

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                           |                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | DIN EN 18031-1            |  |
| ICS 33.060.20; 35.030                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Einsprüche bis 2024-07-03 |                                                                                     |
| <div>Entwurf</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                           |                                                                                     |
| <p><b>Gemeinsame Sicherheitsanforderungen für Funkanlagen –<br/>Teil 1: Funkanlagen mit Internetanschluss;<br/>Deutsche und Englische Fassung prEN 18031-1:2023</b></p> <p>Common security requirements for radio equipment –<br/>Part 1: Internet connected radio equipment;<br/>German and English version prEN 18031-1:2023</p> <p>Exigences de sécurité communes applicables aux équipements radioélectriques connectés à<br/>l'internet;<br/>Version allemande et anglaise prEN 18031-1:2023</p> <p><b>Anwendungswarnvermerk</b></p> <p>Dieser Entwurf mit Erscheinungsdatum 2024-05-03 wird der Öffentlichkeit zur Prüfung und Stellungnahme<br/>vorgelegt.</p> <p>Weil das beabsichtigte Dokument von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses<br/>Entwurfs besonders zu vereinbaren.</p> <p>Stellungnahmen werden erbeten</p> <ul style="list-style-type: none"><li>– vorzugsweise online im Norm-Entwurfs-Portal von DIN unter <a href="http://www.din.de/go/entwuerfe">www.din.de/go/entwuerfe</a> bzw. für Norm-<br/>Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter <a href="http://www.entwuerfe.normenbibliothek.de">www.entwuerfe.normenbibliothek.de</a>,<br/>sofern dort wiedergegeben;</li><li>– oder als Datei per E-Mail an <a href="mailto:nia@din.de">nia@din.de</a> möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im<br/>Internet unter <a href="http://www.din.de/go/stellungnahmen-norm-entwuerfe">www.din.de/go/stellungnahmen-norm-entwuerfe</a> oder für Stellungnahmen zu Norm-<br/>Entwürfen der DKE unter <a href="http://www.dke.de/stellungnahme">www.dke.de/stellungnahme</a> abgerufen werden;</li><li>– oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin<br/>oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.</li></ul> <p>Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind,<br/>mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.</p> <p>Gesamtumfang 253 Seiten</p> <p>DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)</p> |                           |                                                                                     |

## 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 beigelegt. 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](http://www.din.de)) durch eine Suche nach der Dokumentennummer aufgerufen werden.

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

## Inhalt

|                                                                                                                     | Seite |
|---------------------------------------------------------------------------------------------------------------------|-------|
| Europäisches Vorwort . . . . .                                                                                      | 5     |
| Einleitung . . . . .                                                                                                | 6     |
| 1 Anwendungsbereich . . . . .                                                                                       | 7     |
| 2 Normative Verweisungen . . . . .                                                                                  | 7     |
| 3 Begriffe . . . . .                                                                                                | 7     |
| 4 Anwendung dieser Norm . . . . .                                                                                   | 11    |
| 5 Anforderungen . . . . .                                                                                           | 13    |
| 5.1 [ACM] Zugangssteuerungsmechanismus (en: Access Control Mechanism) . . . . .                                     | 13    |
| 5.1.1 [ACM-1] Anwendbarkeit von Zugangssteuerungsmechanismen . . . . .                                              | 13    |
| 5.1.2 [ACM-2] Angemessene Zugangssteuerungsmechanismen . . . . .                                                    | 17    |
| 5.2 [AUM] Authentisierungsmechanismus (en: Authentication Mechanism) . . . . .                                      | 20    |
| 5.2.1 [AUM-1] Anwendbarkeit von Authentisierungsmechanismen für externe Schnittstellen . . . . .                    | 21    |
| 5.2.2 [AUM-2] Angemessene Authentisierungsmechanismen für externe Schnittstellen . . . . .                          | 27    |
| 5.2.3 [AUM-3] Authentifikator-Validierung . . . . .                                                                 | 30    |
| 5.2.4 [AUM-4] Änderung von Authentifikatoren . . . . .                                                              | 33    |
| 5.2.5 [AUM-5] Verhinderung von statischen und Vorgabewerten . . . . .                                               | 37    |
| 5.2.6 [AUM-6] Schutz vor Brute-Force-Angriffen . . . . .                                                            | 41    |
| 5.3 [SUM] Sicherer Aktualisierungsmechanismus (en: Secure Update Mechanism) . . . . .                               | 44    |
| 5.3.1 [SUM-1] Anwendbarkeit von Aktualisierungsmechanismen . . . . .                                                | 44    |
| 5.3.2 [SUM-2] Sichere Aktualisierungen . . . . .                                                                    | 48    |
| 5.3.3 [SUM-3] Automatisierte Aktualisierungen . . . . .                                                             | 52    |
| 5.4 [SSM] Sicherer Speichermechanismus (en: Secure Storage Mechanism) . . . . .                                     | 55    |
| 5.4.1 [SSM-1] Anwendbarkeit von sicheren Speichermechanismen . . . . .                                              | 55    |
| 5.4.2 [SSM-2] Angemessener Integritätsschutz für sichere Speichermechanismen . . . . .                              | 59    |
| 5.4.3 [SSM-3] Angemessener Vertraulichkeitsschutz für sichere Speichermechanismen . . . . .                         | 61    |
| 5.5 [SCM] Sicherer Kommunikationsmechanismus (en: Secure Communication Mechanism) . . . . .                         | 64    |
| 5.5.1 [SSM-1] Anwendbarkeit von sicheren Kommunikationsmechanismen . . . . .                                        | 64    |
| 5.5.2 [SCM-2] Angemessener Integritäts- und Authentizitätsschutz für sichere Kommunikationsmechanismen . . . . .    | 68    |
| 5.5.3 [SCM-3] Angemessener Vertraulichkeitsschutz für sichere Kommunikationsmechanismen . . . . .                   | 72    |
| 5.5.4 [SCM-4] Angemessener Wiederholungsschutz für sichere Kommunikationsmechanismen . . . . .                      | 75    |
| 5.6 [RLM] Resilienzmechanismus (en: Resilience Mechanism) . . . . .                                                 | 79    |
| 5.6.1 [RLM-1] Anwendbarkeit von Resilienzmechanismen . . . . .                                                      | 79    |
| 5.7 [NMM] Netzwerküberwachungsmechanismus (en: Network Monitoring Mechanism) . . . . .                              | 83    |
| 5.7.1 [NMM-1] Anwendbarkeit eines angemessenen Netzwerküberwachungsmechanismus . . . . .                            | 83    |
| 5.8 [TCM] Verkehrssteuerungsmechanismus (en: Traffic Control Mechanism) . . . . .                                   | 87    |
| 5.8.1 [TCM-1] Anwendbarkeit eines angemessenen Verkehrssteuerungsmechanismus . . . . .                              | 87    |
| 5.9 [CCK] Vertrauliche kryptographische Schlüssel (en: Confidential Cryptographic Keys) . . . . .                   | 90    |
| 5.9.1 [CCK-1] Angemessene vertrauliche kryptographische Schlüssel (CCKs) . . . . .                                  | 90    |
| 5.9.2 [CCK-2] Mechanismen zur Erzeugung vertraulicher kryptographischer Schlüssel . . . . .                         | 92    |
| 5.9.3 [CCK-3] Keine fest einprogrammierten vertraulichen kryptographischen Schlüssel . . . . .                      | 95    |
| 5.9.4 [CCK-4] Verhinderung von statischen Vorgabewerten für vertrauliche kryptographische Schlüssel . . . . .       | 97    |
| 5.10 [GEC] Allgemeine Gerätefähigkeiten (en: General Equipment Capabilities) . . . . .                              | 101   |
| 5.10.1 [GEC-1] Aktuelle Software und Hardware ohne öffentlich bekannte ausnutzbare Schwachstellen . . . . .         | 101   |
| 5.10.2 [GEC-2] Begrenzung der Offenlegung von Diensten über entsprechende Netzwerkschnittstellen . . . . .          | 103   |
| 5.10.3 [GEC-3] Konfiguration von optionalen Diensten und zugehörigen offengelegten Netzwerkschnittstellen . . . . . | 106   |

