipment generated for an algorithm used for cryptographic protection is appropriate when

— a successful attack on it does not affect other CCKs used or generated by this equipment or by other equipment and the algorithm has an adequate strength using this CCK to resist attacks proportionate to its use and targeting to break its confidentiality and integrity.

5.9.1.3 Guidance

An important aspect which determines the required strength of CCKs against attacks is the lifetime of the CCK. Long term CCKs which are stored and used repeatedly for a long period of time need to have a longer in time resistance against attacks compared to short term CCKs which are usually generated on the equipment and only used for a short time. Session keys used for a single communication session to encrypt the transferred assets are a typical example for short term keys.

The strength of CCKs depends on 3 parameters:

— their entropy

— their length and

— on the cryptographic algorithm with which they are used.

CCKs need to have length and entropy adequate to their expected lifetime, to the cryptographic algorithm they are used with and to their intended use. Please refer to [CRY-1] Best practice Cryptography for more guidance. Special care is to be taken for CCKs which are not used anymore, for instance these are to be deleted. It is recommended to follow recognised best practices for that.

Additional good security practices need also to be taken into account. For instance, it is a good security practice to use one CCK for a single purpose. It is also recommended that the same CCK is not replicated and used on the different specimens/units of this equipment.

5.9.1.4 Assessment criteria

5.9.1.4.1 Assessment objective

The assessment addresses the requirement CCK-1.

5.9.1.4.2 Required information

[E.Doc.CCK] List of CCKs used by the equipment. For each CCK in the list

1. Provide purpose of use (encryption, integrity protection, and authentication).
2. Provide algorithm and algorithm modes with which it is used.
3. Specify the length.
4. Provide information about the entropy.
   4.1. Precise the best practice recommendations followed for the choice of this length and entropy.
   4.2. else if no best practices are followed provide explanation why this length and entropy are considered to be appropriate for the algorithm and its purpose of use.
5. its lifetime. Precise if the CCK has a limited lifetime or limited number of usages. If so, specify the lifetime, respectively the allowed number of usages.
6. how the CCK is accessed
7. if the CCK is generated on the equipment or preinstalled before placement of the equipment on the market.
8. The generation method with which the CCK is, respectively was, generated.

5.9.1.4.3 Conceptual assessment

5.9.1.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether all confidential cryptographic keys are listed in [E.Doc.CCK] and provide all the requested information regarding each confidential cryptographic key.

5.9.1.4.3.2 Preconditions

None.

5.9.1.4.3.3 Assessment units

Check if all confidential cryptographic keys that are used by the equipment are actually listed in [E.Doc.CCK]. Check in particular the mechanisms described for secure communication, access control and secure storage. Are all confidential cryptographic keys used by the equipment for one of those mechanisms listed in [E.Doc.CCK]?

5.9.1.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if

— all confidential cryptographic keys used by the equipment for secure communication according to SCM are listed in [E.Doc.CCK],

— all confidential cryptographic keys used by the equipment for secure storage according to SSM are listed in [E.Doc.CCK],

— all confidential cryptographic keys used by the equipment for access control according to ACM are listed in [E.Doc.CCK], and

— there is no other evidence that [E.Doc.CCK] is incomplete; and

The verdict FAIL for the assessment case is assigned otherwise.

5.9.1.4.4 Functional completeness assessment

5.9.1.4.4.1 Assessment purpose

The purpose of this assessment case is to establish whether the provided information and rationale on the appropriateness of CCKs used by the equipment is correct.

5.9.1.4.4.2 Preconditions

None

5.9.1.4.4.3 Assessment units

For each CCK indicated in the document [E.Doc.CCK], it shall be assessed that the CCK adheres to best practise cryptography, compare requirement CRY-1.

Assess in particular:

— the length of the CCK,

— the entropy used for generating it

— the algorithm with which the CCK will be used,

— the lifetime, resp. number of possible usages of the CCK, and

— how the CCK is accessed.

5.9.1.4.4.4 Assignment of verdict

The verdict PASS is assigned if the assessments CRY-1 all result in the verdict PASS.

The verdict FAIL is assigned otherwise.

5.9.1.4.5 Functional sufficiency assessment

None

5.9.2 [CCK-2] Confidential cryptographic key generation mechanisms

5.9.2.1 Requirement

Generation of Confidential cryptographic keys on the equipment shall adhere to best practices.

5.9.2.2 Rationale

CCKs that are generated by the equipment and used to protect assets, need to be appropriate to prevent successful attacks based on weak CCKs. An appropriate CCK generation mechanism ensures that CCKs have the necessary properties based on the associated risks and the operational conditions of the equipment.

5.9.2.3 Guidance

The security properties of a produced CCK typically depend on one or more of the following factors:

— the chosen algorithm (enclosing amongst other the set of possible values of a CCK);

— the properties of used random number generators (contributing amongst other to the amount of information an attacker has to guess in order to reconstruct a CCK); and

— the properties of other information (such as other CCK) that is used.

Risks based on the CCKs associated to the protected asset may include the expected damage caused by an attacker's unauthorized access to a protected asset via:

— guessing a CCK; or

— reconstructing a CCK based on accessible information.

It is therefore essential that the CCK generation mechanism will not generate weak CCK and will not provide information about CCK generation.

The possible damage caused by unauthorized access to a protected asset by an attacker, depends on the criticality of the asset, the intended use and on the intended operational environment of use.

NOTE 1 There are a number of well-recognised standards for key generation mechanisms. For instance, recognised best practices for Random Number Generators are NIST SP800-90A[9], NIST SP800-90B[10], NIST SP800-90C[11], BSI AIS31[16].

Recognised best practices for key derivation are for instance described here NIST SP 800-108r1[12], NIST SP 800-132[13], SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms.

5.9.2.4 Assessment criteria

5.9.2.4.1 Assessment objective

The assessment addresses the requirement CCK-2.

5.9.2.4.2 Required information

[E.Doc.CCK] List of CCKs used by the equipment. For each CCK in the list

1. Provide purpose of use (encryption, integrity protection, and authentication).
2. Provide algorithm and algorithm modes with which it is used.
3. Specify the length.
4. Provide information about the entropy.
   4.1. Precise the best practice recommendations followed for the choice of this length and entropy.
   4.2. else if no best practices are followed provide explanation why this length and entropy are considered to be appropriate for the algorithm and its purpose of use.
5. its lifetime. Precise if the CCK has a limited lifetime or limited number of usages. If so, specify the lifetime, respectively the allowed number of usages.
6. how the CCK is accessed
7. if the CCK is generated on the equipment or preinstalled before placement of the equipment on the market.
8. The generation method with which the CCK is, respectively was, generated.

Document [E.Doc.CCK-2] describes for each CCK generation mechanism the following

— The random number sources. Specify the best practices followed by the random number source. Specify if it is certified in one of the internationally recognised security certification schemes, e.g., EUCC/SOGIS Common Criteria, FIPS 140-2[17], FIPS 140-3[18]

— The random number generator (RNG). Specify whether it is a deterministic or a non-deterministic RNG. Specify the best practices followed by the RNG. Specify if the RNG is certified in one of the internationally recognised security certifications, e.g., EUCC/SOGIS Common Criteria, FIPS 140-2[17], FIPS 140-3[18]

— Specify the CCK derivation mechanism/ establishment mechanism. Specify the algorithms which are used for that. Specify which best practices the CCK derivation/CCK establishment mechanism follows.

5.9.2.4.3 Conceptual assessment

5.9.2.4.3.1 Assessment purpose

The purpose of this assessment case is to establish whether all CCK generation mechanisms listed in [E.Doc.CCK-2] are appropriate.

5.9.2.4.3.2 Preconditions

None

5.9.2.4.3.3 Assessment units

Check that all CCKs generated by one of the mechanisms listed in [E.Doc.CCK-2] adhere to best practise cryptography, compare the previous requirement and requirement CRY-.

5.9.2.4.3.4 Assignment of verdict

The verdict PASS is assigned if the assessment units is successfully validated.

The verdict FAIL is assigned otherwise.

5.9.2.4.4 Functional completeness assessment

5.9.2.4.4.1 Assessment purpose

The purpose of this assessment case is to establish

— whether all CCKs generation mechanisms on the equipment are listed in [E.Doc.CCK-2] and

— whether for each CCK generation mechanism the document [E.Doc.CCK-2] provides a complete information as required in CCK-1.

5.9.2.4.4.2 Preconditions

None

5.9.2.4.4.3 Assessment units

a) Check that there is no evidence for other CCK generation mechanisms on the equipment through a consistency check with [E.Doc.CCK].

b) For each CCK generation mechanism in [E.Doc.CCK-2], verify whether it provides complete information as requested in CCK-1.

5.9.2.4.4.4 Assignment of verdict

The verdict PASS is assigned if the assessment units a) and b) are successfully validated.

The verdict FAIL is assigned otherwise.

5.9.2.4.5 Functional sufficiency assessment

None

5.9.3 [CCK-3] No hard-coded confidential cryptographic keys

5.9.3.1 Requirement

Confidential cryptographic keys shall not be hard coded in equipment software.

