

DIN EN 17927



ICS 35.030; 35.240.95

Einsprüche bis 2023-02-02

Entwurf

**Sicherheitsbewertungsstandard für IoT-Plattformen –
Eine effektive Methode zur Anwendung der Cybersicherheitsbewertung
und Wiederverwendung für vernetzte Produkte;
Deutsche und Englische Fassung prEN 17927:2022**

Security Evaluation Standard for IoT Platforms (SESIP) –

An effective methodology for applying cybersecurity assessment and re-use for connected products;

German and English version prEN 17927:2022

Norme d'évaluation de la sécurité pour les plateformes IoT –

Une méthodologie efficace pour appliquer l'évaluation de la cybersécurité et la réutilisation des produits connectés;

Version allemande et anglaise prEN 17927:2022

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2022-12-02 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

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

Gesamtumfang 219 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (prEN 17927:2022) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

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

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

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

IEC 62443-4-2	siehe	DIN EN IEC 62443-4-2
ISO 31000:2018	siehe	DIN ISO 31000:2018-10
ISO/IEC 15408-1:2009	siehe	DIN EN ISO/IEC 15408-1:2020-12
ISO/IEC 15408-2:2008	siehe	DIN EN ISO/IEC 15408-2:2020-12
ISO/IEC 15408-3:2008	siehe	DIN EN ISO/IEC 15408-3:2021-06
ISO/IEC 17000:2020	siehe	DIN EN ISO/IEC 17000:2020-09
ISO/IEC 17065:2012	siehe	DIN EN ISO/IEC 17065:2013-01
ISO/IEC 27017:2015	siehe	DIN EN ISO/IEC 27017:2021-11
ISO/IEC 30111:2019	siehe	DIN EN ISO/IEC 30111:2020-07

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

Nationaler Anhang NA (informativ)

Literaturhinweise

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

DIN EN ISO/IEC 15408-1:2020-12, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 1: Einführung und allgemeines Modell (ISO/IEC 15408-1:2009); Deutsche Fassung EN ISO/IEC 15408-1:2020*

DIN EN ISO/IEC 15408-2:2020-12, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 2: Sicherheitsfunktionskomponenten (ISO/IEC 15408-2:2008); Deutsche Fassung EN ISO/IEC 15408-2:2020, nur auf CD-ROM*

DIN EN ISO/IEC 15408-3:2021-06, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 3: Komponenten zur Sicherheitskontrolle (ISO/IEC 15408-3:2008, korrigierte Fassung 2011-06-01); Deutsche Fassung EN ISO/IEC 15408-3:2020, nur auf CD-ROM*

DIN EN ISO/IEC 17000:2020-09, *Konformitätsbewertung — Begriffe und allgemeine Grundlagen (ISO/IEC 17000:2020); Dreisprachige Fassung EN ISO/IE 17000:2020*

DIN EN ISO/IEC 17065:2013-01, *Konformitätsbewertung — Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren (ISO/IEC 17065:2012); Deutsche und Englische Fassung EN ISO/IEC 17065:2012*

DIN EN ISO/IEC 27017:2021-11, *Informationstechnik — Sicherheitsverfahren — Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste*

DIN EN ISO/IEC 30111:2020-07, *Informationstechnik — IT-Sicherheitsverfahren — Prozesse für die Behandlung von Schwachstellen (ISO/IEC 30111:2019); Deutsche Fassung EN ISO/IEC 30111:2020*

DIN ISO 31000:2018-10, *Risikomanagement — Leitlinien*

— Leerseite —

<i>Titel de:</i>	Sicherheitsbewertungsstandard für IoT-Plattformen – Eine effektive Methode zur Anwendung der Cybersicherheitsbewertung und Wiederverwendung für vernetzte Produkte
<i>Titel en:</i>	Security Evaluation Standard for IoT Platforms (SESIP) – An effective methodology for applying cybersecurity assessment and re-use for connected products
<i>Titel fr:</i>	Norme d'évaluation de la sécurité pour les plateformes IoT – Une méthodologie efficace pour appliquer l'évaluation de la cybersécurité et la réutilisation des produits connectés

Inhalt

	Seite
Europäisches Vorwort	6
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Überblick	9
4.1 Allgemeines	9
4.2 SESIP-Konzepte	10
4.3 IoT-Anwendungsfälle und Bedrohungsmodell.....	10
4.3.1 Allgemeines	10
4.3.2 Architektur.....	11
4.3.3 Vermögenswerte.....	11
4.3.4 Angreifer und Bedrohungen.....	12
4.4 Lebenszyklus eines vernetzten Produkts.....	13
4.5 Wiederverwendbarkeit beim SESIP	14
4.5.1 Allgemeines	14
4.5.2 Aufbau vernetzter Produkte aus vernetzten Plattformen.....	15
4.5.3 Additivzusammensetzung im Rahmen von SESIP.....	17
4.6 Zugänglichkeit und Transparenz.....	20
4.7 Selbstbewertung der Sicherheit in SESIP.....	21
4.8 Katalog der Sicherheitsfunktionen und Vertrauenswürdigkeitspakete.....	22
4.9 SESIP-Profile und -Zuordnungen	22
4.9.1 Allgemeines	22
4.9.2 SESIP-Profile.....	22
4.9.3 SESIP-Zuordnungen	23
5 Sicherheitsfunktionsanforderungen (SFR).....	23
5.1 Allgemeines	23
5.2 Identifizierung und Attestierung von Plattformen und Anwendungen	24
5.2.1 Verifizierung der Plattformidentität.....	24
5.2.2 Verifizierung der Identität der Plattforminstanz	25
5.2.3 Attestierung der Echtheit der Plattform	25
5.2.4 Sichere Initialisierung der Plattform	25
5.2.5 Attestierung des Zustands der Plattform	26
5.2.6 Attestierung der Echtheit der Anwendung	26
5.2.7 Attestierung des Zustands der Anwendung.....	26
5.3 Produktlebenszyklus: Zurücksetzen auf Werkseinstellungen/Installieren/Aktualisieren/Außerbetriebnahme.....	27
5.3.1 Allgemeines	27
5.3.2 Zurücksetzen der Plattform auf die Werkseinstellungen	27
5.3.3 Sichere Installation der Anwendung.....	28
5.3.4 Sichere Aktualisierung der Plattform	28
5.3.5 Sichere Aktualisierung der Anwendung	29
5.3.6 Sichere Deinstallation der Anwendung.....	29
5.3.7 Außerbetriebnahme der Plattform.....	30
5.3.8 Rückgabe der Plattform in der Praxis.....	30

5.4	Sichere Kommunikation	31
5.4.1	Allgemeines	31
5.4.2	Unterstützung für eine sichere Kommunikation	31
5.4.3	Durchsetzung einer sicheren Kommunikation	32
5.5	Zusätzliche Angreiferabwehr	32
5.5.1	Allgemeines	32
5.5.2	Begrenzte Abwehr von physischen Angreifern	33
5.5.3	Physische Angreiferabwehr	33
5.5.4	Software-Angriffsabwehr: Isolierung der Plattform	34
5.5.5	Software-Angriffsabwehr: Isolierung von Plattformteilen	34
5.5.6	Software-Angriffsabwehr: Isolierung von Anwendungsteilen	35
5.6	Kryptographische Funktionalität	35
5.6.1	Kryptographische Operation	35
5.6.2	Generierung kryptographischer Schlüssel	36
5.6.3	Kryptographischer Keystore (Schlüsselspeicher)	37
5.6.4	Kryptographische Generierung von Zufallszahlen	38
5.7	Konformitätsfunktionen	38
5.7.1	Allgemeines	38
5.7.2	Sichere vertrauenswürdige Speicherung	38
5.7.3	Sichere vertrauliche Speicherung	39
5.7.4	Sichere verschlüsselte Speicherung	39
5.7.5	Sichere Datenserialisierung	40
5.7.6	Bereinigung von Restinformationen	40
5.7.7	Erstellung und Speicherung von Auditprotokollen	41
5.7.8	Zuverlässiger Index	41
5.7.9	Sicheres Debugging	42
5.7.10	Sichere Wiederherstellung	42
5.7.11	Sicheres Backup und Wiederherstellung	43
5.7.12	Allgemeines Sicherheitsmerkmal der Plattform	43
5.8	Zugriffskontrolle	43
5.8.1	Privilegierte Zugriffskontrolle	43
5.8.2	Authentifizierte Zugriffskontrolle	44
5.9	Verfügbarkeit	44
5.9.1	Allgemeines	44
5.9.2	Eingeschränkte Anforderungen an die Umgebungsfähigkeit	44
5.9.3	Unterstützung der Verfügbarkeit	45
5.10	Mindestsatz an Sicherheitsfunktionsanforderungen	45
6	Sicherheitsprozesspakete (SPP)	46
6.1	Allgemeines	46
6.2	Sichere Entwicklung	46
6.2.1	Anforderung	46
6.2.2	Wert	46
6.2.3	Überlegungen	47
6.3	Vertrauenswürdige Bereitstellung	47
6.3.1	Anforderung	47
6.3.2	Wert	47
6.3.3	Überlegungen	47
7	Sicherheits-Vertrauenswürdigkeitsanforderungen (SAR)	47
7.1	Sicherheits-Vertrauenswürdigkeitsanforderungen bei SESIP	47
7.2	Anforderungen der Sicherheitsvorgaben	48
7.2.1	Allgemeines	48
7.2.2	ASE_INT.SESIP	48
7.2.3	ASE_OBJ.SESIP	48
7.2.4	ASE_REQ.SESIP	49

7.2.5	ASE_TSS.SESIP	51
7.3	Anforderungen an die Leitfäden	51
7.3.1	AGD_PRE.SESIP	51
7.3.2	AGD_OPE.SESIP	52
7.4	Entwicklungsanforderungen.....	53
7.4.1	ADV_ARC.SESIP	53
7.4.2	ADV_TDS.SESIP	53
7.4.3	ADV_FSP.SESIP	54
7.4.4	ADV_IMP.SESIP.....	54
7.5	Anforderungen an die Lebenszyklusunterstützung	55
7.5.1	ALC_CMC.SESIP.....	55
7.5.2	ALC_CMS.SESIP	56
7.5.3	ALC_DEL.SESIP.....	56
7.5.4	ALC_DVS.SESIP	57
7.5.5	ALC_FLR.SESIP	57
7.5.6	ALC_TAT.SESIP	58
7.6	Prüfanforderungen	58
7.6.1	ATE_COV.SESIP	58
7.6.2	ATE_DPT.SESIP.....	59
7.6.3	ATE_FUN.SESIP	59
7.6.4	ATE_IND.SESIP.....	60
7.7	Anforderungen an die Schwachstellenbewertung	61
7.7.1	Allgemeines	61
7.7.2	AVA_VAN.SESIP1.....	61
7.7.3	AVA_VAN.SESIP2.....	61
7.7.4	AVA_VAN.SESIP3.....	62
7.7.5	AVA_VAN.SESIP4.....	62
7.7.6	AVA_VAN.SESIP5.....	63
8	SESIP-Vertrauenswürdigkeitsstufen	64
8.1	Allgemeines	64
8.2	SESIP-Vertrauenswürdigkeitsstufe 1 (SESIP1).....	64
8.2.1	Allgemeines	64
8.2.2	Ziele	65
8.2.3	Vertrauenswürdigkeitskomponenten.....	65
8.3	SESIP-Vertrauenswürdigkeitsstufe 2 (SESIP2).....	65
8.3.1	Allgemeines	65
8.3.2	Ziele	66
8.3.3	Vertrauenswürdigkeitskomponenten.....	67
8.4	SESIP-Vertrauenswürdigkeitsstufe 3 (SESIP3).....	67
8.4.1	Allgemeines	67
8.4.2	Ziele	68
8.4.3	Vertrauenswürdigkeitskomponenten.....	69
8.5	SESIP-Vertrauenswürdigkeitsstufe 4 (SESIP4).....	69
8.5.1	Allgemeines	69
8.5.2	Ziele	69
8.5.3	Vertrauenswürdigkeitskomponenten.....	70
8.6	SESIP-Vertrauenswürdigkeitsstufe 5 (SESIP5).....	70
8.6.1	Allgemeines	70
8.6.2	Ziele	70
8.6.3	Vertrauenswürdigkeitskomponenten.....	71
Anhang A (informativ) Fallbeispiel für die SESIP-Evaluierung		72
Anhang B (informativ) Leitlinien — Bewertung des Angriffspotentials.....		73
B.1	Grundsätze	73
B.1.1	Allgemeines	73