|                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                       |     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----|
| 5.10.4                                                                                                                                                                                                                                                                                                                                                                                             | [GEC-4] Dokumentation von über Netzwerkschnittstellen zugänglichen Diensten . . . . . | 108 |
| 5.10.5                                                                                                                                                                                                                                                                                                                                                                                             | [GEC-5] Keine unnötigen externen Schnittstellen . . . . .                             | 110 |
| 5.10.6                                                                                                                                                                                                                                                                                                                                                                                             | [GEC-7] Eingabevalidierung . . . . .                                                  | 112 |
| 5.11                                                                                                                                                                                                                                                                                                                                                                                               | [CRY] Kryptographie (en: Cryptography) . . . . .                                      | 117 |
| 5.11.1                                                                                                                                                                                                                                                                                                                                                                                             | [CRY-1] Bewährte Verfahrensweisen für Kryptographie . . . . .                         | 117 |
| Anhang A (informativ) Begründung . . . . .                                                                                                                                                                                                                                                                                                                                                         |                                                                                       | 122 |
| A.1                                                                                                                                                                                                                                                                                                                                                                                                | Allgemeines . . . . .                                                                 | 122 |
| A.2                                                                                                                                                                                                                                                                                                                                                                                                | Begründung . . . . .                                                                  | 122 |
| A.2.1                                                                                                                                                                                                                                                                                                                                                                                              | Normenfamilie . . . . .                                                               | 122 |
| A.2.2                                                                                                                                                                                                                                                                                                                                                                                              | Sicherheit durch Gestaltung (en: Security by Design) . . . . .                        | 122 |
| A.2.3                                                                                                                                                                                                                                                                                                                                                                                              | Werte . . . . .                                                                       | 123 |
| A.2.4                                                                                                                                                                                                                                                                                                                                                                                              | Mechanismen . . . . .                                                                 | 123 |
| A.2.5                                                                                                                                                                                                                                                                                                                                                                                              | Beurteilungskriterien . . . . .                                                       | 124 |
| A.2.6                                                                                                                                                                                                                                                                                                                                                                                              | Sicherheitsparameter . . . . .                                                        | 126 |
| Anhang ZA (informativ) Zusammenhang zwischen dieser Europäischen Norm und der<br>Delegierten Verordnung (EU) 2022/30 zur Ergänzung der Verordnung 2014/53/EU des<br>Europäischen Parlaments und des Rates im Hinblick auf die Anwendung der<br>grundlegenden Anforderungen, wie in Artikel 3(3), Punkt (d), Punkt (e) und Punkt (f)<br>dieser abzudeckenden Verordnung in Bezug genommen . . . . . |                                                                                       | 127 |
| Literaturhinweise . . . . .                                                                                                                                                                                                                                                                                                                                                                        |                                                                                       | 128 |