5.9.3.2 Rationale

Hard-coded confidential cryptographic keys such as hard-coded passwords or PINs can be easily discovered by potential attackers, e.g., via firmware analysis. Furthermore, if a hard-coded parameter is identified, it often allows scalable attacks to several equipment which use the same parameters.

5.9.3.3 Guidance

The main aim is to prevent implementing static security credentials in the equipment. Other security concepts for individual and temporary credentials are available.

5.9.3.4 Assessment criteria

5.9.3.4.1 Assessment objective

The assessment addresses the requirement CCK-3.

5.9.3.4.2 Required information

[E.Doc.CCK] List of CCKs used by the equipment. For each CCK in the list

1. Provide purpose of use (encryption, integrity protection and authentication).
2. Provide algorithm and algorithm modes with which it is used.
3. Specify the length.
4. Provide information about the entropy.
   4.1. Precise the best practice recommendations followed for the choice of this length and entropy.
   4.2. else if no best practices are followed provide explanation why this length and entropy are considered to be appropriate for the algorithm and its purpose of use.
5. its lifetime. Precise if the CCK has a limited lifetime or limited number of usages. If so, specify the lifetime, respectively the allowed number of usages.
6. how the CCK is accessed
7. if the CCK is generated on the equipment or preinstalled before placement of the equipment on the market.
8. The generation method with which the CCK is, respectively was, generated.

[E.Doc.CCK.preinstalled] Complete Documentation of the confidential cryptographic keys that are preinstalled in the equipment. It has to be a subset of [E.Doc.CCK]. For each confidential cryptographic key, specify the same information as for [E.Doc.CCKs]:

1. Provide purpose of use (encryption, integrity protection and authentication).
2. Provide algorithm and algorithm modes with which it is used.
3. Specify the length.
4. Provide information about the entropy.
   4.1 Precise the best practice recommendations followed for the choice of this length and entropy.
   4.2 else if no best practices are followed provide explanation why this length and entropy are considered to be appropriate for the algorithm and its purpose of use.
5. its lifetime. Precise if the CCK has a limited lifetime or limited number of usages. If so, specify the lifetime, respectively the allowed number of usages.
6. how the CCK is accessed
7. if the CCK is generated on the equipment or preinstalled before placement of the equipment on the market. (Note: In our case, all CCKs in [E.Doc.CCK.preinstalled] are preinstalled before placement on the market.)
8. The generation method with which the CCK is, respectively was, generated,

and additionally,

9. The way the CCK is stored on the equipment.

[E.Doc.CCK.generated] Complete Documentation of the confidential cryptographic keys that are to be generated by a generation mechanism for confidential cryptographic keys. It has to be a subset of [E.Doc.CCK].

5.9.3.4.3 Assessment case conceptual

5.9.3.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether no confidential cryptographic keys are hard coded in the equipment's software.

5.9.3.4.3.2 Preconditions

None

5.9.3.4.3.3 Assessment units

For each confidential cryptographic key documented in [E.Doc.CCK.preinstalled], check whether it is hard-coded in the equipment's software according to the documentation.

5.9.3.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if

— all confidential cryptographic keys are NOT hard-coded in the equipment's software according to [E.Doc.CCK.preinstalled] ; and

— there is no evidence that [E.Doc.CCK.preinstalled] is incomplete; and

— there is no evidence that [E.Doc.CCK.preinstalled] is incorrect about the fact if a confidential cryptographic key is hard-coded in the equipment's software.

The verdict FAIL for the assessment case is assigned otherwise.

5.9.3.4.4 Functional completeness assessment

None

5.9.3.4.5 Functional sufficiency assessment

None

5.9.4 [CCK-4] Preventing static default values for confidential cryptographic keys

5.9.4.1 Requirement

Preinstalled confidential cryptographic keys for protecting access to network and/or security assets shall be practically unique per equipment, unless:

— the equipment enforces their generation on first use or,

— the cryptographic key involved is a shared parameter essential to the equipment's operation.

5.9.4.2 Rationale

Equipment can use cryptography and therefore CCKs to protect the assets on the equipment (i.e., network resources). The CCKs are sometimes predefined e.g., in the manufacturing process. CCKs used for the above-mentioned purpose need to be appropriate to prevent successful attacks based on weak CCKs, especially when preinstalled.

When standard values for preinstalled CCK are used, enforcing their setting on first use ensures that risks related to using standard values for preinstalled CCK are reduced.

5.9.4.3 Guidance

CCKs can be preinstalled on the equipment during manufacturing. Preinstalled CCKs that are unique per equipment instance and resist brute force attacks can mitigate cyber security risk associated with the specific use of the CCK. Knowing a CCK for one equipment must not enable an attacker to deduce the corresponding CCK for a different equipment – this is what "practically unique" means.

The required strength of CCKs against attacks depends also on the lifetime of the CCK. For instance, long term CCKs which are stored and used repeatedly during the whole life of the equipment need to provide respectively stronger attack resistance compared to short term CCKs which are usually generated on the equipment and typically used for a short time.

It is a good security practice to use one CCK for a single purpose and that if a CCK of one instance of an equipment is compromised, CCKs on other instances are not endangered.

5.9.4.4 Assessment criteria

5.9.4.4.1 Assessment objective

The assessment addresses the requirement CCK-4.

5.9.4.4.2 Required information

[E.Doc.DT.CCK-4] Description of the selected path through the decision tree shown in Figure 23 for each confidential cryptographic key.

[E.Just.DT.CCK-4] Justification for the selected path through the decision tree shown in Figure 23 for each confidential cryptographic key.

[E.Doc.CCK.preinstalled] Complete Documentation of the confidential cryptographic keys that are present on the equipment.

[E.Doc.CCK-3.generator] Documentation of the method that was used to generate the confidential cryptographic keys that are listed in [E.Doc.CCK.preinstalled].

For each confidential cryptographic key whose generation/setting is not enforced on first use: [E.Doc.CCK-3.generator] Documentation of the method that was used to generate the confidential cryptographic key.

5.9.4.4.3 Conceptual assessment case

5.9.4.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether preinstalled confidential cryptographic keys are sufficiently independent from each other.