B.1.2	Identifizierungs- und Ausnutzungsphasen	73
B.1.3	Physische (lokale) Angriffe und Fernangriffe	73
B.2	Bewertung des Angriffspotentials	73
Anhang C (informativ) Beispiele für Anwendungsfälle		76
C.1	Generische Beispiele	76
C.1.1	IoT-Cloud-Konnektivitätsplattform	76
C.1.2	Vertrauensgrundlage (RoT, en: Roots of Trust) bei einem Mikrocontroller	78
C.2	Beispiele für spezifische Anwendungsfälle	81
C.2.1	Allgemeines	81
C.2.2	Sichere Aktualisierung eines Produkts (OTA)	81
C.2.3	Ein Produkt zur Blutzuckermessung (DTSec)	82
Anhang D (informativ) Vorlage für Sicherheitsvorgaben		85
D.1	Allgemeines	85
D.2	Titelblatt der Sicherheitsvorgaben	85
D.3	Einleitung	85
D.3.1	Allgemeines	85
D.3.2	ST-Verweisung	85
D.3.3	Plattformverweisung	86
D.3.4	Enthaltene Leitfäden	86
D.3.5	(Optional) Sonstige Zertifizierung	86
D.3.6	Funktionsübersicht und Beschreibung der Plattform	86
D.4	Sicherheitszielsetzungen für die Betriebsumgebung	87
D.4.1	Plattformzielsetzungen für die Betriebsumgebung	87
D.4.2	(Optional) Übernommene Zielsetzungen für die Betriebsumgebung	88
D.5	Sicherheitsanforderungen und Implementierung	88
D.5.1	Sicherheits-Vertrauenswürdigkeitsanforderungen	88
D.5.2	Sicherheitsfunktionsanforderungen	89
D.5.3	(Optional) Sicherheitsprozesspaket	90
D.5.4	(Optional) Zusätzliche Anforderungen an funktionale Sicherheit/Prozesse	91
D.6	Abbildung und Angemessenheitsbegründungen	91
D.6.1	Allgemeines	91
D.6.2	Angemessenheit von SESIP1	92
D.6.3	Angemessenheit von SESIP2	93
D.6.4	Angemessenheit von SESIP3	94
D.6.5	Angemessenheit von SESIP4	96
D.6.6	Angemessenheit von SESIP5	99
Anhang E (normativ) Leitlinien für die Zusammensetzung		102
E.1	Einleitung	102
E.2	SESIP-Zusammensetzungsprozess	102
E.3	Aktivitäten zur Evaluierung der SESIP-Zusammensetzung	103
E.3.1	Allgemeines	103
E.3.2	Leitlinien für den Entwickler des zu integrierenden Plattformteils	104
E.3.3	Leitlinien für den Evaluator des zu integrierenden Plattformteils	104
E.3.4	Leitlinien für den Entwickler der Zusammensetzung	105
E.3.5	Leitlinien für den Evaluator der Zusammensetzung	107
Anhang F (informativ) SESIP im gesamten Prozess der Produktsicherung		110
F.1	Einleitung	110
F.2	Domäne der Risikoanalyse	110
F.3	Domäne der Angriffsmethoden	111
F.4	Sicherheitsbewertung	111
F.5	Mängelbeseitigung	112
Literaturhinweise		113

Europäisches Vorwort

Dieses Dokument (prEN 17927:2022) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Einleitung

Dieses Dokument legt den Sicherheitsbewertungsstandard für IoT-Plattformen (SESIP, en: Security Evaluation for Secure IoT Platforms) fest. Es umfasst allgemeine Anforderungen für Sicherheitsfunktionsanforderungen (SFR), Sicherheitsprozesspakete (SPP) und Sicherheits-Vertrauenswürdigkeitsanforderungen (SAR), die bei der Evaluierung und Zertifizierung von IoT-Plattformen verwendet werden sollen.

SESIP ist eine Methode für die Sicherheitsevaluierung von Plattformen, auf denen vernetzte Produkte eingesetzt werden. Der Begriff „Plattform“ in SESIP ist definiert als die Implementierung zugrunde liegender Funktionen für eine Anwendungsschicht; eine Plattform kann in „Plattformteile“ unterteilt werden.

SESIP befasst sich nicht mit dem endgültigen vernetzten Produkt selbst, sondern die Ergebnisse der SESIP-Evaluierung der vernetzten Plattform sollen als Nachweis für die Konformitätsbekundung von Normen für vernetzte Produkte verwendet werden können.

Damit ist SESIP nicht redundant zu den aktuellen IoT-Normen, sondern ein Tool, auf das sich diese Normen durch Wiederverwendung von Ergebnissen stützen können. Für einen Produkthanbieter ist es in der Tat unmöglich, mit vertretbarem Aufwand Bewertungsnachweise für alle Plattformteile zu erbringen, die von verschiedenen Entwicklern/Herstellern stammen.

Die spezifischen Ziele dieser SESIP-Methode werden im Folgenden zusammengefasst:

- Zugänglichkeit für alle interessierten Parteien an IoT-Produkten;
- Bereitstellung klarer, aber harmonisierter Sicherheitsansprüche;
- Berücksichtigung der Erfordernisse für die Markteinführung durch Bereitstellung einer optimierten und effizienten Methode;
- Ermöglichung der Wiederverwendung von Evaluierungsergebnissen in verschiedenen Produkten und/oder zwischen verschiedenen Normen und Vermeidung redundanter Evaluierungen derselben Plattform(-teile) ohne Mehrwert;
- Unterstützung beim Nachweis der Konformität von vernetzten Produkten mit den Normen für vernetzte Produkte.

Die Erfüllung dieser Ziele ermöglicht es SESIP, die Gesamtsicherheit in IoT-Ökosystemen zu erhöhen, indem die Anzahl der Sicherheitsevaluierungen durch Klarheit in den Sicherheitsansprüchen und optimierte Bemühungen gesteigert wird.

1 Anwendungsbereich

Dieses Dokument beschreibt eine Methode zur Evaluierung der Cybersicherheit namens SESIP für Plattformen und Plattformteile von vernetzten IoT-Produkten. Sicherheitsansprüche in SESIP werden auf der Grundlage der von diesen Plattformen angebotenen Sicherheitsdienste gestellt. Plattformteile können aus Hardware und Software bestehen. SESIP zielt darauf ab, die Vergleichbarkeit zwischen unabhängigen Sicherheitsbewertungen und deren Wiederverwendung zu unterstützen. SESIP bietet eine Reihe gemeinsamer Anforderungen für die Sicherheitsfunktionalität von Plattformteilen, die auf die grundlegenden Plattformen von nicht anwendungsspezifischen Geräten Anwendung finden. Die Methode beschreibt die Wiederverwendung von Evaluierungsergebnissen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 17000:2020, *Conformity assessment — Vocabulary and general principles*

ISO/IEC 17065:2012, *Conformity assessment — Requirements for bodies certifying products, processes and services*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 17000:2020, ISO/IEC 17065:2012 und 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

zusammengesetzte Plattform

Plattform, die eine zertifizierte Plattform integriert (Teil)

3.2

vernetzte Anwendung Anwendung

übergreifende Softwareschicht, die einen IoT-Anwendungsfall für den Benutzer auf der zugrunde liegenden vernetzten Plattform implementiert

3.3

vernetzter Anwendungsteil Anwendungsteil

Teilmenge der vernetzten Anwendung, die durch einen bestimmten Kontext (z. B. Daten, Ressourcen usw.) definiert ist und vom Rest der Anwendung isoliert werden soll

3.4

vernetzte Plattform Plattform

Hardware und/oder Software, die sichere Dienste für eine vernetzte Anwendung bereitstellt

3.5

Entwickler für vernetzte Plattformen

Plattformentwickler

Entwickler, die Plattformen (Teile) bauen und diese an Produkthanbieter oder andere Plattformentwickler liefern, und die die Sicherheit der von ihnen gebauten Plattformen (Teile) zertifizieren müssen

3.6

vernetztes Plattformteil

Plattformteil

Teil

Hardware und/oder Software, die eine Teilmenge der Funktionen einer vernetzten Plattform implementiert und die separat evaluiert werden kann, z. B. die Hardware, eine kryptographische Bibliothek, ein Betriebssystem

3.7

vernetztes Produkt

Produkt

Kombination aus einer vernetzten Plattform und einer vernetzten Anwendung, die ein Produkthanbieter auf den Markt bringt

3.8

Schlüsselspeicher

Repository, in dem Zertifikate, private Schlüssel oder Geheimnisse gespeichert werden können

3.9

SESIP-Profil

generisches Sicherheitsprofil für einen Plattfortmtyyp (Teil), Vorlage für SESIP-Sicherheitsvorgaben einer Plattform des durch das Profil anvisierten Typs

3.10

SESIP-Sicherheitsvorgabe

SESIP-ST

ST, en: security target

Erklärung der SESIP-Sicherheitsanforderungen in Form von Sicherheitsfunktionen (SFR und SPP) und Evaluierungsaufgaben (SAR), die während der Evaluierung einer Plattform (eines Teils) zu berücksichtigen sind

4 Überblick

4.1 Allgemeines

Dieser Abschnitt bietet einen Überblick über die wesentlichen Grundsätze des SESIP:

- Grundkonzepte der Methode;
- ein an das IoT-Ökosystem angepasstes Bedrohungsmodell;
- ein an die vernetzten Produkte im IoT-Ökosystem angepasster Lebenszyklus;
- Wiederverwendbarkeit, ein wesentliches Ziel von SESIP, um die zunehmende Komplexität der vernetzten Plattformen, die im IoT-Ökosystem evaluiert werden müssen, zu vertretbaren Kosten zu bewältigen;

- Zugänglichkeit, die erforderlich ist, um Produkthanbieter zu ermutigen, die in evaluierten vernetzten Plattformen enthaltenen Sicherheitsmerkmale zu nutzen; die Ergebnisse einer Evaluierung sollen für sicherheitsbewusste Entwickler zugänglich und nutzbar sein, ohne dass sie Evaluierungsspezialisten sein müssen;
- Selbstbewertung der Sicherheit in SESIP.

4.2 SESIP-Konzepte

SESIP ist aus der Normenreihe ISO 15408 ([4] [5] [6]) hervorgegangen, die auf die Evaluierung von vernetzten Plattformen im Kontext des IoT spezialisiert ist und die folgenden Basiskonzepte enthält:

- SESIP übernimmt die wichtigsten Definitionen und allgemeinen Konzepte, die in ISO 15408-1 [4] eingeführt wurden.
- SESIP-Sicherheitsfunktionsanforderungen (SFR) für die von Plattformen (Teilen) zu implementierenden und zu evaluierenden Sicherheitsmerkmalen; SESIP verwendet nicht den in ISO 15408-2 [5] definierten SFR-Katalog, sondern behält das Konzept eines SFR-Katalogs bei, der auf das IoT-Ökosystem spezialisiert ist, wobei jedoch jede SFR auf der Ebene des endgültigen Dienstes für den Benutzer liegt.
- SESIP-Sicherheitsprozesspakete (SPP) für die Sicherheitsprozesse, die vom Entwickler der zu evaluierenden Plattform zu implementieren sind.
- SESIP-Sicherheits-Vertrauenswürdigkeitsanforderungen (SAR) für die durchzuführenden Evaluierungsaufgaben; SESIP behält die Kategorisierung der Sicherheits-Vertrauenswürdigkeitsanforderungen und die zugehörige Art der Entwicklereingaben wie in ISO 15408-3 [6] bei, definiert jedoch den Inhalt wie in 7.1 beschrieben neu.
- SESIP-Vertrauenswürdigkeitsstufen; SESIP verwendet nicht die in ISO 15408-3 [6] definierten „EAL“-Pakete, sondern definiert seine eigenen, an das IoT-Ökosystem angepassten Vertrauenswürdigkeitspakete: die SESIP-Stufen (siehe Abschnitt 8).

Einzelheiten zur SESIP-Implementierung dieser Konzepte sind in den Abschnitten 5 bis 8 enthalten.

SESIP ist eine Evaluierungsmethode, die so genau wie möglich definiert, wie die Sicherheit eines Produkts, in diesem Fall einer vernetzten Plattform, zu evaluieren ist. Ebenso legt die SESIP kein spezifisches Verfahren fest und regelt auch nicht ausdrücklich die Grundsätze der gegenseitigen Anerkennung von Zertifikaten, sondern gibt lediglich Hinweise und Anleitungen. Ein SESIP-Evaluierungs-/Zertifizierungsprogramm, das auf dieser SESIP-Evaluierungsmethode basiert, wird voraussichtlich in einem anderen Dokument vom Eigentümer des Zertifizierungsprogramms definiert werden.

4.3 IoT-Anwendungsfälle und Bedrohungsmodell

4.3.1 Allgemeines

IoT ist ein weit gefasster Begriff, der jedoch immer ein Produkt („Ding“) und eine Form der Konnektivität („Internet“) beinhaltet. SESIP konzentriert sich auf die „Ding“-Seite des IoT und auf die Sicherheit der vernetzten Plattformen, auf denen die vernetzten Produkte basieren.

4.3.2 Architektur

Eine vernetzte Plattform umfasst in der Regel die folgenden Komponenten:

- Hardware (Prozessor, Speicher, möglicherweise ein sicheres Element, mindestens eine Netzwerkschnittstelle, möglicherweise einige Sensoren) und zugehörige Funktionen, z. B. Firmware, Bootloader und Vertrauensgrundlage.
- Es wird davon ausgegangen, dass die vernetzte Plattform über mindestens eine Netzwerkschnittstelle verfügt, die direkt oder indirekt mit einem Netzwerk verbunden und für potentielle Angreifer zugänglich ist.
- Ein Betriebssystem, das die Grundlage für die Ausführung von vernetzten Anwendungen auf der Hardware bildet.
- Eine Netzverbindungsschicht (z. B. Comm-Bibliothek), die die Verbindung des Produkts mit dem Backend oder anderen Produkten ermöglicht.
- Software-Anwendungsdienste für vernetzte Anwendungen, die Produkthanbietern einen Anwendungsrahmen zur Verfügung stellen (z. B. Krypto-Bibliothek, sichere Speicherung, Identitäts- und Attestierungsfunktionen).