## Bilder

|          |                                                       |     |
|----------|-------------------------------------------------------|-----|
| Bild 1   | — Entscheidungsbaum für Anforderung ACM-2 . . . . .   | 19  |
| Bild 2   | — Entscheidungsbaum für Anforderung AUM-1-1 . . . . . | 23  |
| Bild 3   | — Entscheidungsbaum für Anforderung AUM-1-2 . . . . . | 26  |
| Bild 4   | — Entscheidungsbaum für Anforderung AUM-2 . . . . .   | 29  |
| Bild 5   | — Entscheidungsbaum für Anforderung AUM-3 . . . . .   | 32  |
| Bild 6   | — Entscheidungsbaum für Anforderung AUM-4 . . . . .   | 35  |
| Bild 7   | — Entscheidungsbaum für Anforderung AUM-5 . . . . .   | 39  |
| Bild 8   | — Entscheidungsbaum für Anforderung AUM-6 . . . . .   | 43  |
| Bild 9   | — Entscheidungsbaum für Anforderung SUM-1 . . . . .   | 47  |
| Bild 10  | — Entscheidungsbaum für Anforderung SUM-2 . . . . .   | 50  |
| Bild 11  | — Entscheidungsbaum für Anforderung SUM-3 . . . . .   | 54  |
| Bild 12  | — Entscheidungsbaum für Anforderung SSM-1 . . . . .   | 57  |
| Bild 13  | — Entscheidungsbaum für Anforderung SSM-2 . . . . .   | 60  |
| Bild 14  | — Entscheidungsbaum für Anforderung SSM-3 . . . . .   | 63  |
| Bild 15  | — Entscheidungsbaum für Anforderung SCM-1 . . . . .   | 66  |
| Bild 16  | — Entscheidungsbaum für Anforderung SCM-2 . . . . .   | 70  |
| Bild 17  | — Entscheidungsbaum für Anforderung SCM-3 . . . . .   | 74  |
| Bild 18  | — Entscheidungsbaum für Anforderung SCM-4 . . . . .   | 77  |
| Bild 19  | — Entscheidungsbaum für Anforderung RLM-1 . . . . .   | 81  |
| Bild 20  | — Entscheidungsbaum für Anforderung NMM-1 . . . . .   | 85  |
| Bild 21  | — Entscheidungsbaum für Anforderung TCM-1 . . . . .   | 88  |
| Bild 22  | — Entscheidungsbaum für Anforderung CCK-4 . . . . .   | 99  |
| Bild 23  | — Entscheidungsbaum für Anforderung GEC-7 . . . . .   | 115 |
| Bild 24  | — Entscheidungsbaum für Anforderung CRY-1 . . . . .   | 120 |
| Bild A.1 | — Beispiel für einen Entscheidungsbaum . . . . .      | 124 |

## Tabellen

|             |             |     |
|-------------|-------------|-----|
| Tabelle 1   | — . . . . . | 11  |
| Tabelle A.1 | — . . . . . | 123 |

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

|                                                                                                                  |     |
|------------------------------------------------------------------------------------------------------------------|-----|
| Tabelle A.2 —                                                                                                    | 125 |
| Tabelle ZA.1 — Zusammenhang zwischen dieser Europäischen Norm und der<br>Richtlinie 2014/53/EU [Amtsblatt L 153] | 127 |

## 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

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

— 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

#### **Password**

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](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 *Gerätesoftware* 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<br>(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.<br><br>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.<br><br>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:

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

- 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
endif
@enduml
```

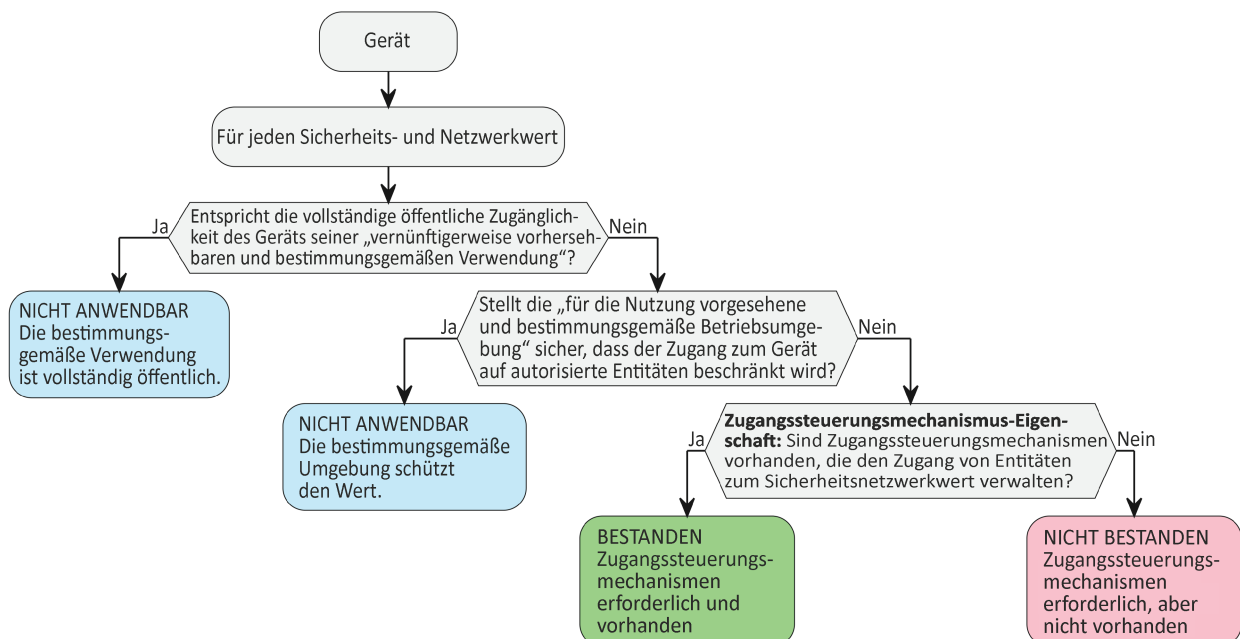


**Bild 1 — Entscheidungsbaum für Anforderung ACM-1**

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

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

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

- 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
```