5.9.4.4.3.2 Preconditions

None

5.9.4.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each confidential cryptographic key;
if (Is this CCK used for protecting\none or several network\nand/or security assets? )
then (Yes)
    if (Does the equipment enforce\nthe generation of this CCK on first use? ) then (Yes)
      #application :NOT APPLICABLE\ncondition for requirement's\napplicability not met for
this CCK;
      detach;
    else (No)
      switch (Is this CCK practically unique per unit? )
      case ( \nYes)
        #lightgreen :PASS;
        detach;
      case ( \nNo)
       #pink :FAIL;
        detach;
      endswitch
    endif
else (No)
  #application :NOT APPLICAPLE\ncondition for requirement's\napplicability not met for
this CCK;
  detach;
endif
@enduml
```

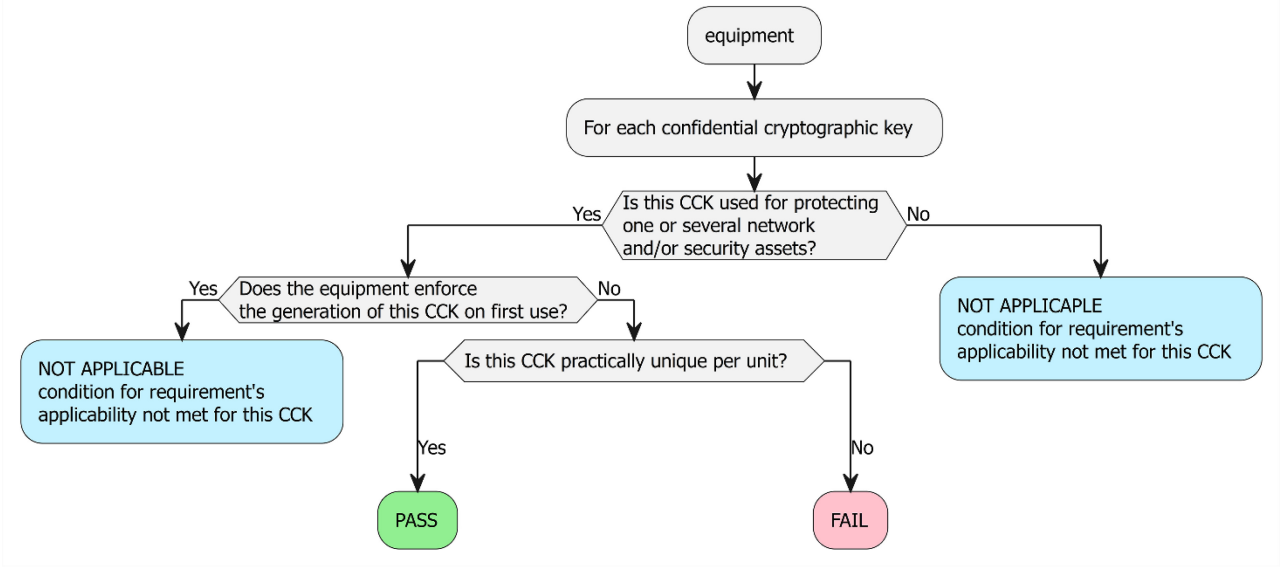

Figure 22 — Decision Tree for requirement CCK-4.

For each confidential cryptographic key documented in [E.Doc.CCK.preinstalled], check whether the path through the decision tree documented in [E.Doc.DT.CCK-4] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.CCK-4], examine its justification documented in [E.Just.DT.CCK-4].

5.9.4.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all paths through the decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.9.4.4.4 Functional completeness assessment

None.

5.9.4.4.5 Functional sufficiency assessment

5.9.4.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether preinstalled confidential cryptographic keys are sufficiently independent from each other.

5.9.4.4.5.2 Preconditions

Two instances of the equipment are needed for this test. Both are in an operational state.

5.9.4.4.5.3 Assessment units

For each confidential cryptographic key documented in [E.Doc.CCK.preinstalled], functionally confirm that the respective CCK of the two equipment’s are practically unique, i.e., they are not the same and there is no obvious way to derive one from the other. This functional test may not always be possible as the assessor will usually not have access to the CCKs. Where the confidential cryptographic keys come together with associated public cryptographic keys (e.g., private/public key pairs), the assessor can at least compare the public cryptographic keys and check if they differ between the two items of equipment.

5.9.4.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that the confidential cryptographic keys are not practically unique.

The verdict FAIL for the assessment case is assigned if there is evidence that the confidential cryptographic keys are not practically unique.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

5.10 [GEC] General equipment capabilities

5.10.1 [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities

5.10.1.1 Requirement

The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security and network assets unless:

— such publicly know vulnerability cannot be exploited in the specific conditions of the equipment;

— such publicly known exploitable vulnerability has been mitigated.

5.10.1.2 Rationale

Equipment can consist of hardware and software provided by many providers and the manufacturer might not have visibility into the security practices of these providers, which poses risks to the manufacturer.

Management of hardware and software supply chain security risks goes beyond the scope of this document but in order to comply with this requirement, it is essential that the manufacturer can identify publicly known exploitable vulnerabilities in the hardware and in the third-party software, both commercial and open-source software, used in the equipment and can handle these vulnerabilities.

By using more secure hardware and software, the risk posed by the attack surface is reduced.

5.10.1.3 Guidance

To facilitate software vulnerability monitoring, the manufacturer of the equipment keeps technical documentation of the software of the equipment, including both open-source software and commercial off the shelf components. Likewise, technical documentation of hardware can assist in the identification of the hardware vulnerabilities.

To identify the publicly known exploitable vulnerabilities in the hardware and software of the equipment, the manufacturer consults the NVD vulnerability database.

Different factors the manufacturer considers when assessing the publicly known exploitable vulnerabilities, include, but are not limited to:

— attack surface of the equipment and vectors/paths by which an attacker can gain access to the equipment to exploit the vulnerability;

— the evidence that the vulnerability has been actively exploited or it already has documented proof-of-concept or code exploits;

— the security capabilities and mechanisms implemented in the equipment which can mitigate the exploitation of the vulnerability;

— the “equipment’s intended use”;

— the equipment's “intended operational environment of use” including the threat environment and the security capabilities and additional countermeasures provided by the environment which can mitigate or remediate the exploitation of the vulnerability.

5.10.1.4 Assessment criteria

5.10.1.4.1 Assessment objective

The assessment addresses the requirement GEC-1.

5.10.1.4.2 Required information

[eDoc.SoftwareDocumentation] Description of the software of the equipment, including their versions, that affect the security assets and the network assets.

[eDoc.HardwareDocumentation] Description of the hardware of the equipment that affect the security assets and the network assets.

[E.Doc.ListOfVulnerabilities] Documented list of all the hardware or software publicly known exploitable vulnerabilities in the hardware and software of the equipment under test. The document includes also the manufacturer justification about the remediation, mitigation and non-exploitation of the listed hardware or software publicly known exploitable vulnerabilities.

5.10.1.4.3 Conceptual assessment

5.10.1.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the hardware or software publicly known exploitable vulnerabilities present in the hardware and software of the equipment under test, in factory default state, have been mitigated, remediated or non-exploitable.

5.10.1.4.3.2 Preconditions

None.

5.10.1.4.3.3 Assessment units

Assess the completeness of the public known exploitable vulnerabilities list in [E.Doc.ListOfVulnerabilities] for each hardware or software documented in [eDoc.SoftwareDocumentation] and [eDoc.HardwareDocumentation].

5.10.1.4.3.4 Assignment of verdict

The verdict PASS is assigned if the document [E.Doc.ListOfVulnerabilities] lists and provides a status (i.e., mitigated, remediated or not exploitable) for each hardware and software publicly known exploitable vulnerabilities (completeness of the publicly known exploitable vulnerabilities list).

The verdict FAIL for the assessment case is assigned otherwise.

5.10.1.4.4 Functional completeness assessment

5.10.1.4.4.1 Assessment purpose

The purpose of this test case is the functional assessment of the equipment under test to verify the completeness of the documentation: that the vulnerabilities present in the equipment are only those listed in [E.Doc.ListOfVulnerabilities] and the exploitation, or the impact of its exploitation or both, are remediated, mitigated or non-exploited as documented.

5.10.1.4.4.2 Preconditions

The equipment must be in operational and factory default state.

The date for the source of the vulnerabilities to be used in the assessment of the list of publicly known exploitable vulnerabilities must be recent.

5.10.1.4.4.3 Assessment units

Assessment of the vendor justification (i.e., remediated, mitigated or not exploitable) for each of the publicly known exploitable vulnerability in [E.Doc.ListOfVulnerabilities].

a) Functionally assess whether the equipment under test includes other publicly known exploitable vulnerabilities which are not listed in [E.Doc.ListOfVulnerabilities].
b) For each of the publicly known exploitable vulnerabilities in [E.Doc.ListOfVulnerabilities], functionally assess the vendor justification for its mitigation, remediation or non-exploitability.
c) For each of the publicly known exploitable vulnerabilities in [E.Doc.ListOfVulnerabilities] the assessment may complement b) by unit test present under publicly known exploitability condition (e.g., an exploitable code attached to a CVE).

5.10.1.4.4.4 Assignment of verdict

The verdict PASS is assigned if:

— every publicly know vulnerability is documented in [E.Doc.ListOfVulnerabilities]; and

— for all publicly known vulnerabilities present in [E.Doc.ListOfVulnerabilities] there is no evidence that they can be exploited when the equipment under test is used and operates in the documented conditions.

The verdict FAIL is assigned otherwise.

5.10.1.4.5 Functional sufficiency assessment

None.

5.10.2 [GEC-2] Limit exposure of services via related network interfaces

5.10.2.1 Requirement

In factory default state the equipment shall only expose network interfaces or services via network interfaces affecting security or network assets which are necessary for equipment setup or for basic operation of the equipment in the intended operational environment of use.

5.10.2.2 Rationale

An important factor for reducing the potential risk that the network resource of the equipment becomes compromised for instance to harm the network, are exposed services. Therefore, these exposed services need to be limited to those that are necessary for equipment setup and to operate the equipment in the intended operational environment of use.

5.10.2.3 Guidance

The configuration of equipment can vary depending on how the equipment is manufactured.

Generally, a differentiation is to be made between two types of equipment:

— Multipurpose equipment (e.g., Smartphones, Laptops): Offered services and functionality of multipurpose equipment are only under the control of the manufacturer until they are delivered. The activated (and documented) network services can only be influenced before the equipment is delivered.

— Equipment with a controlled fixed functionality (e.g., Sensors, Routers): Offered services and functionality of the equipment are embedded in an equipment-specific software (firmware) which is provided by the manufacturer. The activated (and documented) network services can be influenced during the lifecycle of the equipment.

5.10.2.4 Assessment criteria

5.10.2.4.1 Assessment objective

The assessment addresses the requirement GEC-2.

5.10.2.4.2 Required information

[E.Doc.NetworkInterfaces.exposure] Documentation of network interfaces and exposed services via network interfaces in factory default state of the equipment. This documentation will include the information and description for each network interface or exposed service via network interfaces and if they are required for the basic operation or for the setup of the equipment or if they are optional

[E.Doc.SecurityAsset.GEC-2] Documentation of each security asset that is accessible via network interfaces.

[E.Doc.NetworkAsset.GEC-2] Documentation of each network asset that is accessible via network interfaces.

[E.Just.NetworkInterfaces.exposureRisk] Documented analysis, rationale and verdict regarding the risk for the security assets documented in [E.Doc.SecurityAsset.GEC-2] and network assets documented in [E.Doc.NetworkAsset.GEC-2] related to the exposure of network interfaces and services via network interface in factory default state.

If the equipment implements a setup process

[E.Doc.setup] Documentation how to setup the equipment

5.10.2.4.3 Conceptual assessment