In Bild 4-1 ist ein Beispiel für eine vernetzte Plattform dargestellt:

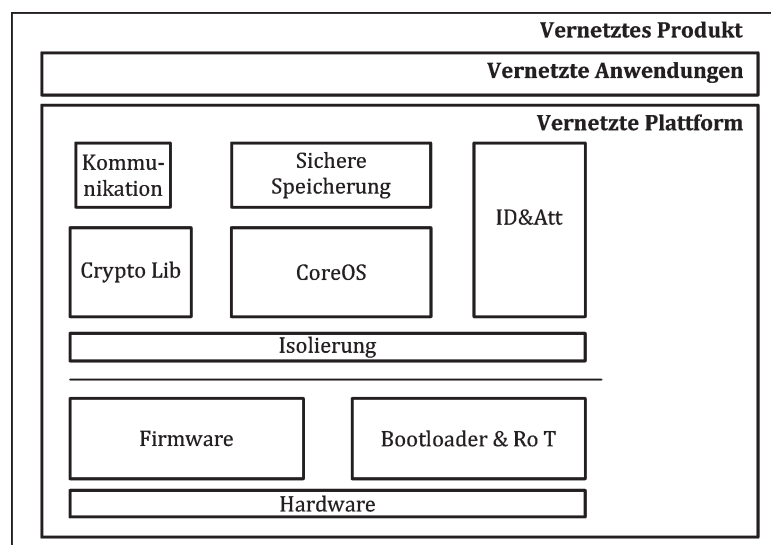


Bild 4-1 — Beispiel für eine vernetzte Produktarchitektur

4.3.3 Vermögenswerte

Die Vermögenswerte der Plattform hängen von der Plattformimplementierung und dem Anwendungsfall ab. Die in Tabelle 4-1 aufgeführte Liste typischer Hauptvermögenswerte wurde jedoch von einer Gruppe interessierter Parteien des IoT erstellt:

Tabelle 4-1 — Hauptvermögenswerte einer vernetzten Plattform

Vermögenswert	Schutzmaßnahmen
Benutzerdaten (lokal)	Datenschutzbelange sind von wesentlicher Bedeutung. Der Schutz der Vertraulichkeit, Integrität und Authentizität muss bereitgestellt sein.
Benutzerangaben (Authentisierungsdaten)	Geheimnisse sind vertraulich zu behandeln. Sekundärdaten (wie Zähler) müssen angemessen geschützt werden (Vertraulichkeit, Integrität).
Daten bei der Übertragung (Internet)	Vertraulichkeit und Integrität sind oft unerlässlich, ebenso wie die Authentizität.
Daten bei der Übertragung (lokal)	Integrität ist oft unerlässlich. Vertraulichkeit ist keine systematische Anforderung. Authentizität ist seltener.
Code, einschließlich Plattformcode und Anwendungscode	Integrität und Authentizität sind starke Anforderungen. Vertraulichkeit ist optional.
Produktidentität	Integrität und Einzigartigkeit sind erforderlich.
Konfiguration und Systemdaten	Integrität und Authentizität sind erforderlich.
Lebenszyklusbezogene Daten	Integrität ist erforderlich.

Es wird davon ausgegangen, dass nicht alle Plattformen eine vollständige Abdeckung bieten, aber solche Einschränkungen müssen bei der Beanspruchung von SESIP-SFR sorgfältig begründet werden (z. B. begrenzte Bandbreite oder Altprotokoll).

Die Vermögenswerte dürfen weiter in verschiedene Kritikalitätsstufen eingeteilt werden, die auf der entsprechenden Ebene in der Plattform (Teil) geschützt werden – im Falle einer Mehrfach-Vertrauenswürdigkeitsplattform, siehe 4.5.2. So kann es beispielsweise verschiedene Stufen von kryptographischen Schlüsseln geben, je nach ihrer Funktion und ihrem Lebenszyklus. In diesem Fall:

- Die Schutzmechanismen müssen auf jeder Stufe angemessen sein.
- Die Vermögenswerte müssen nutzbar sein, ohne dass sie einer niedrigeren Stufe offengelegt werden.
- Die Nutzung der Vermögenswerte von einer niedrigeren Stufe aus muss in geeigneter Weise kontrolliert werden (Zugangskontrolle).

4.3.4 Angreifer und Bedrohungen

4.3.4.1 Basisszenario

Das Mindest- und Pflichtbedrohungsmodell in SESIP ist ein Angreifer, der während der Ausnutzungsphase nur Fernzugriff (keinen physischen) auf die vernetzte Plattform hat (siehe Anhang B). Damit wird das Hauptproblem des IoT angegangen, nämlich ein skalierbarer Angriff, der über eine Fernverbindung zur vernetzten Plattform ausgeführt wird.

Dennoch kann der Angreifer jede Art von vorläufigem Angriff auf eine vernetzte Plattform (Teil), die er besitzt, durchführen, einschließlich physischer Angriffe; dies muss für das Basisszenario in einer Identifizierungsphase berücksichtigt werden (siehe Anhang B).

Außerdem werden in diesem Basisszenario Bedrohungen im Zusammenhang mit nicht vertrauenswürdiger Software, die auf vernetzte Plattformen geladen werden könnte, nicht berücksichtigt.

4.3.4.2 Erweitertes Szenario – physischer Zugang

Wenn vernetzte Plattformen für Angreifer physisch zugänglich sind, kann das Bedrohungsmodell erweitert und durch die Verwendung der SFR „Begrenzter physischer Widerstand des Angreifers“ und „Physischer Widerstand des Angreifers“ abgedeckt werden. Beispiele für typische Szenarien, in denen Angreifer physischen Zugang zu einem Opferprodukt haben, sind:

- Vernetzte Plattform, die außerhalb einer physisch geschützten Umgebung eingesetzt wird, z. B. eine Türklingel oder eine IP-Kamera im Freien.
- Vorübergehender physischer Zugang; z. B. „Evil-Maid“-Angriffe, bei denen der Angreifer vorübergehend physischen Zugang zu dem Produkt hat, das bereits von einem Benutzer erworben wurde, oder „Lieferketten“-Angriffe, bei denen der Angreifer ein kompromittiertes Produkt an das Ziel liefert.

4.3.4.3 Erweitertes Szenario – nicht vertrauenswürdige Software

Wenn nicht vertrauenswürdige Software auf vernetzte Plattformen geladen werden kann, entweder durch den Benutzer oder durch ein externes Unternehmen, und dies Auswirkungen auf die Plattform, ihre Teile oder ihre Anwendungen haben könnte, kann das Basisbedrohungsmodell erweitert und durch die Verwendung der SFR „Software-Angriffsabwehr: Isolierung der Plattform“, „Software-Angriffsabwehr: Isolierung von Plattformteilen“ und „Software-Angriffsabwehr: Isolierung von Anwendungsteilen“ abgedeckt werden.

4.4 Lebenszyklus eines vernetzten Produkts

Für vernetzte Produkte und die vernetzten Plattformen, aus denen jedes Produkt besteht, können verschiedene Lebenszyklusmodelle angewendet werden. Dennoch lassen sich bei den meisten Produkten einige Muster finden, die für die Sicherheit von Bedeutung sind:

Die Anbieterbereitstellung ist die Phase, in der das Produkt mit Zugangsdaten ausgestattet wird, die mit dem Backend des Anbieters geteilt werden und die es dem Produkt ermöglichen, sicher mit dem Backend zu kommunizieren und Verwaltungsvorgänge durchzuführen. Diese Phase endet in der Regel mit der Auslieferung des Produkts an den Kunden.

Die Benutzerbereitstellung ist die Phase, in der das Produkt mit den Zugangsdaten eines Benutzers und spezifischen Daten ausgestattet wird, die es dem Produkt ermöglichen, diesen Benutzer zu vertreten. Diese Phase endet in der Regel mit der normalen Gebrauchsphase des Produkts.

Der normale Gebrauch ist der normale Zustand des Produkts, bis eines der folgenden Ereignisse eintritt:

- Der Benutzer setzt das Produkt auf die Werkseinstellungen zurück, wodurch alle benutzerbezogenen Daten und Zugangsdaten gelöscht werden und das Produkt für die Übergabe an eine andere Stelle vorbereitet wird (z. B. zum Weiterverkauf, zur Rückgabe oder sogar zur vorübergehenden Aufbewahrung). Das Produkt ist dann wieder für die Benutzerbereitstellung verfügbar, aber ein Benutzer sollte nicht die Möglichkeit haben, das Produkt in eine frühere Lebenszyklusphase zurückzubringen.
- Der Benutzer nimmt das Produkt außer Betrieb, bevor er es entsorgt. Dieser beendete Zustand ist unumkehrbar.

Einige Produkte können einen zusätzlichen Zustand in Bezug auf die Rückgabe in der Praxis enthalten, in dem spezielle Debugging-Funktionen verfügbar sind. Alle Benutzerdaten und Zugangsdaten müssen vor Erreichen dieses Zustands entfernt worden sein.

Der in Bild 4-2 dargestellte Produktlebenszyklus wird in den SFR als Verweisung verwendet, wenn Verweisungen auf einen Lebenszyklus erforderlich sind.

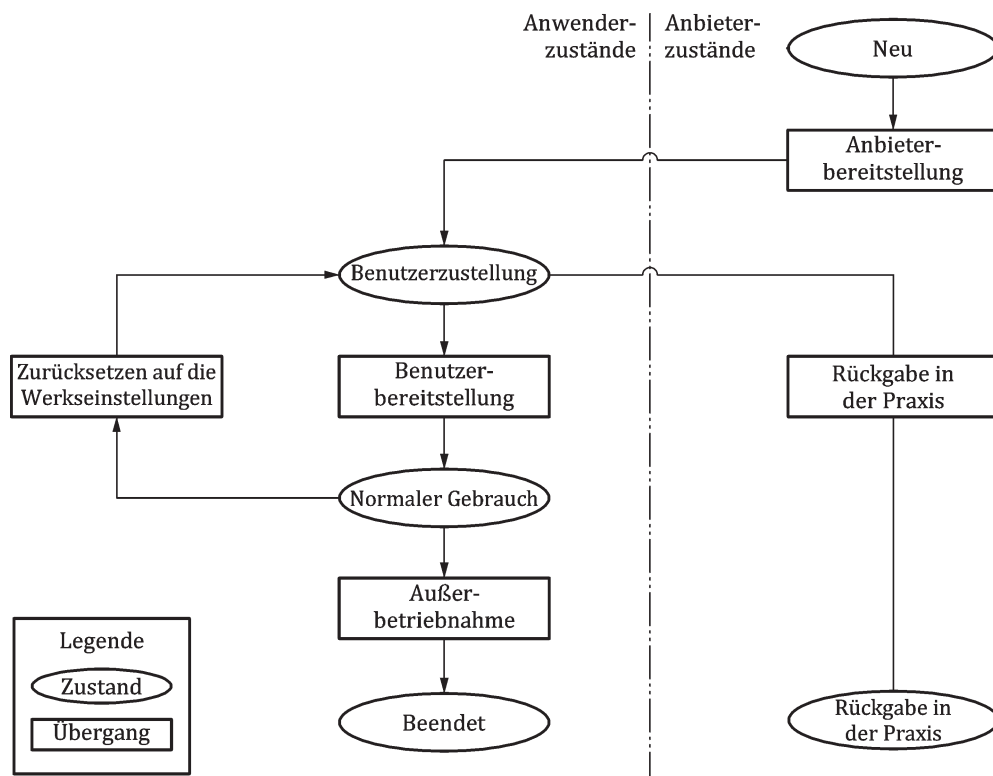


Bild 4-2 — Lebenszyklus des Referenzprodukts

Es ist zu beachten, dass die Zustände des Anbieters nur vom Anbieter erreicht werden können, entweder vor der Lieferung des Produkts oder nach der Rückgabe des Produkts durch den Benutzer.

Neben dem Produktlebenszyklus können auch die vernetzte Plattform und einige ihrer Teile unterschiedliche Lebenszyklen haben, die ebenfalls für die Sicherheit von Bedeutung sind. Solche Sicherheitslebenszyklen sind produktspezifisch, und ihr Beitrag zur Sicherheit der vernetzten Plattform (des Teils) sollte in den entsprechenden Sicherheitsvorgaben beschrieben werden.

4.5 Wiederverwendbarkeit beim SESIP

4.5.1 Allgemeines

Vernetzte Produkte sind komplex, oft viel komplexer als die meisten Produkte, deren Sicherheit bis heute offiziell zertifiziert wurde. SESIP trägt diesem Umstand Rechnung, indem es eine spezielle Methode für die vernetzten Plattformen bereitstellt, auf denen diese Produkte basieren. Vernetzte Plattformen werden häufig durch die Zusammenstellung mehrerer bereits vorhandener Hardware- und Softwarekomponenten gebaut; einige von ihnen enthalten Sicherheitskomponenten, die kritische Vermögenswerte schützen und auf einer hohen Vertrauenswürdigkeitsstufe evaluiert werden müssen. Solche Komponenten sind oft in mehrere miteinander vernetzte Plattformen integriert, die auf unterschiedliche Anwendungsfälle abzielen.

Die SESIP-Methode definiert Wege zur unabhängigen Evaluierung von Teilmengen von Komponenten, die dann als Plattformteile bezeichnet werden können, und zur Wiederverwendung der Evaluierungsergebnisse in jeder vernetzten Plattform. Diese Ergebnisse können aus einer Evaluierung nach der SESIP-Methode, aber auch aus anderen kompatiblen externen Evaluierungen stammen.

4.5.2 Aufbau vernetzter Produkte aus vernetzten Plattformen

4.5.2.1 Wiederverwendung externer Evaluierungen

Wie in Abschnitt 4.3 erwähnt, konzentriert sich SESIP auf die „Dinge“ im IoT und insbesondere auf die Lösungen, auf denen diese vernetzten Dinge aufgebaut sind, die wir als „vernetzte Produkte“ bezeichnen. Jedes vernetzte Produkt gehört zu einer Kategorie oder einem vertikalen Bereich, und für die gängigsten Arten von vernetzten Produkten (z. B. IoT für Verbraucher, IoT für die Industrie, vernetzte Fahrzeuge usw.) werden wahrscheinlich spezielle Sicherheitsstandards entwickelt. Für jeden Typ ist eine spezifische Risikoanalyse erforderlich, um die entsprechenden Funktions- und Vertrauenswürdigkeitsanforderungen zu bestimmen, was dann zur Erstellung eines spezifischen Evaluierungsprogramms führen kann.