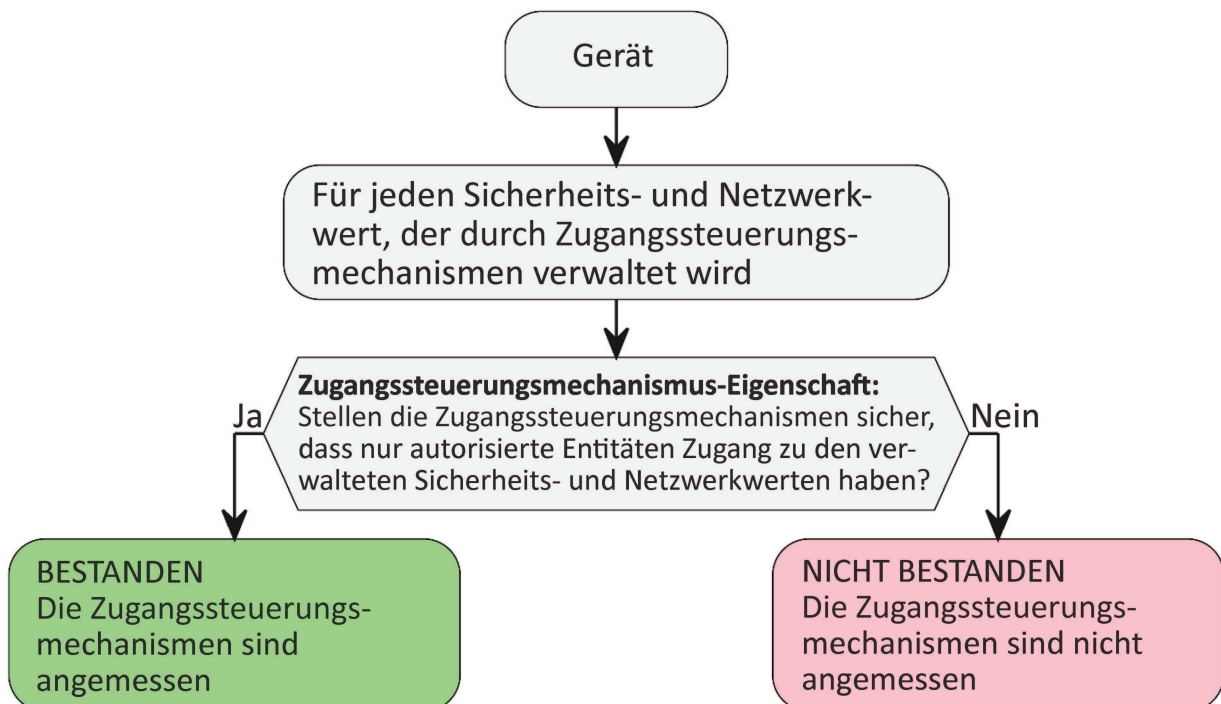


Bild 1 — Entscheidungsbaum für Anforderung ACM-2

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

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).

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

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.DTAUM-1-1] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 3 für jeden Sicherheits- und Netzwerkwert.

[E.Just.DTAUM-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 Netzwerkerts, 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 Netzwerkerten 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\nthe
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
    