5.10.2.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each exposure of network interfaces or services via network interfaces in factory default state of the equipment are restricted to the ones which are necessary for equipment setup or for the basic operation of the equipment and the risk related to security and network assets was justified for each network interface and services exposed via network interface

5.10.2.4.3.2 Preconditions

None.

5.10.2.4.3.3 Assessment units

— Assessment based on [E.Just.NetworkInterfaces.exposureRisk] for each network interface and via network interface exposed service in [E.Doc.NetworkInterfaces.exposure] whether the associated risk was justified in relation to security and network assets

— Assessment based on [E.Doc.NetworkInterfaces.exposure] if the exposure of network interfaces and services via network interfaces is limited to the ones which are required for the setup as described in [E.Doc.Setup] or the basic operation of the equipment.

5.10.2.4.3.4 Assignment of verdict

The verdict PASS is assigned if for each network interface and via network interface exposed service of the equipment:

— The associated risk described in [E.Just.NetworkInterfaces.exposureRisk] was justified in relation to the security and network assets

— the exposure described in [E.Doc.NetworkInterfaces.exposure] is limited to network interfaces or services exposed via network interfaces which are required for setup or for the basic operation of the equipment.

The verdict FAIL is assigned otherwise.

5.10.2.4.4 Functional completeness assessment

5.10.2.4.4.1 Assessment purpose

The purpose of this test case is the functional validation to ensure that only network interfaces or via network interfaces exposed services of the factory default state which are required for setup or for the basic operation of the equipment in the intended operational environment of use are exposed concerning to completeness of the documentation and the correctness of implementation.

5.10.2.4.4.2 Preconditions

The equipment must be in operational factory default state and if available setup or another configuration did not take place until now.

Network connection to check exposure of services via network interfaces is established

5.10.2.4.4.3 Assessment units

— Functionally Assessment whether there are further network interfaces or services activated and exposed via network interfaces in factory default state, which are not listed in [E.Doc.NetworkInterfaces.exposure] or are not required for setup according to [E.Doc.Setup] or to operate the equipment in basic operation.

— Search to reveal any via the equipment exposed network interfaces or services in factory default state, even if the related network interfaces or services are not activated or documented in [E.Doc.NetworkInterfaces.exposure].

5.10.2.4.4.4 Assignment of verdict

The verdict PASS is assigned if:

— every discovered network interface or via network interface exposed service in factory default state is documented; and

— for all network interfaces or via network interface exposed services in factory default state there is evidence provided that they are necessary to setup the equipment or for the basic operation according to [E.Doc.Setup] and [E.Doc.NetworkInterfaces.exposure]. There is no evidence that the implementation of the network interfaces or via the network interfaces exposes services which differs from its documentation.

The verdict NOT APPLICABLE is assigned if:

— There is no physical connection via network interfaces available in factory default state of the equipment

The verdict FAIL is assigned otherwise.

5.10.2.4.5 Functional sufficiency assessment

None

5.10.3 [GEC-3] Configuration of optional services and the related exposed network interfaces

5.10.3.1 Requirement

Optional network interfaces or services exposed via network interfaces affecting security or network assets, which are part of the factory default state of the equipment shall have the option for an authorized user to be able to enable and disable the interface or service.

5.10.3.2 Rationale

This will reduce the attack surface related to network interfaces and to the services exposed via these.

5.10.3.3 Guidance

The equipment provides a functionality to configure (enable/disable) the optional services and the related exposed network interfaces.

The configuration of network related services ought to be protected according to Access control mechanism (ACM) and Authentication mechanism (AUM).

5.10.3.4 Assessment criteria

5.10.3.4.1 Assessment objective

The assessment addresses the requirement GEC-3.

5.10.3.4.2 Required information

[E.Doc.NetworkInterfaces.exposure] Documentation of network interfaces and exposed services via network interfaces which are part of the factory default state of the equipment. This documentation needs to include the information for each network interface or exposed service via network interfaces if they are required for the basic operation or for the setup of the equipment or if they are optional

[E.Doc.configuration] configuration instructions

[E.Doc.SecurityAsset.GEC-3] Documentation of each security asset that is accessible via network interfaces.

[E.Doc.NetworkAsset.GEC-3] Documentation of each network asset that is accessible via network interfaces.

[E.Just.NetworkInterfaces.exposureRisk] Documented analysis, rationale and verdict regarding the risk for the security assets documented in [E.Doc.SecurityAsset.GEC-3] and network assets documented in [E.Doc.NetworkAsset.GEC-3] related to the exposure of network interfaces and services via network interface which are part of the factory default state.

5.10.3.4.3 Conceptual assessment

5.10.3.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each optional via network interface exposed service which is part of the factory default state of the equipment is configurable, at least with the option to enable and disable the service.

5.10.3.4.3.2 Preconditions

None

5.10.3.4.3.3 Assessment units

- Assessment based on [E.Just.NetworkInterfaces.exposureRisk] for each network exposed service in [E.Doc.NetworkInterfaces.exposure]whether the associated risk was justified in relation to security and network assets

- Assessment based on [E.Doc.NetworkInterfaces.exposure] and based on [E.Doc.configuration] if the optional exposed network interfaces and via network interfaces exposed optional services which are part of the factory default state are configurable with at least the option to enable and disable the optional network interface or via network interfaces exposed optional services**.**

5.10.3.4.3.4 Assignment of verdict

The verdict PASS is assigned if for each network interface and via network interface exposed service of the equipment:

- the configuration, at least with the option to enable and disable the network interface or services exposed via network interfaces, which are part of the factory default state, described in [E.Doc.configuration] and in [E.Doc.NetworkInterfaces.exposure] is possible for all optional network interfaces and via network interface exposed optional services.

- There is no optional documented network related exposure of services in [E.Doc.NetworkInterfaces.exposure] available

The verdict FAIL is assigned otherwise.

5.10.3.4.4 Functional completeness assessment

5.10.3.4.4.1 Assessment purpose

The purpose of this assessment case is the functional validation to proof that all optional network interfaces and via network exposed optional services which are part of the factory default state are

configurable, at least with the option to enable and disable the service. Therefore, the completeness of documentation and also the correctness of the implementation needs to be examined.

5.10.3.4.4.2 Preconditions

The equipment is operational and if available the setup is done.

Physical network connection to check exposure of services via network interfaces is established.

5.10.3.4.4.3 Assessment units

- Functionally assessment whether there are optional network interfaces or services activated and exposed via network interfaces, which are not listed in [E.Doc.NetworkInterfaces.exposure] or [E.Doc.configuration] or are not configured to be active.

- Search to reveal any via the equipment exposed network interface or via network interface exposed services, even if the related services are not activated or documented in [E.Doc.NetworkInterfaces.exposure].

5.10.3.4.4.4 Assignment of verdict

The verdict PASS is assigned if:

- every discovered via network exposed interface or service is documented; and

- for all optional network interfaces or via network interfaces exposed optional services there is evidence provided they are configurable, at least with the option to enable and disable.

- There is no evidence that the implementation of optional network interfaces and optional via network exposed services differs from its documentation.

The verdict FAIL is assigned otherwise.

5.10.3.4.5 Functional sufficiency assessment

None

5.10.4 [GEC-4] Documentation of exposed services via network interfaces

5.10.4.1 Requirement

The equipment's user documentation shall contain a description of all services which are exposed via network interfaces and which are delivered as part of the factory default state.

5.10.4.2 Rationale

The equipment itself and the surrounding network needs to be configured properly to assure functionality of the equipment and to support the security of the network. Therefore, it is important to provide user information regarding the exposed network services.

5.10.4.3 Guidance

All services that are exposed via network interfaces are to be listed in the documentation. In addition to the list of services, the description of the services could contain the purpose of each service.

The influence of the manufacturer on the configuration of the equipment can vary.

Generally, a differentiation is to be made between two types of equipment:

— Multipurpose equipment (e.g., Smartphones, Laptops): Offered services and functionality of multipurpose equipment are only under the control of the manufacturer until they are delivered. The activated and documented network services can only be influenced before the equipment is delivered. Services provided by general purpose operating systems, e.g. Windows or Android could be excluded as long there are not under the control of the manufacturer.

— Equipment with a controlled fixed functionality (e.g., Sensors, Routers): Offered services and functionality of the equipment are embedded in an equipment-specific software (firmware) which is provided by the manufacturer. The activated and documented network services can be influenced during the lifecycle of the equipment.

5.10.4.4 Assessment criteria

5.10.4.4.1 Assessment objective

The assessment addresses the requirement GEC-4.

5.10.4.4.2 Required information

[E.Doc.UserDoc.NetworkInterfaces.exposure] User documentation of network interfaces and exposed services via network interfaces in factory default state of the equipment. This documentation needs to include the information and description for each network interface or exposed service via network interfaces and if they are required for the basic operation or for the setup of the equipment or if they are optional.

5.10.4.4.3 Conceptual assessment

5.10.4.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether all services which are exposed via network interfaces and are delivered as part of the factory default state are described in the user documentation.

5.10.4.4.3.2 Preconditions

None.

5.10.4.4.3.3 Assessment units

— Assessment based on [E.Doc.UserDoc.NetworkInterfaces.exposure] for each network exposed service whether it is described in the user documentation, and also it is stated if the services is required for setup or to operate the equipment in the intended operational environment of use or if it is an optional service.