In einem solchen Kontext mit mehreren Systemen werden die Sicherheitsanforderungen der SESIP-Methode so definiert, dass eine Gleichwertigkeit mit den Anforderungen anderer Systeme hergestellt werden kann. Nach erfolgreicher Kompatibilitätsanalyse ermöglicht dies die Wiederverwendung von Evaluierungsergebnissen zwischen verschiedenen Systemen.

4.5.2.2 Evaluierungen der Wiederverwendung von Plattformteilen

4.5.2.2.1 Allgemeines

Eine typische vernetzte Plattform ist kein monolithisches Bauteil, da sie Hardware, einschließlich mindestens eines [Mikro-]Controllers oder [Mikro-]Prozessors, und Software, einschließlich mindestens eines Betriebssystems, umfasst. Eine vernetzte Plattform umfasst möglicherweise viele weitere Komponenten, z. B. für die Kommunikation oder die Sicherheit. Ein Anbieter baut seine vernetzte Plattform in der Regel durch die Auswahl von Hardware- und Softwarekomponenten auf, die in der Regel von verschiedenen Drittanbietern stammen, und fügt sie dann zusammen.

Jeder Anbieter in dieser Lieferkette muss eine Bewertung der Sicherheit vornehmen, bis hin zum Integrator, der dafür sorgt, dass die gesamte vernetzte Plattform sicher ist. Die Aufrechterhaltung der Sicherheit während des gesamten Montageprozesses kann recht komplex sein, es sei denn, alle Anbieter dieser Komponenten (Hardware und Software) verwenden eine gemeinsame Methode.

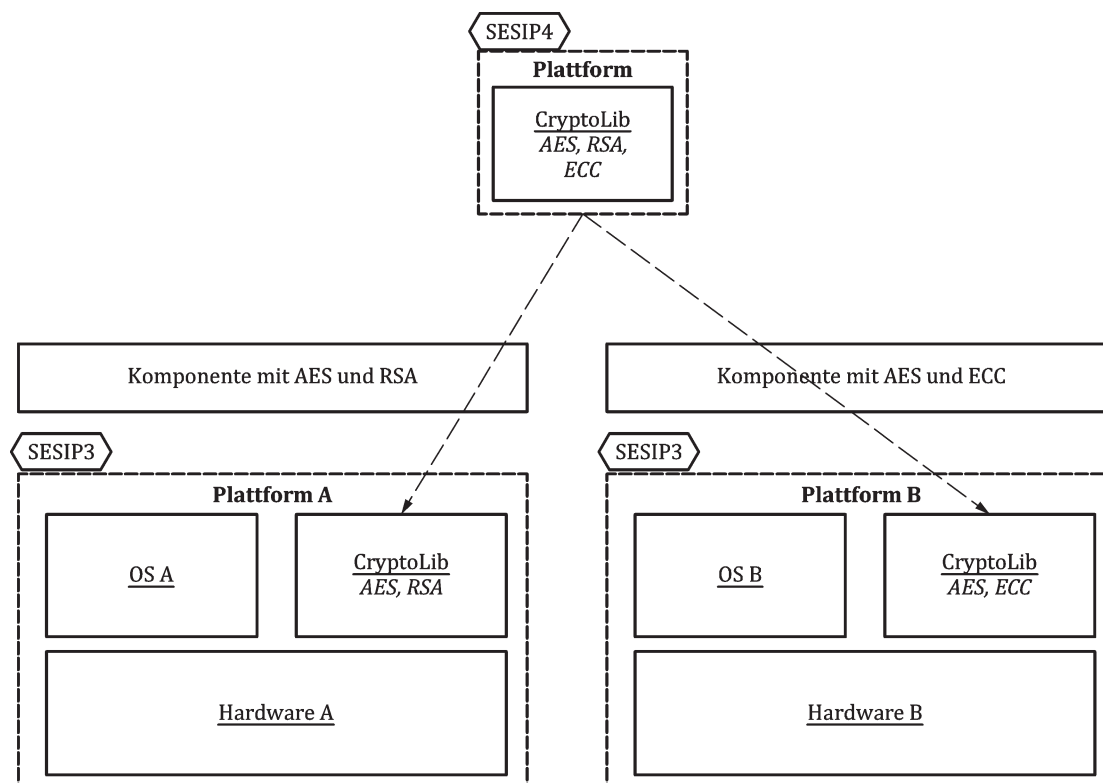
Um dies anzugehen, berücksichtigt SESIP die folgenden Wiederverwendungskontexte:

- Wiederverwendung von evaluierten Plattformteilen in mehreren Plattformen (Teilen);
- Wiederverwendung von evaluierten Plattformteilen von einer Hosting-Plattform (Teil) zu einer anderen.

4.5.2.2.2 Wiederverwendung von evaluierten Plattformteilen in mehreren Plattformen (Teilen)

SESIP ermöglicht die Evaluierung von Plattformteilen, einzeln oder in Kombination (siehe 4.5.3), so dass die Evaluierungsergebnisse dieser Plattformteile in verschiedenen vernetzten Produkten anwendbar bleiben.

Ein Beispiel ist in Bild A.4-3 dargestellt:



Legende

-  Vertrauenswürdigkeitsanspruch
-  Anwendungsbereich der Evaluierung
-  Wiederverwendet in

Bild 4-3 — Beispiel für die Wiederverwendung von Evaluierungsergebnissen auf mehreren Plattformen (Teilen)

4.5.2.2.3 Wiederverwendung von evaluierten Plattformteilen von einer Hosting-Plattform (Teil) zu einer anderen

Ein weiterer Fall von Wiederverwendung, der im Rahmen von SESIP zulässig ist: Wenn ein Teil innerhalb einer bestimmten Plattform (Teil) evaluiert wurde, können die entsprechenden Evaluierungsergebnisse für die Integration in eine andere Plattform (Teil) wiederverwendet werden.

Ein Beispiel ist in Bild A.4-4 dargestellt:

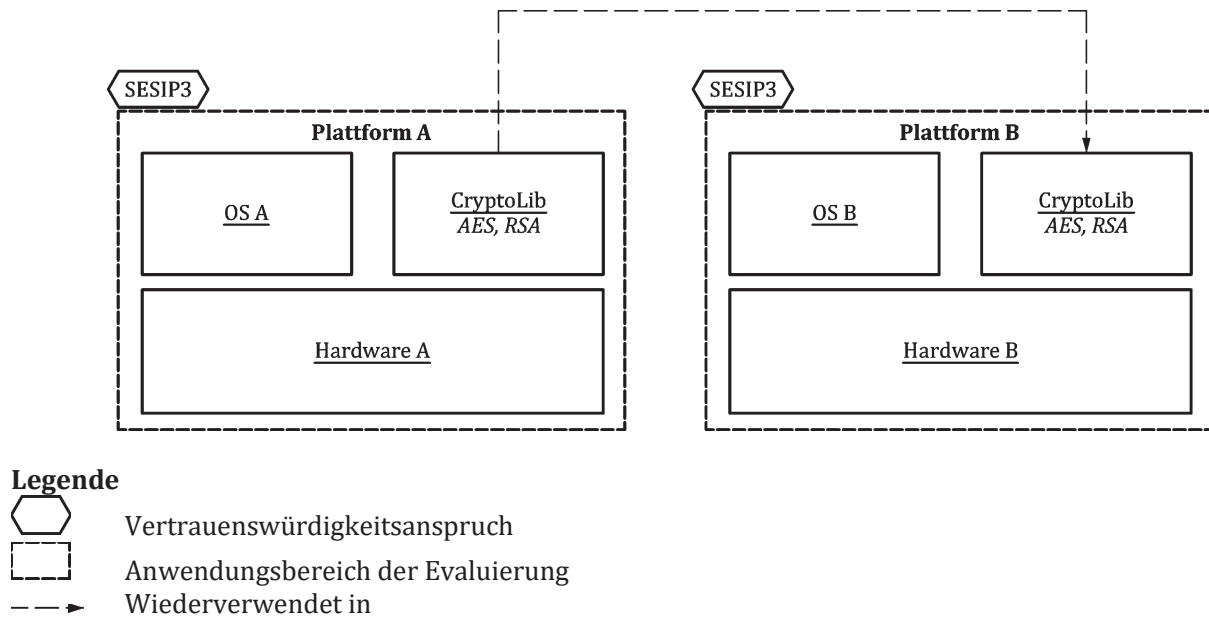


Bild 4-4 — Beispiel für die Wiederverwendung von Evaluierungsergebnissen von einer Plattform (Teil) zu einer anderen

In allen Fällen stützt sich die Wiederverwendung von Evaluierungsnachweisen insbesondere auf die Leitlinien für die Sicherheitsintegration der einzelnen Komponenten; die Bewertung der vernetzten Plattformen, in die evaluierte Plattformteile integriert sind, erfordert dann die Verifizierung, dass die Leitlinien für die sichere Integration und die Zusammensetzungsregeln (siehe 4.5.2) beachtet werden.

Es ist zu beachten, dass der Aufwand für die Wiederverwendung je nach Anwendungsfall variiert, von einfacher Portabilität mit wenigen Verifizierungen, z. B. vollständige Selbstkontrolle der Sicherheitsfunktionalität, bis hin zu einer Reihe spezieller Aufgaben, die im integrierenden Bereich durchgeführt werden müssen und die in den zuvor erwähnten Integrations- und Zusammensetzungsleitlinien zu definieren sind. In jedem Fall ist der Aufwand deutlich geringer als bei einer erneuten Evaluierung von evaluierten Teilen in einer neuen Plattform (Teil).

Die Verwendung von SESIP als Kernmethode ermöglicht es den Anbietern, ein klares Verständnis der Annahmen und Anleitungen der von ihnen integrierten Komponenten von Drittanbietern zu erhalten, indem sie die von den Anbietern der Komponenten während der Evaluierung ihrer Plattform (eines Teils) bereitgestellten Nachweise wiederverwenden.

4.5.2.3 Wiederverwendung der Plattformevaluierung in vernetzten Produkten

Die meisten vernetzten Produkte werden von Anbietern entwickelt, die eine oder mehrere spezielle Anwendung(en) auf einer generischen oder standardmäßigen vernetzten Plattform aufbauen. SESIP konzentriert sich auf die vernetzte Plattform, um eine Grundlage für die Sicherheitsbewertung und möglicherweise die Zertifizierung von vernetzten Produkten zu schaffen. Er befasst sich mit der Sicherheitsstufe des gesamten Betriebssystems einschließlich der Dienste, die für die Speicherung, Installation, Initialisierung und Ausführung dieser Anwendung verwendet werden, sowie mit dem Datenschutz.

4.5.3 Additivzusammensetzung im Rahmen von SESIP

4.5.3.1 Allgemeines

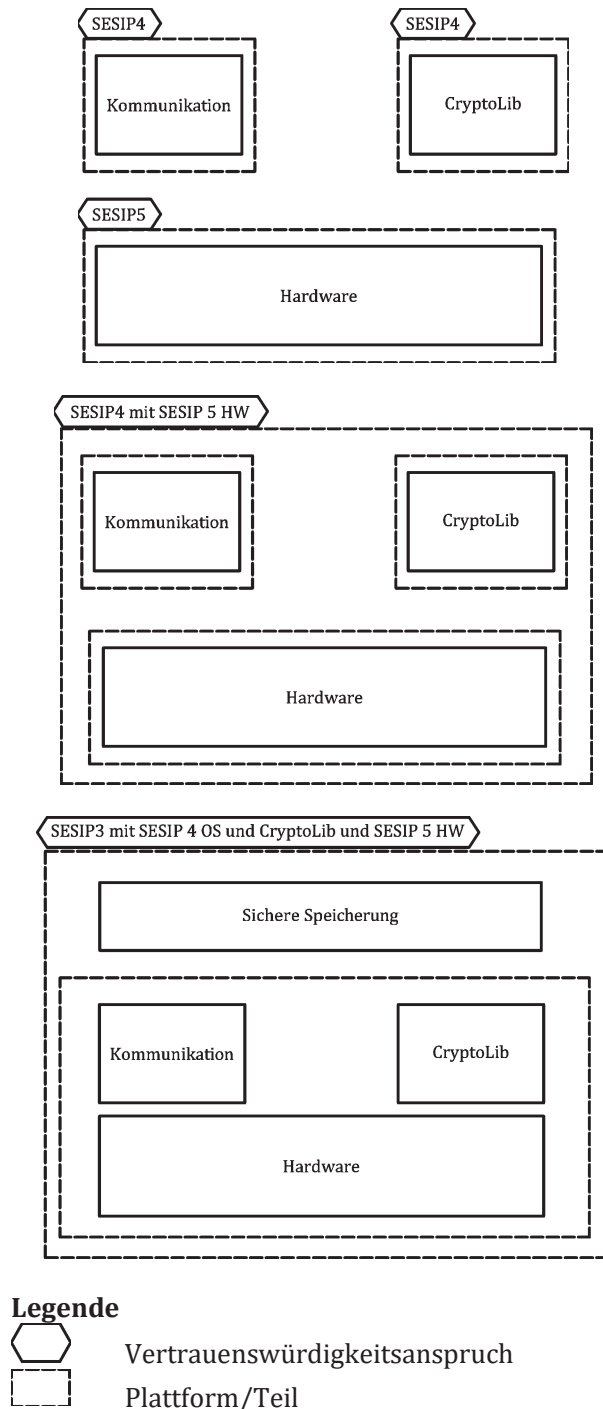
Das Ziel der Additivzusammensetzung ist die vereinfachte Evaluierung einer vernetzten Plattform durch die Wiederverwendung früherer Evaluierungsergebnisse von Plattformen (Teilen).