```

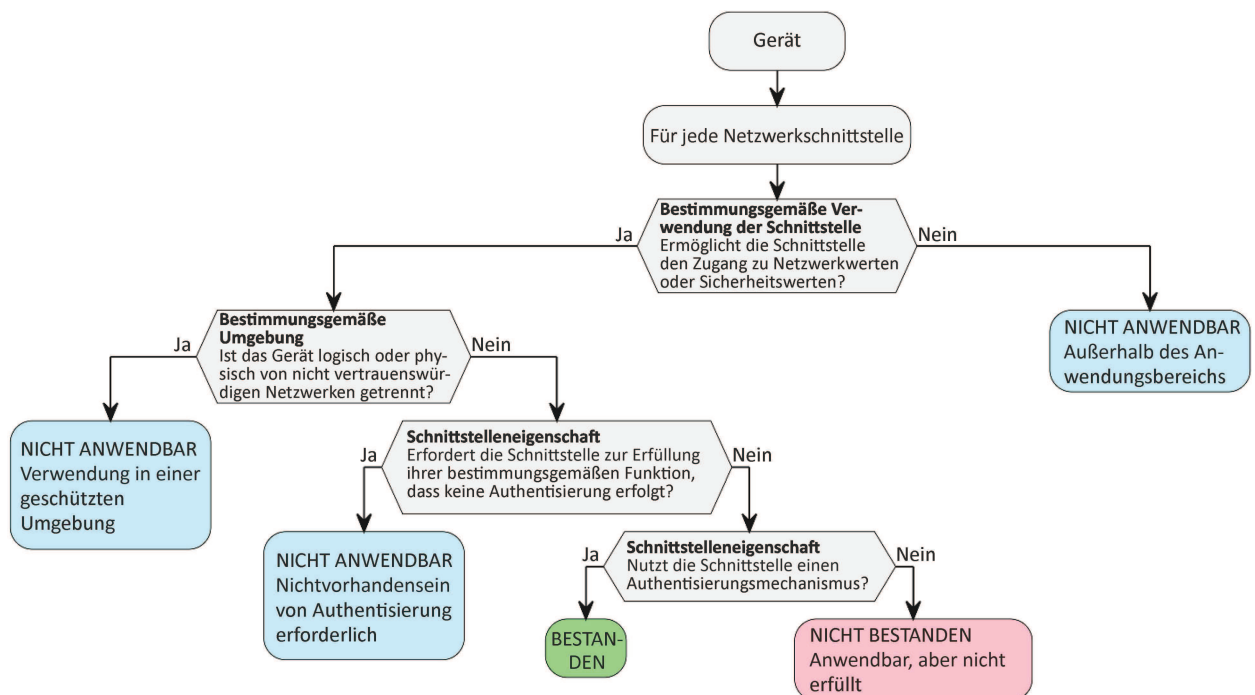


**Bild 2 — Entscheidungsbaum für Anforderung AUM-1-1**

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 Netzwerkerts, 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 Netzwerkerten 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
endif
else (No)
    #application :NOT APPLICABLE \nOut of scope;
    detach
endif
@enduml
```

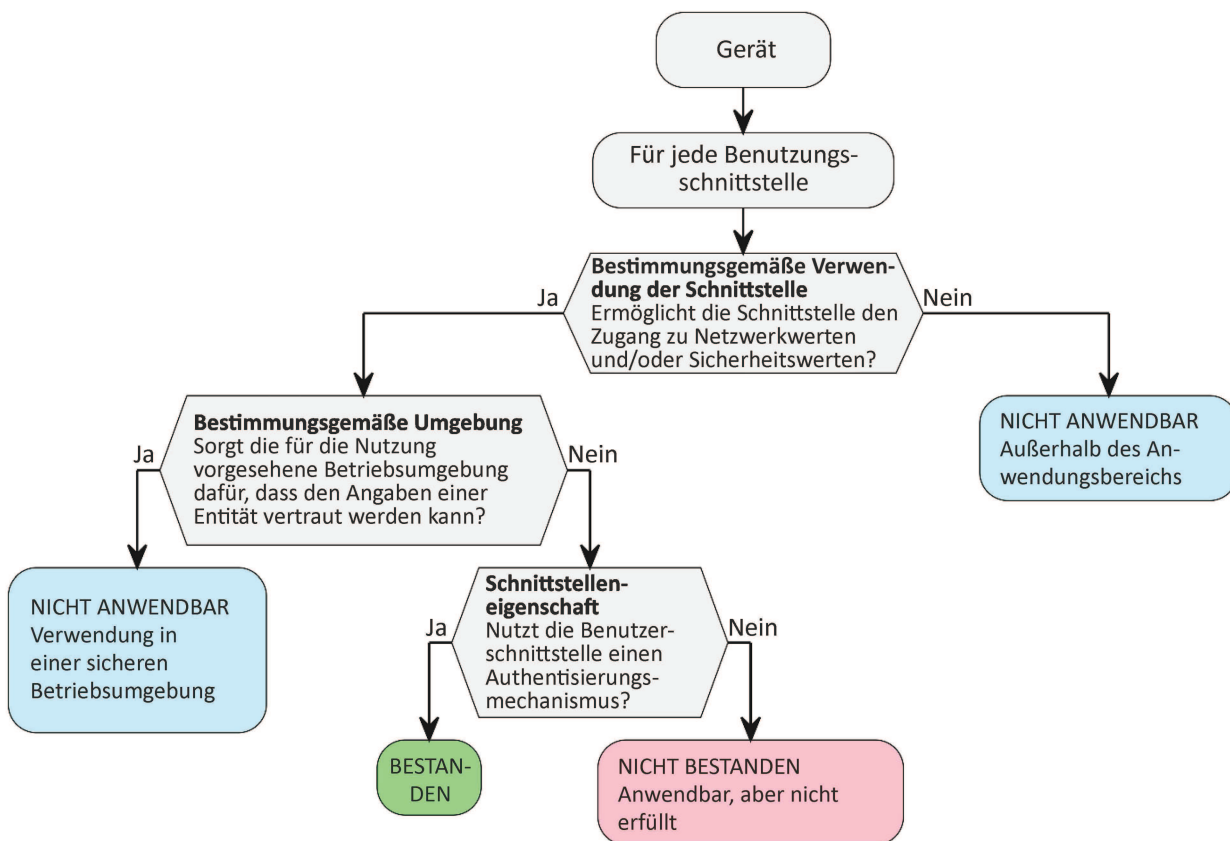


**Bild 3 — Entscheidungsbaum für Anforderung AUM-1-2**

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.DTAUM-2-1] dokumentierte Pfad durch den Entscheidungsbaum mit „NICHT ANWENDBAR“ oder „BESTANDEN“ endet.