5.10.4.4.3.4 Assignment of verdict

The verdict PASS is assigned if for each via network exposed service of the equipment:

— there is a description in the user documentation and also it is stated if the service is required for setup or to operate the equipment in the intended operational environment of use or if it is an optional service.

— The description in the user documentation is not in contradiction with the information provided in [E.Doc.UserDoc.NetworkInterfaces.exposure]

The verdict FAIL is assigned otherwise.

5.10.4.4.4 Functional completeness assessment

None.

5.10.4.4.5 Functional sufficiency assessment

None.

5.10.5 [GEC-5] No unnecessary external interfaces

5.10.5.1 Requirement

Equipment shall only make external interfaces necessary for:

— the “equipment’s intended use”; and

— the “intended operational environment of use”.

5.10.5.2 Rationale

External communication interfaces need to be kept to the minimum in order to minimise the potential attack surface.

5.10.5.3 Guidance

In cases where unnecessary external interface is physically protected by its intended operational environment of use and cannot be attacked, then this is considered as not provided by the equipment. Interfaces that are disabled or blocked are considered as not provided by the equipment.

External interfaces on equipment might include interfaces that are intentionally used for internal system communication.

5.10.5.4 Assessment criteria

5.10.5.4.1 Assessment objective

The assessment addresses the requirement GEC-5.

5.10.5.4.2 Required information

If the equipment implements a setup process

— [E.Doc.setup] Complete Setup instructions for the equipment

If non-network related external interfaces are available

— [E.Doc.NonNetworkInterfaces] Documentation of non-network related external interfaces

— [E.Doc.SecurityAsset.GEC-5] Documentation of each security asset that is accessible via non-network related interfaces.

— [E.Doc.NetworkAsset.GEC-5] Documentation of each network asset that is accessible via non-network related interfaces.

— [E.Just.NonNetworkInterfaces.exposureRisk] Documented analysis, rationale and verdict regarding the risk for the security assets documented in [E.Doc.SecurityAsset.GEC-3] and network assets documented in [E.Doc.NetworkAsset.GEC-3] related to the exposure of non-network related external interfaces.

5.10.5.4.3 Conceptual assessment

5.10.5.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each exposure external interfaces in factory default state of the equipment is restricted to the ones which are necessary for equipment setup or to operate as intended in the intended operational environment of use.

5.10.5.4.3.2 Preconditions

None.

5.10.5.4.3.3 Assessment units

Based on [E.Just.NonNetworkInterfaces.exposureRisk] for each non-network related externally exposed interface in [E.Doc.NonNetworkInterfaces] check whether the interface is necessary for setup of the equipment as described in [E.Doc.setup] or is necessary to operate the equipment as intended and in the intended operational environment of use and also the associated risk was justified in relation to security and network assets.

5.10.5.4.3.4 Assignment of verdict

The verdict PASS is assigned if for each non-network related external Interface of the equipment:

— the exposure of the in [E.Doc.NonNetworkInterfaces] listed external communication interfaces are limited to non-network related external interfaces which are required for setup described in [E.Doc.setup] or to operate the equipment as intended in the intended operational environment of use.

— The associated risk described in [E.Just.NonNetworkInterfaces.exposureRisk] was justified in relation to security and network assets in consideration of the intended use and the intended operational environment of use.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— There are no non-network related external interfaces available at the equipment

The verdict FAIL is assigned otherwise.

5.10.5.4.4 Functional completeness assessment

5.10.5.4.4.1 Assessment purpose

The purpose of this test case is the functional validation to ensure that only external interfaces which are required for setup or to operate the equipment as intended in the intended operational environment of use are exposed concerning to completeness of the documentation and the correctness of implementation.

5.10.5.4.4.2 Preconditions

The equipment is in the factory default state and if available setup and configuration did take place already.

5.10.5.4.4.3 Assessment units

— Functionally assessment whether there are further external non-network interfaces exposed, which are not listed in [E.Doc.NonNetworkInterfaces] or are not required for setup according to [E.Doc.Setup] or to operate the equipment as intended and in the intended operational environment of Use.

— Search to reveal and access any via the equipment exposed non-network related external interfaces even if the related function is not activated or documented in [E.Doc.NonNetworkInterfaces].

5.10.5.4.4.4 Assignment of verdict

The verdict PASS is assigned if:

— every revealed external non- network related interface is documented; and

— for all external non-network related interfaces there is evidence provided that they are necessary to setup the equipment according [E.Doc.Setup] or to operate the equipment as intended in the intended operational environment of use.

— If there were revealed non-network related interfaces which are not necessary for setup the equipment according [E.Doc.Setup] or to operate the equipment as intended in the intended operational environment of use the associated risk described in [E.Just.NonNetworkInterfaces.exposureRisk] justifies in relation to security and network assets why the interface is still made accessible.

— There is no evidence that the implementation of external non-network related interfaces differs from its documentation.

The verdict NOT APPLICABLE is assigned if:

— There are no non-network related external interfaces available at the equipment

The verdict FAIL is assigned otherwise.

5.10.5.4.5 Functional sufficiency assessment

None.

5.10.6 [GEC-7] Input validation

5.10.6.1 Requirement

The equipment shall use input validation functionality on external interface inputs to prevent the corruption, extraction or misuse of security assets and network assets and the loss of functionality.

5.10.6.2 Rationale

Input validation is necessary to validate that any input that is provided to the equipment is compliant to the expected input and has the properties that are required to process the data correctly.

Improper input validation is regarded as one of the most common and dangerous software weaknesses which also contributes to several other software weaknesses like out-of-bounds write, and improper neutralization which can lead to various injection vulnerabilities (e.g., SQL injection, OS command injection and path traversal).

Especially data from potentially untrusted sources like any input received via network interfaces, need to be subject to input validation by checking the input for both syntax and semantics correctness. These checks ought to be done as early as possible when processing any input to avoid propagating invalid and perhaps even malicious input. The necessary rigor is related to the:

— risks to the assets; and

— syntax and semantics checks related to the input data type; and

— trustworthiness of the source that provided the input.

5.10.6.3 Guidance

Improper input validation is one of the root causes for many security vulnerabilities, input can only be successfully processed when it has been established that the input is valid by checking the syntax and semantics of the input, both on the raw data and metadata.

Syntax validation is checking the input is delivered in the correct structure, for instance:

— the format of a date entry (e.g., dd-mm-yyyy or mm-dd-yyyy);

— the use of a decimal point or comma in a numeric input;

— the length of a text input;

— correct headers and structures for various file types (e.g., validate a .ZIP. .BMP or .JPEG file structure);

— a valid json, xml or html file.

Semantics validation is checking that the input is delivered with correct values, for instance:

— a value that is outside the expected range (e.g., a number that is too small or too large, a birthday in the future);

— special characters which are not be allowed in a text input, e.g., special escape characters used for SQL injection ;

— incorrect data size and offset values in a structure (e.g., an incorrect size might cause a buffer overrun when data is copied without checks, or a negative offset might copy incorrect data from the stack);

Using regular expressions is one method to validate for instance text input, a developer could also consider other techniques to ensure an input can be successfully processed such as filtering and encoding.

Further guidance's to be considered are:

— Common Weakness Enumeration: Improper input validation (CWE-20), encoding/escaping (CWE-116), Improper Neutralization of Special Elements (CWE-138) and filtering (CWE-790);

— Open Web Application Security Project (OWASP) Input Validation Cheat Sheet;

— IEC EN 62443-4-2[2] CR 3.5 (Input validation) and

— ETSI EN 303 645[5] 5.13 (Validate input data).

5.10.6.4 Assessment criteria

5.10.6.4.1 Assessment objective

The assessment addresses the requirement GEC-7.

5.10.6.4.2 Required information

[E.Doc.DT.GEC-7] Description of the selected path through the decision tree in Figure 24for each of the external network interfaces and user interfaces.

[E.Just.DT.GEC-7] Justification for the selected path through the decision tree in Figure 24 for each of the external network interfaces and user interfaces.

[E.Doc.GEC-7] Complete documentation of all external network interfaces and user interfaces including information on any used APIs, protocols, input data types, file formats and whether syntactic and semantic correctness are checked.

5.10.6.4.3 Conceptual assessment

5.10.6.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the input validation functionality of the equipment is applied to the external network interfaces and user interfaces and provides appropriate protection against common attacks considering the intended use of the equipment and its intended operational environment of use.

5.10.6.4.3.2 Preconditions

None.

5.10.6.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
:For each external interface;
  if (Is the interface capable of recieving input?) then (Yes)
    if (Is this a user interface?) then (\n\nYes)
      if (Is the intended use and functionality \nof the user interface documented
\nincluding any relevant input \ndata types supported?) then (Yes)
        if (Is the syntactic and semantic \ncorrectness checked?) then (No)
           #pink :FAIL\nInput not validated;
           detach;
       else (Yes)
           #lightgreen :PASS\nInput validated;
       endif
        detach;
    else (No)
           #pink :FAIL\nDocumentation\nincomplete;
           detach;
    endif
    else (No)
      if (Is the intended use and functionality \nof the interface documented including
\nany relevant input data types, APIs, \nprotocols, file formats, etc.?) then (No)
```

```
            #pink :FAIL\nDocumentation\nincomplete;
          detach;
        else (Yes)
          if (Is the syntactic and semantic \ncorrectness checked?) then (No)
            #pink :FAIL\nInput not validated;
            detach;
          else (Yes)
            #lightgreen :PASS\nInput validated;
          endif
        endif
        endif
        detach;
    detach;
    else (No)
     #application :NOT APPLICABLE\nInterface does not \nprocess input;
     detach;
    endif
@enduml
```