SESIP ermöglicht verschiedene Zusammenstellungsszenarien:

- Kombination von zuvor evaluierten Plattformteilen
- Kombination von zu evaluierendem(n) Plattformteil(en) mit bereits evaluiertem(n) Plattformteil(en)
- Kombination einer zu evaluierenden Plattform mit bereits evaluierten Plattformteilen

Die Additivzusammensetzung ermöglicht die sukzessive Zusammensetzung von Plattformteilen zu größeren Teilen, die ihrerseits evaluiert und in größere Plattformteile integriert werden können, wie in Bild 4-5 veranschaulicht. Jede Zusammensetzung profitiert von der Wiederverwendung der Evaluierungsergebnisse des zuvor integrierten Plattformteils. Solche Integrationen und die damit verbundene Evaluierung der Zusammensetzung können durchgeführt werden, bis eine vollständige IoT-Plattform erreicht ist, die bereit ist, Teil eines IoT-Geräts zu sein. Das endgültige IoT-Gerät kann sich auf die nacheinander evaluierten Plattformteile stützen und jedes Evaluierungsergebnis wiederverwenden. Alle Akteure der Lieferkette profitieren von der Additivzusammensetzung: von der Evaluierung eines Hardwareblocks über die Evaluierung von Zwischenmodulen bis hin zu einem evaluierten Gerät.

Ein Beispiel für ein Zusammensetzungsszenario ist in Bild 4-5 dargestellt:



Einzelne Evaluierungen

Jede Reihe von Komponenten, die in eine vernetzte Plattform integriert werden sollen, kann individuell evaluiert werden

Zusammensetzung 1

Jede zuvor einzeln evaluierte Vorgabe kann Teil einer Zusammensetzung werden

Zusammensetzung 2

Die Zusammensetzung 1 kann dann mit einer noch nicht evaluierten Oberschicht kombiniert werden. Sie wird Teil dieser neuen Zusammensetzung

Bild 4-5 — Beispiel für Zusammensetzungsszenarien

4.5.3.2 Regeln für die Evaluierung der Zusammensetzung

Die Evaluierung eines Plattformteils, der in eine größere Plattform (Teil) integriert werden soll, muss Zusammensetzungsleitlinien hervorbringen, die Regeln auflisten, die von jedem anderen Plattformteil, der mit ihm interagiert, eingehalten werden müssen. Dies muss als Ziel für die Umwelt beschrieben und in den Leitlinien nach den Anforderungen von SESIP-ASE und AGD ausdrücklich erwähnt werden (siehe Einzelheiten unter 7.2).

Bei der Evaluierung einer Zusammensetzung von Plattformteilen muss bewertet werden, ob die Leitlinien (einschließlich der Ziele für die Umgebung, der Benutzerleitlinien, der Integrationsleitlinien usw.) für jeden Plattformteil eingehalten werden.

Bei der Evaluierung einer Zusammensetzung von Plattformteilen müssen die Auswirkungen der Zusammensetzung auf die korrekte Sicherheitsfunktion der Plattformteile bewertet werden.

Anhang E skizziert die Schritte eines Zusammensetzungsprozesses und enthält detaillierte Leitlinien für jeden Akteur.

4.5.3.3 Vertrauenswürdigkeitsstufe von Zusammensetzungen

Es kann zu einer Zusammensetzung zwischen Plattformteilen kommen, die auf unterschiedlichen Vertrauenswürdigkeitsstufen evaluiert werden. Standardmäßig kann die Zusammensetzung höchstens die niedrigste Vertrauenswürdigkeitsstufe der Plattformteile beanspruchen, aus denen sie zusammengesetzt ist. So kann beispielsweise eine vernetzte Plattform, die sich aus einem SESIP2-Plattformteil und einem SESIP5-Plattformteil zusammensetzt, nicht auf einer höheren Gesamtstufe als SESIP2 zertifiziert werden, ohne dass zusätzliche Nachweise über den SESIP2-Teil oder über seine Verwendung durch den SESIP5-Plattformteil erbracht werden.

In einem solchen Fall dürfen die Sicherheitsvorgaben jedoch eine Teilmenge der SFR ausweisen, die eine höhere Vertrauenswürdigkeit erfordern. In diesem Fall können die Sicherheitsvorgaben die Vertrauenswürdigkeitsstufe des Teils mit hoher Vertrauenswürdigkeit beanspruchen, vorausgesetzt, dass die vom höheren Teil abgedeckten SFR für den Leser klar erkennbar sind. Anhand des Beispiels aus dem vorigen Absatz könnte die vernetzte Plattform beanspruchen, SESIP2 zu sein, wobei ein SESIP5-Teil nur die SFR des SESIP5-Teils abdeckt. Die Vertrauenswürdigkeitsstufe für eine solche Evaluierung muss als „SESIP2 mit SESIP5-Teil(en)“ bezeichnet werden.

Darüber hinaus könnte die SESIP-Stufe eines einzelnen Plattformteils auch erhöht werden, wenn er mit einem anderen Plattformteil zusammengesetzt wird, der Sicherheitsmerkmale mit einer höheren Vertrauenswürdigkeitsstufe bietet; dies muss durch Nachweise auf der Zusammensetzungsstufe belegt werden.

Es wird erwartet, dass solche Evaluierungen mit Mehrfach-Vertrauenswürdigkeit die Anforderungen der Industrie an die Zusammensetzung erfüllen. So können beispielsweise Branchenanforderungen vorschreiben, dass kritische Vermögenswerte wie bestimmte kryptographische Schlüssel oder Zugangsdaten durch ein manipulationssicheres Produkt wie ein sicheres Element besonders geschützt werden müssen, während andere, weniger kritische Vermögenswerte ein geringeres Maß an Schutz erfordern. In diesem Fall muss die vernetzte Plattform, wie oben beschrieben, eine Teilmenge nach einer höheren Vertrauenswürdigkeitsstufe evaluieren lassen.

4.6 Zugänglichkeit und Transparenz

Die IoT-Sicherheit bleibt eine Herausforderung. Eine SESIP-Evaluierung wird IoT-Anbietern helfen, vernetzte Plattformen auszuwählen, die eine angemessene Sicherheitsstufe bieten, aber SESIP zielt auch darauf ab, sicherzustellen, dass diese Anbieter in der Lage sind, die von den evaluierten Plattformen (Teilen) bereitgestellten Sicherheitsmerkmale in ihren Produkten angemessen zu nutzen. Dies wird hauptsächlich durch die Sicherheitsvorgaben erreicht, die zu einem Dokument werden sollen, das von in Sicherheitsfragen versierten Entwicklern, die jedoch keine Evaluierungsspezialisten sind, genutzt werden kann. Dies kann erreicht werden, indem sichergestellt wird, dass die Sicherheitsvorgaben transparent und lesbar sind, dass die Sicherheitsentscheidungen eindeutig und begründet sind und dass SESIP eine gewisse Konsistenz zwischen den Sicherheitsvorgaben sicherstellen kann.

Zu diesem Zweck müssen die SESIP-Sicherheitsvorgaben mehrere wesentliche Merkmale erfüllen:

- Die Sicherheitsziele sind die Konkretisierung der Risikoanalyse und informieren den Leser über die vom Produkt abzudeckenden Sicherheitsfunktionen. Sie müssen vom Verfasser der Sicherheitsvorgaben so

beschrieben werden, dass Entwickler diese Funktionen nutzen können und dass die Wiederverwendung von SESIP-Nachweisen erleichtert wird.

- Die SESIP-Sicherheitsfunktionsanforderungen (SFR), die die Sicherheitszielsetzungen in Implementierungsanforderungen ausdrücken, sind auf vernetzte Plattformen zugeschnitten. Bei SESIP deckt jede SFR für sich genommen einen vollständigen Sicherheitszweck ab. Dadurch können die Benutzer der Sicherheitsvorgaben ein intuitives Verständnis der Sicherheitsanforderungen entwickeln. Es ist zu beachten, dass die Flexibilität bei der Konstruktion von Anforderungen geringer ist, als wenn die Zwecke durch mehrere SFR erfüllt werden; in einem spezifischen Kontext, in dem die Bedürfnisse vorhersehbar sind, wie z. B. bei einer vernetzten Plattform, hat sich eine solche Flexibilität jedoch als nicht vorteilhaft erwiesen. SESIP definiert eine Reihe solcher SFR vor, die in Abschnitt 5 näher erläutert werden.
- Die vom Plattformevaluator verfasste Spezifikationszusammenfassung muss ausreichend detailliert sein, um nachzuweisen, dass die SFR von der spezifischen Implementierung erfüllt werden.
- In der vom Entwickler der Plattform(-teile) verfassten zusammenfassenden Beschreibung des Prozesses zur Mängelbeseitigung muss insbesondere erläutert werden, wie die Aufdeckung einer Schwachstelle und die anschließende Analyse zur Entwicklung und Verteilung einer Plattformaktualisierung oder zu anderen Abhilfemaßnahmen führen kann.
- Es muss eine Verweisung auf die Benutzerführung enthalten sein, zusammen mit einer Beschreibung, wie ein potentieller Benutzer auf diese Dokumentation zugreifen kann.

Es ist zu beachten, dass Zugänglichkeit nicht notwendigerweise eine zu starke Vereinfachung bedeutet; insbesondere ist die Semantik der SESIP-SFR genau definiert, so dass es keine Unklarheiten über die Bedeutung der SFR gibt, selbst wenn sie in einfacher Sprache ausgedrückt sind.

Die SESIP-Sicherheitsvorgaben und die Dokumentation, auf die sie verweisen, sind als zugängliche Dokumentation gedacht, zumindest für potentielle Benutzer der Plattform (des Teils); dies kann in einzelnen Systemen präzisiert werden, abhängig von der Sicherheitsempfindlichkeit der evaluierten Plattformen (Teile).

4.7 Selbstbewertung der Sicherheit in SESIP

Eine Selbstbewertung der Sicherheit ist mit SESIP möglich, aber da Selbstbewertung in der Branche viele verschiedene Bedeutungen hat, ist es wichtig, sie hier zu definieren.

Die Selbstbewertung der Sicherheit durch den Entwickler beruht auf dem Nachweis, dass alle Sicherheitsanforderungen in Form einer in den SESIP-Sicherheitsvorgaben enthaltenen Begründung ordnungsgemäß abgedeckt sind.

Eine solche Begründung muss für Folgendes vorgesehen werden:

- jede beanspruchte Sicherheitsfunktionsanforderung, mit einer Beschreibung, wie diese Anforderung durch die Implementierung abgedeckt wird;
- im Falle einer Zusammensetzung jede Sicherheitszielsetzung für die von einem Plattformteil definierte Umgebung, um nachzuweisen, wie diese Zielsetzung erfüllt wird und/oder sie erneut als Sicherheitszielsetzung für die Plattformumgebung zu definieren;
- die Beanspruchung der Mängelbeseitigung, mit einer Beschreibung eines konformen Prozesses;
- jedes Dokument, das für die beanspruchte Sicherheits-Vertrauenswürdigkeitsstufe erforderlich ist, mit einer Erläuterung, wie auf diese Dokumentation zugegriffen werden kann;
- öffentlich bekannte Schwachstellen der Plattform (Teil), mit Bereitstellung einer Schwachstellenprüfung.

Jede Begründung basiert auf einer Selbstbewertung des Entwicklers, die von einem externen Plattform-Evaluator validiert werden muss. Der Umfang der vom Plattform-Evaluator durchgeführten Arbeiten hängt von der gewählten Vertrauenswürdigkeitsstufe ab.

4.8 Katalog der Sicherheitsfunktionen und Vertrauenswürdigkeitspakete

SESIP umfasst Kataloge mit Sicherheitsfunktionen als einen wesentlichen Teil der Methode:

- Den Katalog der Sicherheitsfunktionsanforderungen (SFR), der eine konsistente Definition von Plattformen (Teilen) ermöglicht und einen fairen Vergleich zwischen ihnen unterstützt.
- Den Katalog der Sicherheitsprozesspakete (SPP), der es dem Plattformentwickler ermöglicht, in jeder Phase des Lebenszyklus der Plattform spezifische sichere Prozesse zu beanspruchen und deren Anwendung zu verifizieren.

Diese Kataloge definieren eine Reihe von Sicherheitsfunktionen, die für Plattformen (Teile) wesentlich sind und für die es in der Gemeinschaft ein geteiltes Verständnis gibt. Diese Sicherheitsfunktionen sind daher eher für Produkthanbieter zugänglich; sie vereinfachen auch die Wiederverwendbarkeit und tragen zum Formalismus von SESIP bei (siehe vorherige Unterabschnitte).

Diese Sicherheitsfunktionen werden sich im Laufe der Zeit weiterentwickeln, und zwar entsprechend der Entwicklung der IoT-Sicherheits Herausforderungen, des vermehrten Gebrauchs der SESIP-Methode und den von den vernetzten Plattformen bereitgestellten Sicherheitsreaktionen. Plattform-(Teil-)Anbieter möchten ihre Angebotspalette möglicherweise auch durch plattformspezifische oder innovative Sicherheitsfunktionen, die ihren Kunden einen Mehrwert bieten, differenzieren, und es ist möglich, solche Funktionen nach der SESIP-Methode evaluieren zu lassen.

Es wird jedoch auch erwartet, dass die Methode die nötige Stabilität bietet, um ein kohärentes Zertifizierungsökosystem aufzubauen und zu erhalten. Wenn also eine Funktion mit keiner der im SESIP-Katalog definierten SFR/SPP übereinstimmt, kann einem Anbieter im Rahmen des Systems gestattet werden, produktspezifische SFR/SPP hinzuzufügen, solange sie ausdrücklich als solche gekennzeichnet und klar von den bereits im Katalog vorhandenen SFR/SPP getrennt sind.