Für jeden in [E.Doc.DTAUM-1-2] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Just.DTAUM-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!“.

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

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 Netzwerkerts, 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

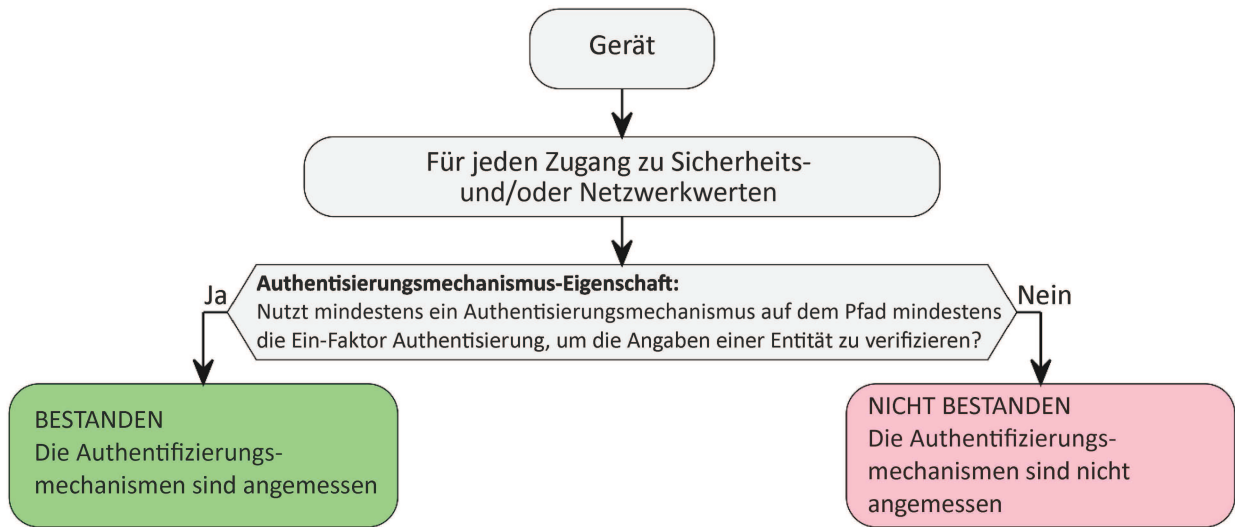


**Bild 4 — Entscheidungsbaum für Anforderung AUM-2**

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
```

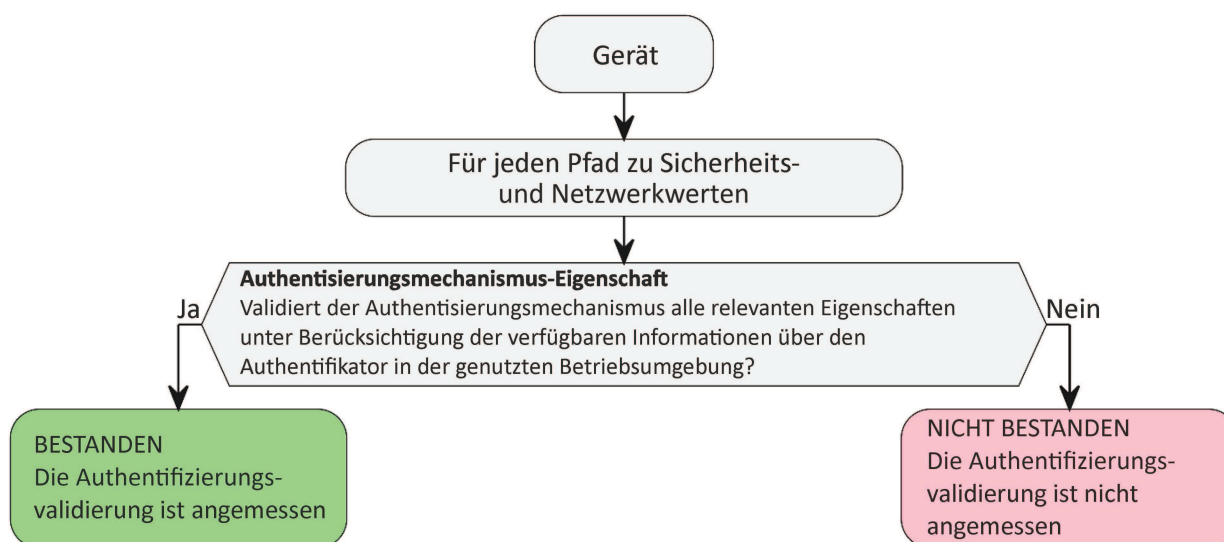


**Bild 5 — Entscheidungsbaum für Anforderung AUM-3**

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.DTAUM-4] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 7 für jede Authentifikator-Änderungsfunktionalität.

[E.Just.DTAUM-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
  authenticator \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
  endif
@enduml
```