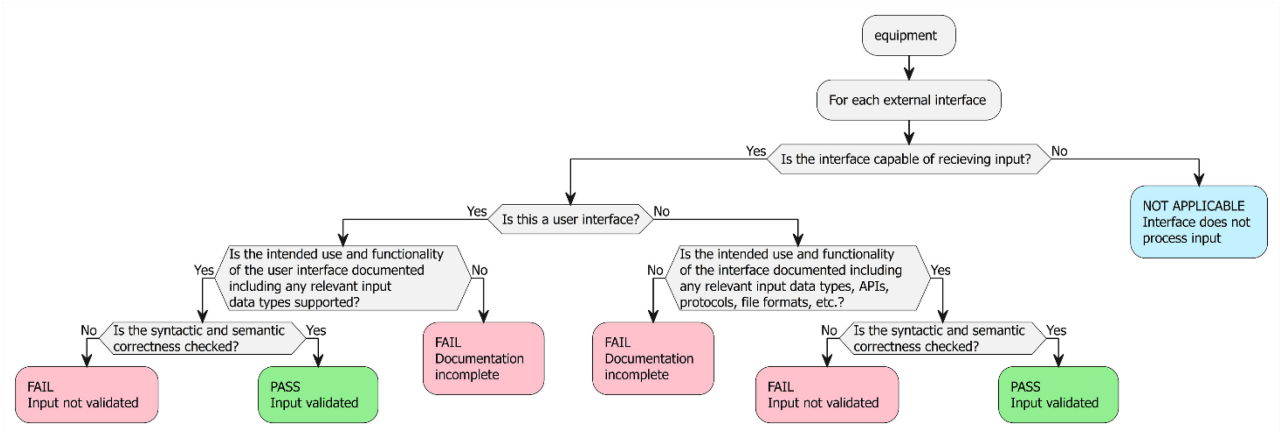

Figure 23 — Decision Tree for requirement GEC-7.

For each external interface documented [E.Doc.GEC-7], check whether the path through the decision tree documented in [E.Doc.DT.GEC-7] ends with “PASS” or “NOT APPLICABLE”.

For each path through the decision tree documented in [E.Doc.DT.GEC-7], examine its justification documented in [E.Just.DT.GEC-7].

5.10.6.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— all paths through the decision tree ends with “PASS” or “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.10.6.4.4 Functional completeness assessment

5.10.6.4.4.1 Assessment purpose

The purpose of this test case is the functional assessment of the techniques to verify the completeness of the documentation.

5.10.6.4.4.2 Preconditions

— The equipment is in an operational state and all external network interfaces and user interfaces, which are part of the intended use, are either enabled or configurable to be enabled, so that each external network interface and user interface can be tested.

— Where authentication is necessary to access an external interface, a means is provided to be able to test the interface.

5.10.6.4.4.3 Assessment units

Functionally assess whether there exist further external network interfaces and user interfaces, which are not listed in [E.Doc.GEC-7].

5.10.6.4.4.4 Assignment of verdict

The verdict PASS is assigned if all external network interfaces and user interfaces are documented.

The verdict FAIL is assigned otherwise.

5.10.6.4.5 Functional sufficiency assessment

5.10.6.4.5.1 Assessment purpose

The purpose of this test case is the functional assessment of the techniques to verify the implementation of the documented techniques.

5.10.6.4.5.2 Preconditions

— The equipment is in an operational state and all external network interfaces and user interfaces, which are part of the intended use, are either enabled or configurable to be enabled, so that each external network interface and user interface can be tested.

— Where authentication is necessary to access an external interface, a means is provided to be able to test the interface.

— Test tools such as but not limited to protocol analysers, input validation testing tools and fuzzing tools.

5.10.6.4.5.3 Assessment units

Functionally assess whether the external network interfaces and user interfaces are resilient against common input attacks considering their functionality, intended use of the equipment and its intended operational environment of use.

5.10.6.4.5.4 Assignment of verdict

The verdict PASS is assigned if all input validation attack attempts were unsuccessful in breaking the equipment's functionality or able to corrupt, extract or misuse any of the assets.

The verdict FAIL is assigned otherwise.

5.11 [CRY] Cryptography

5.11.1 [CRY-1] Best practice Cryptography

5.11.1.1 Requirement

The equipment shall use best practice for cryptography that is used for the protection of the security or network assets.

5.11.1.2 Rationale

Cryptography that is not strong enough for a use case e.g. because it is not suitable or broken and used for the protection of assets poses a security risks to these assets. Using best practices or even more advanced, evidently suitable cryptography supports trust in the cryptographic protection of these assets.

If a cryptographic algorithm is cracked or cryptographic primitives are compromised, it may be necessary to update the equipment accordingly (see requirement SUM) in order to preserve the protection of the assets the cryptography protects. While there is no absolute guarantee that this does not happen to any cryptography that is considered as best practice, it is more likely that cryptography becomes unsuitable for a certain use case, when there is already evidence that such cryptography might become deprecated within the intended lifetime of the equipment.

However, e.g. if the equipment contains a hardware based crypto accelerators that can itself communicate over the internet, it might not be able to be prepared to update cryptography. In these cases it is important that there is no evidence that the cryptography will not be best practice within the intended life time.

5.11.1.3 Guidance

There exists various security guidance that can be used to identify best practices for cryptography, see respective ISO/IEC standards, publicly available crypto catalogues provided by SDOs and public authorities such as sogis.eu , “SOGIS agreed Cryptographic Mechanisms” Vers.1.3 , February 2023 and guidance provided by ENISA and national agencies.

A commonly used cryptographic method for a certain use case, with the lack of evidence for a feasible attack with current readily available techniques, can be considered as best practice.

However, it is also possible to provide evidence, that new cryptography is suitable for a certain use case and can therefore be considered as best practice for cryptography.

Cryptography is often used for protecting the relevant assets, for example:

— Authentication (see AUM),

— Secure update (see SUM),

— Secure storage (see SSM),

— Secure communication (see SCM) and

— Confidential Cryptographic key Generation (see CCK-2).

Cryptographic protection might not be compliant with best practice cryptography if interoperability with legacy systems is required.

If reviewed or evaluated implementations according to the state of the art are publicly available, these may be preferable used to deliver network and security functionalities, particularly in the field of cryptography.

To maintain best practices for cryptography within the intended life time of the equipment concepts to consider are crypto agility additional to the capability of updating cryptography on the equipment in accordance to [SUM].

Elements to observe for the preparation of updating cryptography are amongst others:

— cryptographic schemes, protocols, algorithms, constructors and primes,

— the form of sensitive security parameters being used, and

— specific SSPs, such as roots of trust.

For equipment that cannot have their cryptographic algorithms or primitives updated for example if the implementation or part uses a hardware-based root of trust, it is important that the intended lifetime of the equipment does not exceed the recommended usage lifetime of the cryptographic algorithms and primitives used by the equipment.

5.11.1.4 Assessment criteria

5.11.1.4.1 Assessment objective

The assessment addresses the requirement CRY-1.

5.11.1.4.2 Required information

[E.Doc.DT.CRY-1] Description of the selected path through the decision tree in Figure 25 for each security and network asset.

[E.Just.DT.CRY-1] Justification for the selected path through the decision tree in Figure 25 for each security and network asset.

[E.Doc.SecurityAsset.CRY] Documentation of each security asset that is protected by cryptography.

[E.Doc.NetworkAsset.CRY] Documentation of each network asset that is protected by cryptography.

[E.Doc.SecurityAsset.CRY.CryptoProtect] Documentation of each cryptographic protection for each security asset documented in [E.Doc.SecurityAsset.CRY].

[E.Doc.NetworkAsset.CRY.CryptoProtect] Documentation of each cryptographic protection for each network asset documented in [E.Doc.NetworkAsset.CRY].

NOTE The documentation of a cryptographic protection includes the security properties provided by cryptography.

[E.Doc.CRY-1] Documentation of each used cryptography for each cryptographic protection for each security and network asset.

NOTE Cryptography used for cryptographic protection can amongst others include cryptographic schemes, algorithms, constructors and primes.

5.11.1.4.3 Conceptual assessment

5.11.1.4.3.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the implemented cryptography for protecting security or network assets is considered as best practices.