Was die Sicherheits-Vertrauenswürdigkeitsanforderungen (SAR) betrifft, so dürfen die Anbieter bei einer SESIP-Evaluierung keine zusätzlichen Anforderungen geltend machen. Ein spezielles Zertifizierungsprogramm darf jedoch eine begrenzte Präzisierung der SAR in den SESIP-Stufen beinhalten.

4.9 SESIP-Profil und -Zuordnungen

4.9.1 Allgemeines

SESIP-Profil und SESIP-Zuordnungen sind Dokumente, die die Verwendbarkeit der SESIP-Methode in der Praxis unterstützen sollen.

4.9.2 SESIP-Profil

Die SESIP-Methode ermöglicht die Definition von Sicherheitsprofilen, die für einen Plattfortmty (Teil) generisch sind, z. B. MCU/MPU, kryptographische Bibliothek, Kommunikationsbibliothek usw. Diese werden als SESIP-Profil bezeichnet: Ein SESIP-Profil dokument ist eine generische SESIP-Sicherheitsvorgabe, die die SESIP-Anforderungen in Bezug auf Sicherheitsfunktionen (siehe Abschnitt 5) und Evaluierungsaufgaben (siehe Abschnitt 7) definiert, die während der Evaluierung einer Plattform (eines Teils) des vom Profil angesprochenen Typs zu erfüllen sind.

Die SESIP-Profil sollen von Entitäten oder Gruppen erstellt werden, die Sicherheitsevaluierungen für einen bestimmten Markt benötigen und/oder eine Rolle bei solchen Evaluierungen spielen. Dadurch können sie sicherstellen, dass jede Plattform (Teile), die anhand eines SESIP-Profils evaluiert wird, einen erwarteten

Mindestsatz von Funktionen implementiert und eine vorgegebene Sicherheitsstufe erreicht; da außerdem derselbe Satz von Funktionen auf der Grundlage derselben Evaluierungsaufgaben bewertet wird, ermöglicht dies die Vergleichbarkeit von Evaluierungen verschiedener evaluierter Plattformen (Teile).

Dank der Zugänglichkeit der SESIP-Anforderungen (siehe 4.6) können auch interessierte Parteien ohne besondere Fachkenntnisse im Bereich der Evaluierung ein SESIP-Profil erstellen und verstehen.

Außerdem ist zu beachten, dass Profile die Berücksichtigung von Risiko- und Bedrohungsanalysen für bestimmte Produkttypen ermöglichen; solche Risikoanalysen wurden zuvor von den betreffenden Akteuren erstellt (z. B. durch spezielle Arbeitsgruppen der Industrie). Weitere Details sind Anhang F zu entnehmen.

4.9.3 SESIP-Zuordnungen

Wie in 4.5.1 beschrieben, soll SESIP mit bestehenden Normen arbeiten und ihnen einen Rahmen für die Evaluierung ihrer Anforderungen bieten. SESIP definiert nämlich Sicherheitsanforderungen (siehe Abschnitte 5 und 7), die von den Entwicklern bei Evaluierungen im Rahmen von SESIP geltend gemacht werden können. Diese Anforderungen wurden auf einer Stufe formuliert, die die Abdeckung der Hauptfunktionen von IoT-Plattformen ermöglicht. Daher können die Anforderungen bestehender Normen leicht den SESIP-Anforderungen zugeordnet werden.

Zusammen mit einer solchen Zuordnung können die Ergebnisse der SESIP-Evaluierung als Nachweis der Konformität mit einer IoT-Norm verwendet werden, um zu bestätigen, dass die Sicherheitsfunktionen der IoT-Norm korrekt und effizient umgesetzt wurden.

SESIP-Zuordnungen sollen von Entitäten oder Gruppen verfasst werden, die die Evaluierungsergebnisse von SESIP als Grundlage für den Nachweis der Konformität mit einer Norm verwenden möchten. Der Vorteil der SESIP-Evaluierung in diesem Zusammenhang ist die Wiederverwendung einer ersten SESIP-Evaluierung, um die Konformität mit mehreren Normen nachzuweisen, wobei jede Norm mit einer speziellen Zuordnung verbunden ist.

5 Sicherheitsfunktionsanforderungen (SFR)

5.1 Allgemeines

Vernetzte Plattformen müssen Entwicklern und Evaluatoren von IoT-Anwendungen Funktionalitäten für den Aufbau sicherer Produkte zur Verfügung stellen und eine effiziente Verifizierung der korrekten Nutzung dieser sicheren Plattformen durch Benutzer, Entwickler und Evaluatoren/Zertifizierer ermöglichen. Derartige Bedürfnisse werden durch Sicherheitsfunktionsanforderungen (SFR) ausgedrückt, bei denen es sich um generische Sicherheitsfunktionen handelt, die von vernetzten Plattformen implementiert werden müssen.

Dieser Abschnitt enthält einen Katalog von SFR, die von einer Gruppe von IoT-Akteuren auf der Grundlage ihres eigenen Fachwissens und einer kontinuierlichen Überwachung von Sicherheitsanforderungen an Plattformschichten aus der Praxis (z. B. durch IoT-Normen) definiert wurden und für die eine SESIP-Evaluierung wiederverwendbare Bewertungsergebnisse liefern kann.

Die Entwickler müssen diesen Katalog verwenden, um die SFR auszuwählen, die in den Sicherheitsvorgaben geltend zu machen sind, um die von ihrer Plattform (ihrem Teil) implementierten Sicherheitsmechanismen zu beschreiben und in den Anwendungsbereich der Sicherheitsevaluierung einzubeziehen. Der Text der SFR kann nicht geändert werden; sie können jedoch durch Präzisierungen¹ oder Anwendungshinweise präzisiert und/oder näher spezifiziert werden. Dies ist insbesondere im Falle des SESIP-Profiles (siehe 4.9) und/oder bei der Zuordnung zu den Anforderungen der IoT-Normen nützlich.

1 Die Regeln für die Präzisierung entsprechen denen in ISO/IEC 15408-1:2009, 8.1.4.

Dieser Katalog der SFR kann durch proprietäre SFR in den Sicherheitsvorgaben und SESIP-Profilen erweitert werden, wenn keine im Katalog enthaltenen SFR verwendet werden können, um eine bestimmte Sicherheitsfunktion als Teil der Evaluierung zu fordern.

Die SFR in diesem Katalog werden mit dem Wortlaut der Anforderung, dem „Wert“ und den „Überlegungen“ beschrieben.

- Der Wortlaut der Anforderung beschreibt, was implementiert werden muss; in einigen Anforderungen enthält der Text Felder in spitzen Klammern (< >), die mit den Besonderheiten der Plattformen (Teile) zu befüllen sind.
- Der Abschnitt „Wert“ beschreibt den Mehrwert, den eine Plattform, die diese Funktionalität bietet, für die Benutzer, Evaluatoren und Entwickler von zusammengesetzten IoT-Produkten und -Plattformen hat.
- Der Abschnitt „Überlegungen“ beschreibt, welche Aspekte bei der Evaluierung und Zertifizierung dieser SFR berücksichtigt werden sollten.

5.2 Identifizierung und Attestierung von Plattformen und Anwendungen

Die Identifizierung und Attestierung von Anwendungen, Plattformen und Plattformteilen ermöglicht es Kunden, Entwicklern und Evaluatoren, zu verifizieren, dass sie das evaluierte Produkt besitzen. Komplexere Attestierung ermöglicht einen größeren Anwendungsbereich der bescheinigten Daten und eine höhere Vertrauenswürdigkeit dessen, was bescheinigt wird. Die SFR in diesem Unterabschnitt sind zu verwenden, um Identifizierungs- und Attestierungsanforderungen auszudrücken.

5.2.1 Verifizierung der Plattformidentität

5.2.1.1 Anforderung

5.2.1.1.1 Allgemeines

Die Plattform bietet eine eindeutige Identifizierung der Plattform, einschließlich aller Teile und ihrer Versionen.

5.2.1.1.2 Wert

Die Benutzer können erst dann verifizieren, dass es sich um ein sicheres Produkt handelt, wenn sie die Kennungen der Produktteile (Anwendung und vernetzte Plattform) erhalten können. Die Plattform ist ein entscheidender Baustein dieses Identifizierungsprozesses.

Evaluatoren und Entwickler von Zusammensetzungen müssen ebenfalls in der Lage sein, die Identität zu verifizieren (können aber für eine höhere Vertrauenswürdigkeit eine Attestierung verlangen; siehe 5.2.3).

5.2.1.1.3 Überlegungen

Die ST beschreibt die Plattform und definiert damit alle ihre Teile.

Die Entwickler von Plattformen (Teilen) sind verpflichtet, die Identifizierung (allgemein) eindeutig zu halten: Bei allen Produkten dieses Entwicklers, die in der gleichen Weise wie das evaluierte Produkt gekennzeichnet sind, muss es sich um das evaluierte Produkt handeln. Diese funktionale Anforderung ist für alle Plattformen obligatorisch, damit die Kunden verifizieren können, ob sie die richtige Plattform haben. Im Falle einer Zusammensetzung muss die Identifizierung der Plattform auch die integrierten Teile umfassen.

5.2.2 Verifizierung der Identität der Plattforminstanz

5.2.2.1 Anforderung

Die Plattform bietet eine eindeutige Identifizierung dieser spezifischen Instanziierung der Plattform, einschließlich aller ihrer Teile.

5.2.2.2 Wert

Entwickler von Zusammensetzungen benötigen möglicherweise einen Identifikationsschlüssel für eine bestimmte Instanziierung einer Plattform.

5.2.2.3 Überlegungen

Die Entwickler von Plattformen (Teilen) sind verpflichtet, die individuelle Identifizierung der Instanziierung (allgemein) in Verbindung mit der „Verifizierung der Plattformidentität“ eindeutig zu halten.

Ein typisches Beispiel für die Plattformidentität ist die Seriennummer der Plattform.

5.2.3 Attestierung der Echtheit der Plattform

5.2.3.1 Anforderung

Die Plattform attestiert die „Verifizierung der Identität der Plattform“ < und „Verifizierung der Identität der Plattforminstanz“ > in einer Weise, die sicherstellt, dass die Plattform nicht unentdeckt geklont oder verändert werden kann.

5.2.3.2 Wert

Benutzer, Entwickler und Evaluatoren können verifizieren, ob sie das echte (sichere) Produkt haben und nicht einen unsicheren/unvollständigen Klon. Dies gibt den betreffenden Parteien mehr Sicherheit und macht das echte sichere Produkt unverwechselbar und wertvoll. Zusammen mit der SFR „Verifizierung der Identität der Plattforminstanz“ kann die Authentifizierung dieser Plattform angezeigt werden.

Die Benutzer der nach dieser Norm ausgestellten Plattformzertifikate, wie z. B. spezielle Systeme für Produkte, können diese Attestierung als Mittel zur Identifizierung des echten Produkts verwenden.

5.2.3.3 Überlegungen

Die echte Identifizierung wird verwendet, um sicherzustellen, dass es sich bei einer bestimmten Plattform um eine echte Instanziierung der Plattform handelt und nicht um ein Produkt, das sich als eine solche ausgibt (d. h. ein Klon), so dass der Mechanismus und seine Schlüssel für einen Angreifer wertvoll sind, der versucht, die Plattform zu klonen oder auf andere Weise die Marke und den Ruf des Entwicklers zu missbrauchen. Da der Entwickler möglicherweise für Klone, die sich als die echte Plattform ausgeben, zur Rechenschaft gezogen wird oder zumindest einen Rufschaden erleidet, muss ein solches Ziel des Angreifers bei der Evaluierung berücksichtigt werden.

5.2.4 Sichere Initialisierung der Plattform

5.2.4.1 Anforderung

Die Plattform stellt ihre Integrität und Authentizität während der Initialisierung der Plattform sicher. Wenn die Integrität oder Authentizität der Plattform nicht sichergestellt werden kann, geht die Plattform in < Liste der kontrollierten Zustände > über.

5.2.4.2 Wert

Benutzer, Entwickler und Evaluatoren können darauf vertrauen, dass die Plattform beim Start ihre Integrität und Authentizität überprüft hat, so dass ein einsatzfähiges Produkt auf einer sicheren Plattform läuft.

5.2.4.3 Überlegungen

Eine Plattform, die eine Verletzung der Integrität oder Authentizität feststellt, kann die Funktionen „Zurücksetzen der Plattform auf die Werkseinstellungen“ und/oder „Sichere Aktualisierung der Plattform“ anbieten, um ein bestimmtes Produkt wiederherzustellen, oder die Funktion „Stilllegen der Plattform“, um das Produkt zu neutralisieren.

5.2.5 Attestierung des Zustands der Plattform

5.2.5.1 Anforderung

Die Plattform attestiert den Zustand der Plattform, so dass feststellbar ist, dass sich die Plattform in einem bekannten Zustand befindet.

5.2.5.2 Wert

Benutzer, Evaluatoren und Entwickler von Zusammensetzungen können verifizieren, dass sich die Plattform in einem bekannten Zustand befindet, der Teil der Evaluierung war.

5.2.5.3 Überlegung

Dies setzt voraus, dass die „Attestierung der Echtheit der Plattform“ und die „Sichere Initialisierung der Plattform“ ebenfalls implementiert sind.

5.2.6 Attestierung der Echtheit der Anwendung

5.2.6.1 Anforderung

Die Plattform attestiert, dass die Anwendung nicht unbemerkt geklont oder verändert wurde.