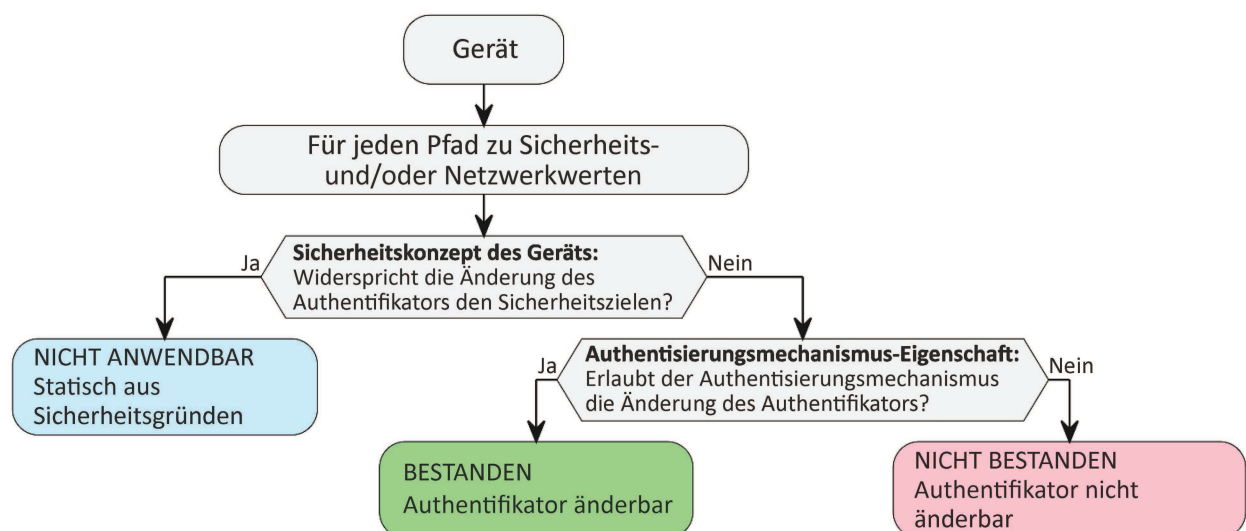


Bild 6 — Entscheidungsbaum für Anforderung AUM-4

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.

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

Für jeden in [E.Doc.DTAUM-4] dokumentierten Pfad durch den Entscheidungsbaum ist seine in [E.Doc.DTAUM-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.

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

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.DTAUM-5] Beschreibung des gewählten Pfads durch den Entscheidungsbaum in Bild 8 für jeden Authentisierungsmechanismus.

[E.Just.DTAUM-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 \nenvoironment;
                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
endif
detach;
else (No)
#application:NOT APPLICABLE\nNo passwords used;
detach;
endif
@enduml
    
```

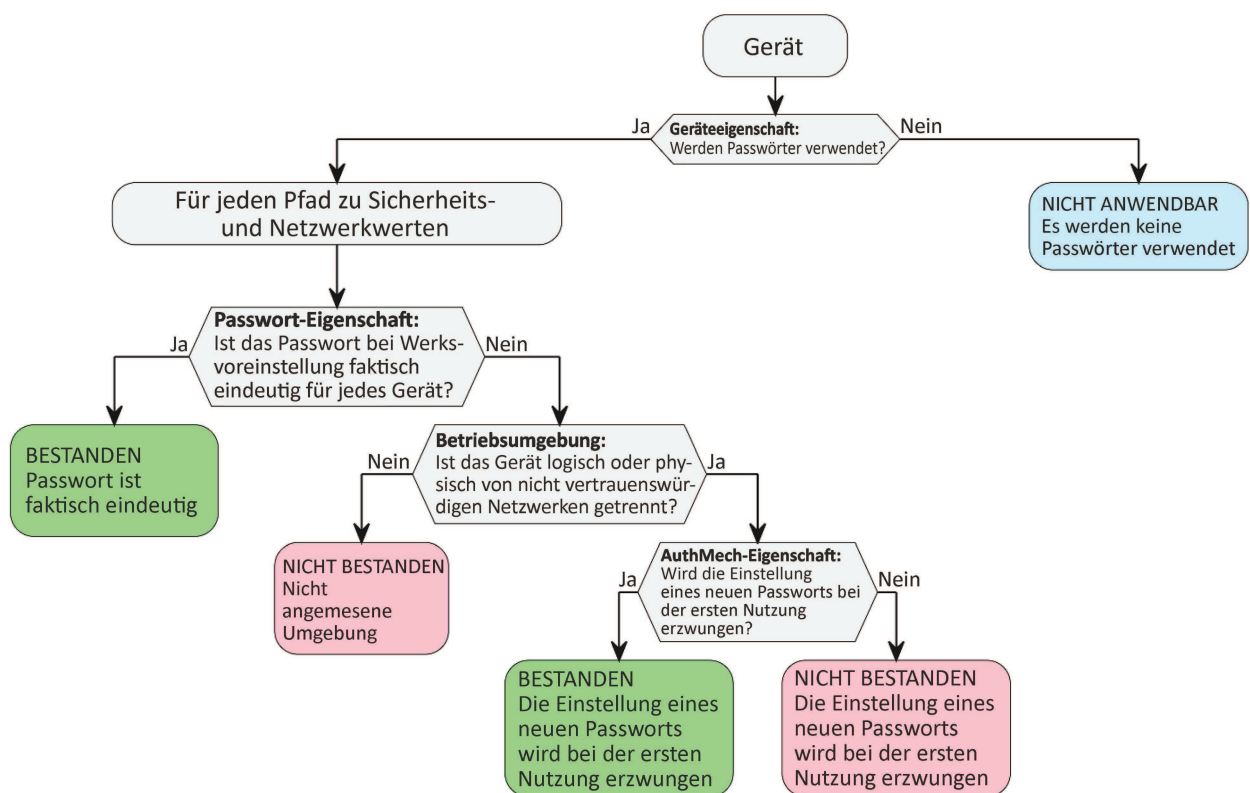


**Bild 7 — Entscheidungsbaum für Anforderung AUM-5**

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

[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
```