5.11.1.4.3.2 Preconditions

None.

5.11.1.4.3.3 Assessment units

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
    :For each security and network asset;
      if (Does the equipment use cryptography\nfor the protection of the security or
network asset?) then (No)
        #application :NOT APPLICABLE\nCryptogaphy not used for protection;
        detach;
      else (Yes)
        :For each cryptoraphic protection of the security or network asset;
          :For each cryptography used for cryptographic protection;
            if (Is the cryptography best practices\nconcerning the protection of the
\nsecurity asset or network asset?) then (No)
              #pink :FAIL\nCryptogaphy is not best practice;
              detach;
            else (Yes)
              #lightgreen :PASS\nCryptogaphy is best practice;
              detach;
            endif
      endif
@enduml
```

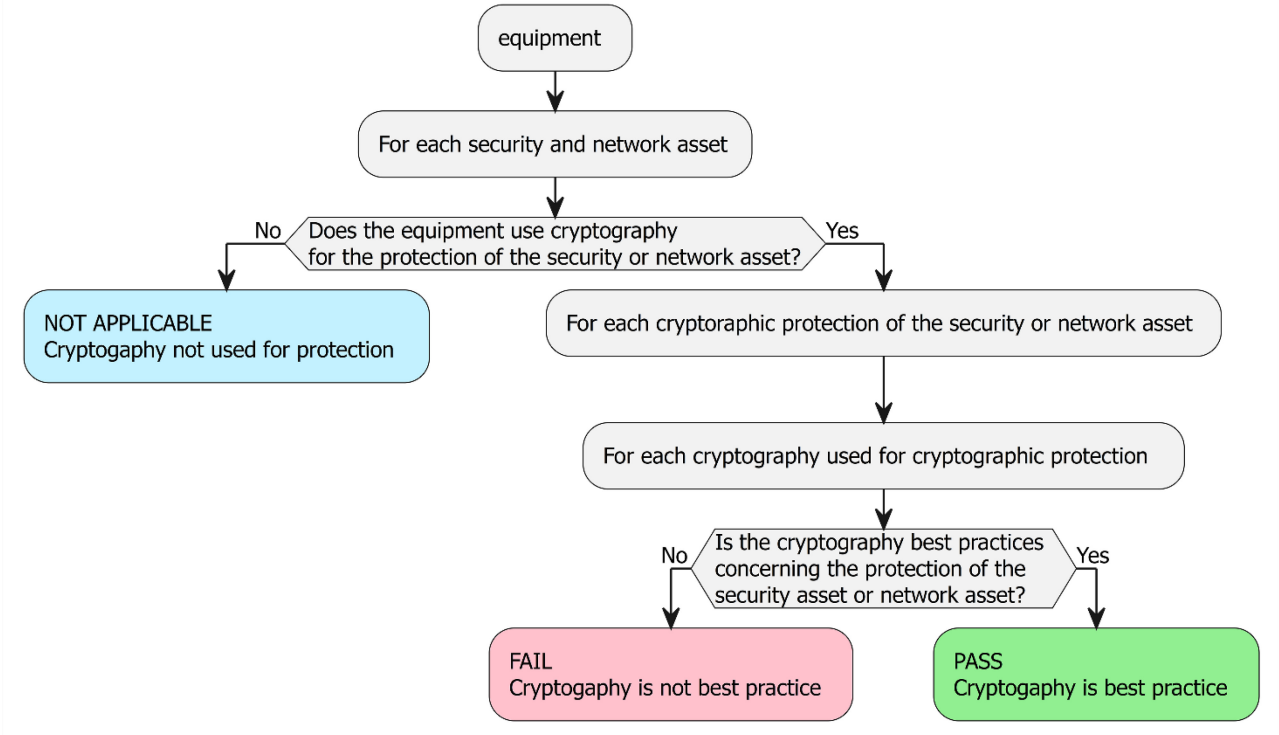

Figure 24 — Decision Tree for requirement CRY-1.

For each security asset documented in [E.Doc.SecurityAsset.CRY] and network asset documented in [E.Doc.NetworkAsset.CRY] , for each cryptographic protection [E.Doc.SecurityAsset.CRY.CryptoProtect] and [E.Doc.NetworkAsset.CRY.CryptoProtect] and for each cryptography documented in [E.Doc.CRY-1], check whether the path through the decision tree documented in [E.Doc.DT.CRY-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Doc.DT.CRY-1], examine its justification documented in [E.Just.DT.CRY-1].

5.11.1.4.3.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

— at least one path through the decision tree ends with “PASS”; and

— no path through the decision tree ends with “FAIL”; and

— all justifications are valid.

The verdict NOT APPLICABLE for the assessment case is assigned if:

— all path through the decision tree end with “NOT APPLICABLE”; and

— all justifications are valid.

The verdict FAIL for the assessment case is assigned otherwise.

5.11.1.4.4 Functional completeness assessment

5.11.1.4.4.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation in [E.Doc.CRY-1] is complete.

5.11.1.4.4.2 Preconditions

The equipment is in an operational state.

5.11.1.4.4.3 Assessment units

For each cryptographic protection documented in [E.Doc.SecurityAsset.CRY.CryptoProtect] and [E.Doc.NetworkAsset.CRY.CryptoProtect], functionally assess whether there is cryptography used on the equipment, which is not documented in [E.Doc.CRY-1].

5.11.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all cryptography found on the equipment are documented in [E.Doc.CRY-1].

The verdict FAIL for the assessment case is assigned if cryptography is found on the equipment that is not documented in [E.Doc.CRY-1].

5.11.1.4.5 Functional sufficiency assessment

None.

Annex A
(informative)

Rationale

A.1 General

This annex provides a rationale for terms and concepts related to this document.

A.2 Rationale

A.2.1 Family of standards

This document belongs to a set of three standards to address the essential requirements defined in articles 3.3.d, 3.3e and 3.3.f of Directive 2014/53/EU and activated by the Commission Delegated Regulation (EU) 2022/30. By using the Radio Equipment Directive, a first step has been made to start to enforce cybersecurity requirements for placing radio equipment on the European market, because a lack of security was and is an increasing concern for society, especially for consumer IoT equipment.

While the three standards focus on different essential requirements (harm to the network, personal data and privacy and protection from (financial) fraud) there are both unique and overlapping requirements in each of them that will require the implementation an increasing number of stronger security controls to protect the network, privacy, and financial assets operating within a developing threat landscape.

Whether one or multiple standards need to be applied to a specific radio equipment is a consideration that must be made through a risk assessment by the economic operator on the need to fulfil the essential requirements of the Radio Equipment Directive. The RED and Blue guides of the European Commission can provide more guidance on this topic.

A.2.2 Security by design

Effective security management requires established security by design processes. This is not covered by this document which defines common security requirements for the equipment. Examples of security by design process standards which would aid in the ability to satisfy the security requirements include:

— IEC 62443-4-1[1]: Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

— NIST 800-160[14]: Systems Security Engineering; Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

— NIST 800-218[15]: Secure Software Development Framework (SSDF)

— Microsoft Security Development Lifecycle (SDL)

— SAFECode Fundamental Practices for Secure Software Development

A.2.3 Assets

To ensure requirements can be aligned across the three horizontal standards - each addressing a specific essential requirement - assets (derived from the essential requirements) have been introduced as the main targets against which to align the requirements:

Table A.1

	3.3.d	3.3.e	3.3.f
Security asset	✓	✓	✓
Network asset	✓		
Privacy asset		✓	
Financial asset			✓

Protecting an asset is not just about the protection of the specific data stored and communicated or otherwise processed by the equipment, but also includes the protection of the functions and the configuration of these functions as used by the equipment. Therefore, the security functionality in particular to protect the integrity of the equipment is termed Security Asset.

A.2.4 Mechanisms

This standard uses the concept of mechanisms to address specific security requirements to facilitate the applicability and appropriateness of the requirements to different types of equipment implementation and use. As this is a horizontal standard it needs to cover a wide range of products and use cases.

If and how generic security objectives are to be achieved depends on the intended use and the intended operational environment of use. They influence the actual required implementation of security measures and the strength of those controls in a specific equipment. A specific security measure might be appropriate for a product but might be too weak or strong for other products or the same product when used in another environment.

The standard provides specific constraints and assessment questions to guide and avoid the full dependence on a manufacturer's scrutiny towards the necessary security measures to address the security concerns related to the intended use and the intended operational environment of use.

To guide the user of this document as to when to apply a certain mechanism, the first requirement addresses the applicability of the mechanism. These requirements may have an 'unless' component that lists the potential conditions for which the mechanism is not required. If it is determined that the mechanism is not applicable then all further requirements in that specific clause are no longer mandatory.

When a mechanism is needed, the sufficiency is determined by evaluating the appropriateness type of the requirement and assessment criteria. Any supporting requirements in the clause are applicable as well.

This decision must be made for each of the items specified, for example when checking the applicability of a requirement on external interfaces, then the decision whether the requirement and all further requirements need to be fulfilled is determined for each external interface independently.

A.2.5 Assessment criteria

The security mechanisms, functionality or other obligations imposed on the equipment have been defined in terms as precise and objective as possible, without compromising the technology-agnostic spirit of the standard. How the equipment implements each will be instantiated by the manufacturer when providing inputs for the compliance test.

A.2.5.1 Decision trees

When a mechanism or requirement is applicable and or appropriate is dependent on the intended use and intended operational environment of use. This document uses decision trees to aid in the decision making and assessment to provide clear direction. An example is shown below.