5.2.6.2 Wert

Die Benutzer können feststellen, dass sie das echte (sichere) Produkt haben und nicht einen unsicheren/unvollständigen Klon. Dies gibt dem Benutzer mehr Sicherheit und macht das echte (sichere) Produkt unverwechselbar und wertvoll.

5.2.6.3 Überlegungen

Dies setzt voraus, dass die „Attestierung der Echtheit der Plattform“ und die „Sichere Initialisierung der Plattform“ ebenfalls implementiert sind.

5.2.7 Attestierung des Zustands der Anwendung

5.2.7.1 Anforderung

Die Plattform attestiert den Zustand der Anwendung.

5.2.7.2 Wert

Benutzer, Evaluatoren und Entwickler von Zusammensetzungen können verifizieren, dass sich die Anwendung in einem bestimmten Zustand befindet. Dieser spezifische Zustand konnte dann mit einem sicheren Zustand verglichen werden, der Teil der Evaluierung war.

5.2.7.3 Überlegungen

Der attestierte Zustand der Anwendung beschränkt sich auf Informationen, die der Plattform zur Verfügung stehen, wie der statische Code und die Konfiguration der Anwendung sowie andere von der Plattform verwaltete Informationen, z. B. der Zustand des Lebenszyklus einer Anwendung.

Dies setzt voraus, dass die „Attestierung der Echtheit der Anwendung“ und die „Attestierung des Zustands der Plattform“ ebenfalls implementiert sind.

5.3 Produktlebenszyklus: Zurücksetzen auf Werkseinstellungen/Installieren/Aktualisieren/Außerbetriebnahme

5.3.1 Allgemeines

Die Plattform muss die geltend gemachten Sicherheitsfunktionsanforderungen stets einhalten, auch in der Anlauf- und Abschaltphase.

Die SFR in diesem Unterabschnitt sind zu verwenden, um andere übliche Lebenszyklusschritte wie die sichere Installation, Aktualisierung und Außerbetriebnahme der Plattform und Anwendung auszudrücken.

Die Vertraulichkeit der Plattform oder der Anwendung kann wichtig sein, z. B. um geistige Eigentumsrechte zu schützen oder weil diese Vertraulichkeit bei einer Schwachstellenanalyse vorausgesetzt wurde. Da diese Lebenszyklusschritte in der Praxis stattfinden können, muss die Vertraulichkeit der Plattform und der Anwendung gewahrt werden.

5.3.2 Zurücksetzen der Plattform auf die Werkseinstellungen

5.3.2.1 Anforderung

Die Plattform kann in den Zustand zurückgesetzt werden, in dem sie sich befindet, wenn das Produkt, in das die Plattform eingebettet ist, an den Benutzer ausgeliefert wird, bevor persönliche Benutzerdaten, Benutzerzugangsdaten oder eine Benutzerkonfiguration auf der Plattform vorhanden sind.

5.3.2.2 Wert

Der Benutzer ruft diese Funktion auf, um das auf der Plattform erstellte Produkt in seinen ursprünglichen Werkszustand zurückzusetzen und den Lebenszyklus von diesem Punkt aus erneut zu starten; dies kann für den Wiederverkauf genutzt werden.

Die Daten des Benutzers werden garantiert vernichtet, unabhängig von der auf der Plattform laufenden Anwendung.

5.3.2.3 Überlegungen

Die Plattform muss auch nach dem Zurücksetzen auf die Werkseinstellungen noch funktionsfähig sein, so dass der Benutzer das Produkt, in das die Plattform eingebettet ist, neu initialisieren kann.

Dieses Zurücksetzen muss alle Daten (einschließlich der Daten der Anwendung) zerstören, die nach der Auslieferung an den Benutzer empfangen wurden, so dass keine dieser Daten kompromittiert werden können, selbst wenn das Produkt auch für einen Angreifer physisch zugänglich ist.

Diese Funktionalität ermöglicht weiterhin die Speicherung eindeutiger Daten der Plattforminstanz, wie z. B. Daten, die für die „Attestierung der Echtheit der Plattform“ und die „Attestierung des Zustands der Plattform“ benötigt werden, so dass die Plattform und das Produkt weiterhin betriebsbereit sind.

Diese Funktionalität ist nicht dazu gedacht, Angriffe abzuwehren, bei denen ein Angreifer vorübergehend physischen Zugang hat und ihn dann an den Benutzer zurückgibt; diese werden durch „Physische Angreiferabwehr“ abgewehrt.

Wenn die Anwendung (teilweise) defekt ist, muss es immer noch möglich sein, das Produkt auf die Werkseinstellungen zurückzusetzen und dann das Produkt mit den nicht mehr wiederherstellbaren (Benutzer-)Daten im Produkt zu entsorgen. Plattformen mit den Funktionalitäten „Sichere verschlüsselte Speicherung“, „Bereinigung von Restinformationen“ oder „Kryptographischer Schlüsselspeicher“ werden diese Anforderung in der Regel leichter erfüllen können.

Das Zerstörungsverfahren muss für die Technologie des permanenten Speichers und das Angriffspotential geeignet sein. Siehe auch „Bereinigung von Restinformationen“.

5.3.3 Sichere Installation der Anwendung

5.3.3.1 Anforderung

Die Anwendung kann vor Ort so installiert werden, dass die <Vertraulichkeit>, Integrität und Authentizität der Anwendung gewahrt bleibt.

5.3.3.2 Wert

Eine Anwendung kann vor Ort installiert werden, auch beim Endbenutzer und an ungesicherten Produktionsstandorten. Entwickler und Evaluatoren von Zusammensetzungen können sicher sein, dass die Anwendung während dieser Installation nicht verändert (oder optional: offengelegt) wird.

5.3.3.3 Überlegung

Der Installationsmechanismus muss sicherstellen, dass eine Anwendung mit der zugrunde liegenden Plattform in ihrer aktuellen Version kompatibel ist, bevor die Anwendung installiert wird.

Eine Plattform, die diese SFR anbietet, sollte in Erwägung ziehen, zusätzlich zur „Sicheren Aktualisierung der Plattform“ auch eine „Sichere Aktualisierung der Anwendung“ anzubieten, die es dem Produkthanbieter ermöglicht, Verfahren zur Mängelbeseitigung anzubieten, die das gesamte Produkt abdecken.

5.3.4 Sichere Aktualisierung der Plattform

5.3.4.1 Anforderung

Die Plattform kann vor Ort auf eine neuere Version aktualisiert werden, so dass die <Vertraulichkeit>, Integrität und Authentizität der Plattform erhalten bleiben.

5.3.4.2 Wert

Die Behebung von Sicherheitsmängeln, Funktionsfehlern oder Verbesserungen kann eine Aktualisierung der Plattform in der Praxis erfordern. Entwickler und Evaluatoren von Zusammensetzungen können sicher sein, dass der Aktualisierungsmechanismus selbst keinen Angriff ermöglicht.

5.3.4.3 Überlegungen

Es ist zu beachten, dass die fehlende Funktionalität in der ST unter ALC_FLR.SESIP erläutert werden muss.

Der Aktualisierungsmechanismus muss Herabstufungsangriffe („Aktualisierung“ auf eine ältere, potentiell anfälligere Version) abwehren. Was eine „ältere“ oder „neuere“ Version ist, muss in ALC_FLR.SESIP definiert werden.

Zu beachten ist auch, dass Aktualisierungen der Plattform einen (allgemeinen) Identifikationsschlüssel nach der „Verifizierung der Plattformidentität“ haben müssen und möglicherweise eine eigene (erneute) Evaluierung und (Neu-)Zertifizierung erfordern.

5.3.5 Sichere Aktualisierung der Anwendung

5.3.5.1 Anforderung

Die Anwendung kann in der Praxis auf eine neuere Version aktualisiert werden, so dass die < Vertraulichkeit, > Integrität und Authentizität der Anwendung erhalten bleiben.

5.3.5.2 Wert

Die Behebung von Sicherheitsmängeln bzw. Funktionsfehlern oder das Vornehmen von Verbesserungen kann eine Aktualisierung der Anwendung in der Praxis erfordern. Entwickler und Evaluatoren von Zusammensetzungen können sicher sein, dass die Anwendung während dieser Aktualisierung nicht offengelegt oder in unangemessener Weise verändert wird.

5.3.5.3 Überlegung

Der Aktualisierungsmechanismus muss Herabstufungsangriffe („Aktualisierung“ auf eine ältere, potentiell anfälligere Version) abwehren. Was eine „ältere“ oder „neuere“ Version ist, muss in ALC_FLR.SESIP definiert werden.

Der Aktualisierungsmechanismus muss vor der Aktualisierung der Anwendung sicherstellen, dass die neue Version der Anwendung mit der zugrunde liegenden Plattform in ihrer aktuellen Version kompatibel ist.

Eine Plattform, die dies anbietet, kann möglicherweise auch die sichere „Installation von Anwendungen“ anbieten.

5.3.6 Sichere Deinstallation der Anwendung

5.3.6.1 Anforderung

Die Anwendung kann in der Praxis so deinstalliert werden, dass alle Anwendungsdaten < mit Ausnahme von < Liste der nicht zerstörten Objekte > > zerstört werden.

5.3.6.2 Wert

Der Benutzer ruft diese Funktionalität auf, bevor er die Anwendungsinstanz entsorgt oder einem Angreifer auf andere Weise potentiell physischen Zugriff auf die Anwendungsinstanz gewährt. Da alle Anwendungsdaten zerstört werden, werden auch die Daten des Anwendungsbenutzers zerstört.

5.3.6.3 Überlegungen

Der Deinstallationsmechanismus muss Herabstufungsangriffe (Deinstallation der neueren Anwendung, „Neuinstallation“ einer älteren, potentiell anfälligeren Version) abwehren. Was eine „ältere“ oder „neuere“ Version ist, muss in ALC_FLR.SESIP definiert werden.

Die sichere Deinstallation muss alle Daten der Anwendung zerstören, die nach der Installation der Anwendung erhalten wurden. Wenn der Anwendungsentwickler ein Anwendungsobjekt als von der Zerstörung während der Deinstallation ausgenommen gekennzeichnet hat (z.B. Informationen, die die Erkennung eines

Herabstufungsangriffs ermöglichen), dann muss der Deinstallationsvorgang alle Anwendungsdaten zerstören, die nicht ausdrücklich als von der Deinstallation ausgenommen gekennzeichnet sind. Die Vernichtung muss so erfolgen, dass die Anwendungsdaten nicht kompromittiert werden können, selbst wenn das Produkt für einen Angreifer physisch zugänglich ist.

Wenn die Anwendung (teilweise) defekt ist, muss es immer noch möglich sein, die Anwendung zu deinstallieren und dann die Anwendung mit den nicht mehr wiederherstellbaren (Benutzer-)Daten im Produkt zu entsorgen. Plattformen mit den Funktionalitäten „Sichere verschlüsselte Speicherung“, „Bereinigung von Restinformationen“ oder „Kryptographischer Schlüsselspeicher“ werden diese Anforderung in der Regel leichter erfüllen können.

Das Zerstörungsverfahren muss für die Technologie des permanenten Speichers und das Angriffspotential geeignet sein. Siehe auch „Bereinigung von Restinformationen“.

5.3.7 Außerbetriebnahme der Plattform

5.3.7.1 Anforderung

Die Plattform kann außer Betrieb genommen werden.

5.3.7.2 Wert

Der Benutzer ruft diese Funktionalität auf, um den Entsorgungszustand der Plattform zu erreichen, ohne dass es einen Weg zurück in den Betriebszustand gibt. Da alle Daten zerstört werden, werden auch die Daten des Benutzers zerstört.

5.3.7.3 Überlegungen

Die Plattform darf nach der Außerbetriebnahme nicht mehr funktionsfähig sein.

Bei der Außerbetriebnahme müssen alle nach der Produktion erhaltenen Daten (einschließlich der Daten der Anwendung) vernichtet werden.

5.3.8 Rückgabe der Plattform in der Praxis

5.3.8.1 Anforderung

Die Plattform kann ohne Benutzerdaten an den Anbieter zurückgegeben werden.

5.3.8.2 Wert

Der Benutzer ruft diese Funktionalität auf, bevor er das Produkt an den Anbieter zurückgibt, falls eine Untersuchung erforderlich ist, z. B. bei einer in der Praxis beobachteten Störung. Da die Daten des Benutzers vernichtet werden, kann der Benutzer sicher sein, dass nicht einmal der Anbieter auf seine persönlichen Informationen zugreifen kann.

5.3.8.3 Überlegungen

Die Rückgabe in der Praxis muss alle Daten (einschließlich der Daten der Anwendung) zerstören, die nach der Auslieferung an den Benutzer empfangen wurden, so dass keine dieser Daten kompromittiert werden können, selbst wenn das Produkt für einen Angreifer oder den Anbieter physisch zugänglich ist.

Diese Funktionalität ermöglicht weiterhin die Speicherung eindeutiger Daten der Plattforminstanz, wie z. B. Daten, die für die „Attestierung der Echtheit der Plattform“ und die „Attestierung des Zustands der Plattform“ benötigt werden, so dass die Plattform und das Produkt weiterhin betriebsbereit sind.

Diese Funktionalität ist nicht dazu gedacht, Angriffe abzuwehren, bei denen ein Angreifer vorübergehend physischen Zugang hat und ihn dann an den Benutzer zurückgibt; diese werden durch „Physische Angreiferabwehr“ abgewehrt.

5.4 Sichere Kommunikation

5.4.1 Allgemeines

Üblicherweise verwendet ein Produkt sichere Kanäle für die Kommunikation mit einem Server, einem anderen vernetzten Produkt oder einem Cloud-Dienst. Die SFR in diesem Unterabschnitt können zur Beschreibung der Plattform, die der Anwendung diese Funktionalität zur Verfügung stellt, verwendet werden.