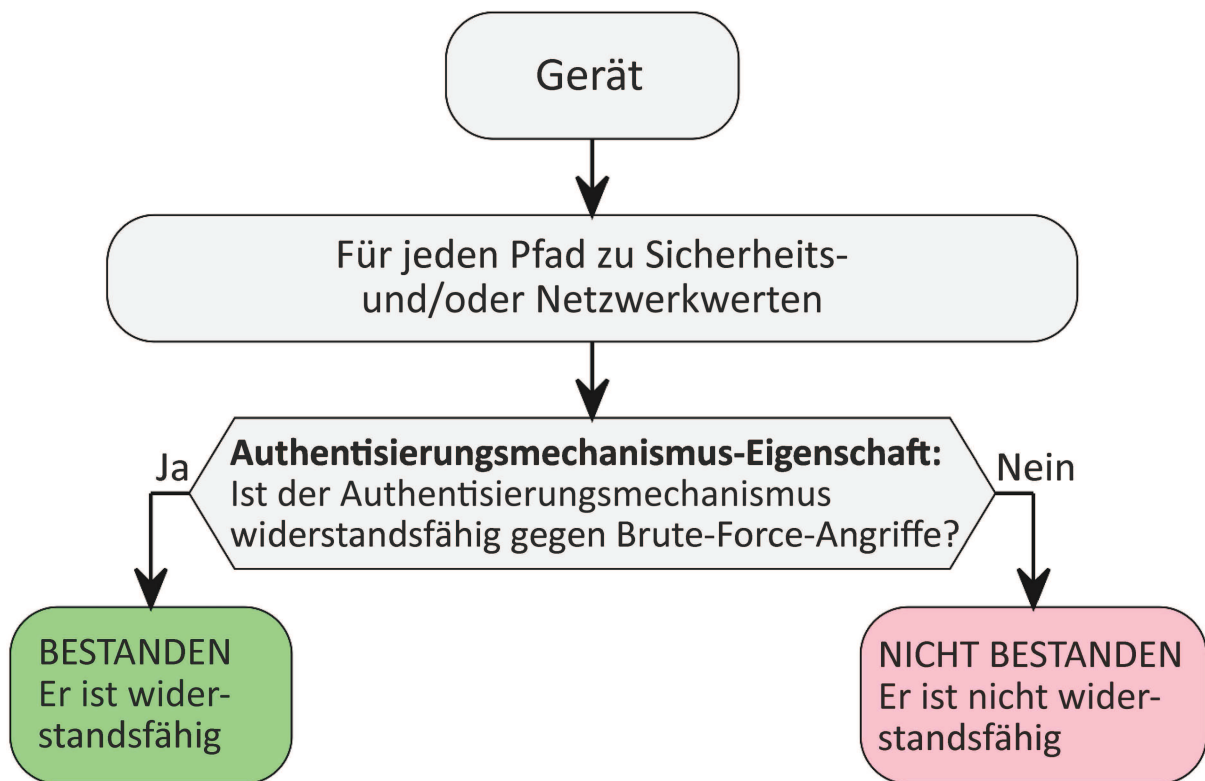


**Bild 8 — Entscheidungsbaum für Anforderung AUM-6**

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 Aktualisierungsmechanismus (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 Geräewartung 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\nnone 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
    
```

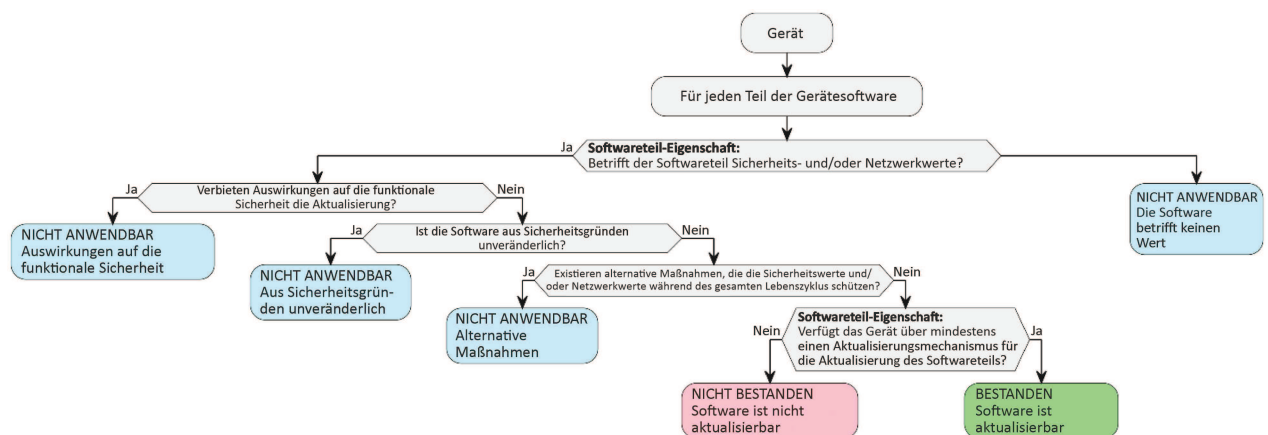


**Bild 9 — Entscheidungsbaum für Anforderung SUM-1**

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 vertrauenswürdigen 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.