```
@startuml
skinparam dpi 600
skinparam defaultFontName Utopia
skinparam defaultFontSize 11
:equipment;
  :For each asset;
    if (Is protection required? ) then (Yes)
      if (Various questions to determine\nif the protection is adequate?) then (Yes)
        #lightgreen :PASS\nProtection is appropriate;
        detach;
        else (No)
         #pink :FAIL\nProtection is not appropriate;
         detach;
      endif
      detach;
    else (No)
      #application :NOT APPLICABLE\nNothing to protect;
      detach;
    endif
@enduml
```

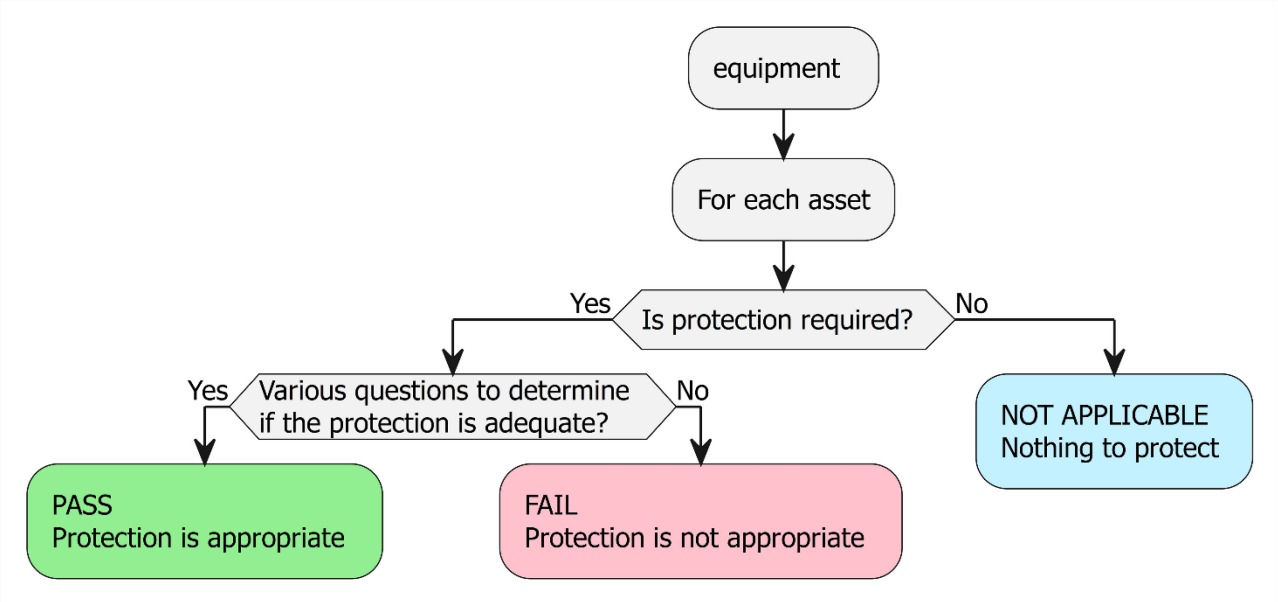

Figure A.1 — Example decision tree

Most decision tree starts with the equipment followed by an element to iterate over (e.g. assets above). For each of those elements questions must be answered on the characteristics of the equipment or related environmental factors. Each decision tree will have at least one or more PASS and FAIL paths and can optionally have one or more NOT APPLICABLE paths. A justification for each selected path will have to be documented.

A.2.5.2 Technical documentation

The assessments depend on the information to be provided as part of the manufacturer's technical documentation. The specific information elements that need to be included in the manufacturers technical documentation for an assessment are indicated as [E.Doc.xxxxx] where xxxxx indicates the

specific desired set of information, for instance [E.Doc.OperationalEnvironment] is the description of the intended operational environment of use for the equipment and [E.Doc.ACM] is the identification of some of the information to be provided for the access control mechanisms assessments.

Some of the expected general information is:

— information on the equipment's intended use

— information on the equipment's expected operational environment of use

— equipment's technical information

— declared state of the art and best practice

— specific details such as a list of external interfaces

— risk assessment

As input for the assessment the paths through the decision trees are indicated as [E.Doc.DT.xxxxxx] and the justification is indicated as [E.Just.DT.xxxxxx]. The table below is just an example of how this could be achieved for the conceptual assessment.

Table A.2

No.	Question	Answer		Rationale/Evidence
1	Intended interface use: Does the interface provide access to network assets or equipment security assets?	Yes (x)	No	Network asset: IP-based communication to the internet Equipment security assets Cloud Account Credentials Common Secret
2	Intended operational environment of use: Does the interface only communicate in trusted networks	Yes	No (x)	It's communicating via the internet
3	Technical interface property: Does the interface require the absence of authentication in order to full-fill its intended use?	Yes	No (x)	No reason for the absence
4	Technical interface property: Does the interface use an authentication mechanism?	Yes (x)	No	Password-based authentication mechanism between the smartphone and the cloud and trust relation based shared secret between Baby monitor and cloud
Assessment case verdict: PASS				

A.2.5.3 Security testing

The adequacy of most security controls is not quantifiable measurable, as there are no equivalents to a thermometer or frequency meter to measure the equipment's security posture or strict definitions to determine when good is good enough.

The outcome therefore is dependent on the evaluator’s knowledge and view of the threat landscape and what is appropriate for a specific equipment in a specific environment, thereby further contributing to the fact that it is difficult to define verifiable, objective, and reproducible test criteria, because even two evaluators might have significantly different views and/or opinions.

Security test tools often use negative testing, demonstrating that certain weaknesses are not manifest, but because security tools are continuously updated, new issues might be found with updated information or when run for a more extensive period - as such this will also not lead to reproducible test results.

The approach taken in this document, therefore, improves the assessment outcome but cannot resolve this issue. Most of the assessments are based on the fact that sufficient information is provided.

A.2.6 Security parameters

A security parameter is information used in security functions to protect assets:

— Per definition, a confidential security parameter (CSP) is secret security related information whose modification or disclosure can compromise the security of an asset. Typical examples are PINs and passwords, symmetric cryptographic keys or private asymmetric cryptographic keys.

— A public security parameter (PSP) is security related public information whose modification can compromise the security of an asset. This means that integrity of PSPs is crucial, but confidentiality of PSPs is not. Typical examples are public cryptographic keys or cryptographic certificates.

— A sensitive security parameter (SSP) is either a CSP or a PSP.

Annex ZA
(informative)

Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered.

This European Standard has been prepared under a Commission's standardization request C(2022) 5637 final to provide one voluntary means of conforming to essential requirements of Directive 2014/53/EU [OJ L 153] of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3).

In case of differences between terms defined in this European standard and terms defined in that Regulation, the terms defined in the Regulation shall prevail.

Once this standard is cited in the Official Journal of the European Union under that Delegated Regulation (EU) 2022/30, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of Directive 2014/53/EU and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Directive 2014/53/EU [OJ L 153]

Essential Requirements of Directive 2014/53/EU	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
3.3.(d)	Clauses 5.1 to 5.11	Covered.
3.3.(e)		
3.3.(f)		

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

Bibliography

[1] IEC EN 62443-4-1, Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

[2] IEC EN 62443-4-2, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

[3] ISO/IEC EN 27002:2022, Information security, cybersecurity and privacy protection - Information security controls

[4] ISO/IEC EN 24760 series, IT Security and Privacy - A framework for identity management

[5] ETSI EN 303 645, Cyber Security for Consumer Internet of Things - Baseline Requirements

[6] ETSI TS 103 701, Cyber Security for Consumer Internet of Things - Conformance Assessment of Baseline Requirements

[7] NIST SP 800-63 series, Digital Identity Guidelines

[8] NIST SP 800-63B, Digital Identity Guidelines - Authentication and Lifecycle Management

[9] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators

[10] NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation

[11] NIST SP 800-90C, Recommendation for Random Bit Generator (RBG) Constructions

[12] NIST SP 800-108r1, Recommendation for Key Derivation Using Pseudorandom Functions

[13] NIST SP 800-132, Recommendation for Password-Based Key Derivation: Part 1: Storage Applications

[14] NIST SP 800-160, Engineering Trustworthy Secure Systems

[15] NIST SP 800-218, Secure Software Development Framework (SSDF) - Recommendations for Mitigating the Risk of Software Vulnerabilities

[16] BSI AIS 31, A Proposal for Functionality Classes for Random Number Generators

[17] FIPS 140-2, Security Requirements for Cryptographic Modules

[18] FIPS 140-3, Security Requirements for Cryptographic Modules