Es ist zu beachten, dass die SFR für sichere Kommunikation verwendet werden sollten, wenn die Plattform sichere Kanäle bereitstellt; wenn die Plattform nur die kryptographischen Dienste bereitstellt, die zur Implementierung der sicheren Kanäle verwendet werden, können die in 5.6, Kryptographische Funktionalität, beschriebenen SFR verwendet werden.

5.4.2 Unterstützung für eine sichere Kommunikation

5.4.2.1 Anforderung

Die Plattform bietet einen oder mehrere sichere Kommunikationskanäle.

Der sichere Kommunikationskanal authentifiziert < Liste der Endpunkte > und schützt vor < Liste der Angriffe, einschließlich Offenlegung, Änderung, Wiederholung, Löschung > von Nachrichten zwischen den Endpunkten, unter Verwendung von < Liste der Protokolle und Maßnahmen > .

5.4.2.2 Wert

Der Produktentwickler kann die sicheren Kommunikationskanäle nutzen.

Der Evaluator/Zertifizierer der Zusammensetzung weiß, dass, wenn der Produktentwickler die Funktionalität verwendet, diese in der oben beschriebenen Weise sicher ist.

Der Benutzer, der sich auf den Produktentwickler und den Zertifizierer für Zusammensetzungen verlässt, kann sicher sein, dass sichere Kanäle verwendet werden.

5.4.2.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Liste der Endpunkte: Die Liste der Endpunkte, die mit den nachstehend aufgeführten Protokollen und Maßnahmen zu schützen sind. Endpunkte können nach ihrer Qualität, nach der Schnittstelle, an die sie angeschlossen sind, oder nach einer allgemeineren Kategorie, z. B. alle lokalen Endpunkte, identifiziert werden. Werden für verschiedene Endpunkte unterschiedliche Protokolle und Maßnahmen verwendet, die unterschiedliche sichere Kommunikationskanäle definieren, so muss die SFR wiederholt werden.
- Liste der Angriffe: Die Liste der zu vermeidenden Sicherheitsprobleme, zu denen in der Regel Offenlegung, Änderung, Wiederholung und Löschung gehören.
- Liste der Protokolle und Maßnahmen: Die Liste der zum Schutz des Kommunikationskanals verwendeten Protokolle und sonstigen Maßnahmen, z. B. TLS 1.2 mit TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 oder IPSEC mit Es ist wichtig, dass genügend Informationen zur Verfügung gestellt werden, um die Qualität der verwendeten Algorithmen richtig zu charakterisieren.

Wenn mehrere verschiedene sichere Kommunikationskanäle vorhanden sind, sollte diese SFR wiederholt werden.

Diese SFR könnte anfällig für irreführende Ansprüche sein; die voll autorisierten Zertifizierungsstellen und Evaluatoren des SESIP müssen sicherstellen, dass dies nicht irreführend ist.

5.4.3 Durchsetzung einer sicheren Kommunikation

5.4.3.1 Anforderung

Die Plattform stellt sicher, dass die Kommunikation mit < Liste der Endpunkte > nur über den/die von der Plattform unterstützten sicheren Kommunikationskanal/-kanäle unter Verwendung von < Liste der Protokolle und Maßnahmen > erfolgen kann.

5.4.3.2 Wert

Der Benutzer und der Evaluator/Zertifizierer der Zusammensetzung können darauf vertrauen, dass das Produkt sicher kommuniziert (üblicherweise mit Cloud-Diensten).

5.4.3.3 Überlegungen

Diese SFR setzt voraus, dass mindestens eine Wiederholung der SFR „Unterstützung für eine sichere Kommunikation“ beansprucht wird.

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Liste der Endpunkte: Die Liste der Endpunkte gibt die sicheren Kanäle an, für die die SFR gilt, wie sie in den entsprechenden SFR „Unterstützung für eine sichere Kommunikation“ definiert wurden.
- Liste der Protokolle und Maßnahmen: Die Liste der für die Implementierung des sicheren Kanals verwendeten Protokolle und sonstigen Maßnahmen.

Diese SFR impliziert, dass die Plattform alle ungesicherten Kommunikationsschichten unter dem sicheren Kommunikationskanal (TCP/IP, DHCP, DNS, BT usw.) verarbeitet und dass die Anwendung keinen direkten Zugang zu den Kommunikationsschichten hat, die diesem sicheren Kanal zugrunde liegen.

Diese SFR könnte anfällig für irreführende Ansprüche sein; die voll autorisierten Zertifizierungsstellen und Evaluatoren des SESIP müssen sicherstellen, dass dies nicht irreführend ist.

5.5 Zusätzliche Angreiferabwehr

5.5.1 Allgemeines

In unserem regulären Angreifermodell haben die Angreifer während der Betriebsphase des Angriffs nur logischen (Netzwerk-)Zugriff auf das Produkt, die Anwendung und die Plattform, und daher:

- haben sie keinen physischen Zugang zu der angegriffenen Produktinstanz, und
- sind nicht in der Lage, ihren eigenen feindlichen Code auf der Plattform auszuführen.

Wenn dieses Angreifermodell nicht gültig ist, ermöglicht das Hinzufügen von SFR aus diesem Unterabschnitt eine Abwehr von physischen und Software-Angreifern.

Es ist zu beachten, dass während der Identifizierungsphase davon ausgegangen wird, dass der Angreifer physischen Zugang zu seiner Plattforminstanz hat, wenn er seinen Angriff vorbereitet.

5.5.2 Begrenzte Abwehr von physischen Angreifern

5.5.2.1 Anforderung

Die Plattform erkennt oder verhindert Angriffe durch einen Angreifer mit physischem Zugang, bevor der Angreifer < Liste der Sicherheitsfunktionsanforderungen > kompromittiert.

5.5.2.2 Wert

Für Situationen, in denen ein physischer Angreifer nur für eine begrenzte Anzahl von Funktionen in Frage kommt, z. B. für wertvolle Vermögenswerte, die einen physischen Angriff rechtfertigen, aber nicht für alle Funktionen. Der Angreifer ist nicht auf seinen physischen Angriff beschränkt, sondern auf das Ziel seines Angriffs (die begrenzte Anzahl von SFR).

5.5.2.3 Überlegungen

Alle Angriffe, die durch physischen Zugang innerhalb des Angriffspotentials ermöglicht werden, müssen berücksichtigt werden.

Mit dieser SFR werden nun auch lokale, nicht vernetzte Schnittstellen wie ein USB-Anschluss oder ein MicroSD-Kartenlesegerät bei der Schwachstellenanalyse als für den Angreifer zugänglich betrachtet (z. B. ein „Evil-Maid“-Angriff).

Angreifen, die Produktions- und Debug-Funktionen wie JTAG- und ISD-Funktionen (miss-)brauchen, wird in der Regel durch die Deaktivierung dieser Funktionen vor der Auslieferung an den Kunden begegnet. Invasive Angriffe, wie z. B. physische Manipulationen oder Störungen, werden in der Regel durch die Erkennung und die Außerbetriebnahme des Produkts abgewehrt, bevor der entdeckte Angriff erfolgreich ist. Nicht-invasive Angriffe, wie z. B. Seitenkanalangriffe, werden in der Regel dadurch abgewehrt, dass geheime Informationen, wie z. B. Zeit, Leistung und EM-Emissionen, nicht über Seitenkanäle weitergegeben werden.

Die Bedrohung durch den Austausch des Produkts wird durch diese SFR nicht abgedeckt; ihr kann mit den SFR „Verifizierung der Identität der Plattforminstanz“ und „Attestierung der Echtheit der Plattform“ begegnet werden, die es einer Anwendung oder einem Benutzer ermöglichen, den Austausch zu erkennen.

5.5.3 Physische Angreiferabwehr

5.5.3.1 Anforderung

Die Plattform erkennt oder verhindert Angriffe durch einen Angreifer mit physischem Zugang, bevor der Angreifer eine der anderen Sicherheitsfunktionsanforderungen kompromittiert.

5.5.3.2 Wert

Für Situationen, in denen ein physischer Angreifer im Spiel ist, wie z. B. bei Produkten, die üblicherweise außerhalb eines gesicherten Bereichs verwendet werden, oder wenn die Produkte sehr wertvolle Werte speichern, die einen physischen Angriff rechtfertigen.

5.5.3.3 Überlegungen

Alle Angriffe, die durch physischen Zugang innerhalb des Angriffspotentials ermöglicht werden, müssen berücksichtigt werden.

Mit dieser SFR werden nun auch lokale, nicht vernetzte Schnittstellen wie ein USB-Anschluss oder ein MicroSD-Kartenlesegerät bei der Schwachstellenanalyse als für den Angreifer zugänglich betrachtet (z. B. ein „Evil-Maid“-Angriff).

Angreifern, die Produktions- und Debug-Funktionen wie JTAG- und ISD-Funktionen (miss-)brauchen, wird in der Regel durch die Deaktivierung dieser Funktionen vor der Auslieferung an den Kunden begegnet. Invasive Angriffe, wie z. B. physische Manipulationen oder Störungen, werden in der Regel durch die Erkennung und die Außerbetriebnahme des Produkts abgewehrt, bevor der entdeckte Angriff erfolgreich ist. Nicht-invasive Angriffe, wie z. B. Seitenkanalangriffe, werden in der Regel dadurch abgewehrt, dass geheime Informationen, wie z. B. Zeit, Leistung und EM-Emissionen, nicht über Seitenkanäle weitergegeben werden.

Die Bedrohung durch den Austausch des Produkts wird durch diese SFR nicht abgedeckt; ihr kann mit den SFR „Verifizierung der Identität der Plattforminstanz“ und „Attestierung der Echtheit der Plattform“ begegnet werden, die es einer Anwendung oder einem Benutzer ermöglichen, den Austausch zu erkennen.

5.5.4 Software-Angriffsabwehr: Isolierung der Plattform

5.5.4.1 Anforderung

Die Plattform sorgt für eine Isolierung zwischen der Anwendung und sich selbst, so dass ein Angreifer, der in der Lage ist, den Code als Anwendung auf der Plattform auszuführen, die anderen Sicherheitsfunktionsanforderungen nicht kompromittieren kann.

5.5.4.2 Wert

Für Situationen, in denen ein Angreifer in der Lage sein kann, seinen eigenen Code auf die Plattform zu laden, oder der Angreifer einen Teil der Anwendung unterwandern könnte.

5.5.4.3 Überlegungen

Dies würde in der Regel zumindest ein Betriebssystem mit einer Trennung von Kernel- und Benutzermodus erfordern.

5.5.5 Software-Angriffsabwehr: Isolierung von Plattformteilen

5.5.5.1 Anforderung

Die Plattform bietet eine Isolierung zwischen den Plattformteilen, so dass ein Angreifer, der in der Lage ist, Code in < Liste der angreifbaren Plattformteile > auszuführen, weder die < Vertraulichkeit und > Integrität von < Liste der geschützten Plattformteile > noch die Bereitstellung anderer Sicherheitsfunktionsanforderungen gefährden kann.

5.5.5.2 Wert

Für Situationen, in denen ein Angreifer in der Lage sein kann, seinen eigenen Code auf innere Teile der Plattform zu laden.

Der Plattformentwickler kann die kritischen Werte in verschiedenen Teilen der Plattform trennen und sie so vor Kompromittierungen in anderen Teilen der Plattform schützen.

5.5.5.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Die Liste der anfälligen Plattformteile definiert die Teile der Plattform, die als potentiell von einem Angreifer kompromittiert angesehen und für Angriffe auf andere Teile der Plattform genutzt werden können.

- Die Liste der geschützten Plattformteile definiert die Teile der Plattform, die als potentiell Ziel von Angriffen gelten, die den Code in anderen kompromittierten Teilen ausführen, und die gegen solche Angriffe geschützt sind.

Für eine Plattform, die diese Funktion anbietet, würde in der Regel auch „Software-Angriffsabwehr: Isolierung der Plattform“ beansprucht werden.

Dies würde in der Regel einen Mikrokern oder eine hardwarebasierte Isolierungstechnologie erfordern.

5.5.6 Software-Angriffsabwehr: Isolierung von Anwendungsteilen

5.5.6.1 Anforderung

Die Plattform bietet eine Isolierung zwischen den Teilen der Anwendung, so dass ein Angreifer, der in der Lage ist, Code als einen der < Liste der Anwendungsteile > auszuführen, die < Vertraulichkeit und > Integrität der anderen Anwendungsteile nicht kompromittieren kann.

5.5.6.2 Wert

Für Situationen, in denen der Produktentwickler die kritischen Werte in seinem eigenen Anwendungsteil (Prozess, Programmdatei usw.) abtrennen und so diese Werte vor Kompromittierungen durch andere Teile des Anwendungscodes schützen möchte, die zu komplex sind, um als sicher ausgewiesen zu werden.

5.5.6.3 Überlegungen

Der variable Teil dieser SFR, die Liste der Anwendungsteile, muss die Teiltypen auflisten, aus denen die Anwendung bestehen kann (Module, Prozesse, Applets) und zwischen denen eine gewisse Isolierung vorzusehen ist.

Dies würde in der Regel ein Betriebssystem mit einer Speichertrennung zwischen Anwendungen oder eine interpreterbasierte Plattform mit ähnlichen Zugriffsregeln, wie z. B. Java Card, erfordern.

5.6 Kryptographische Funktionalität

Dies sind gängige kryptographische Funktionen, die eine Plattform bereitstellen kann und die für den Entwickler einer Zusammensetzung oder für einen Produktbenutzer nützlich sind.

Alle beanspruchten Teile der Spezifikation müssen vollständig implementiert sein, daher sind präzise Referenzen erwünscht. Evaluatoren und Zertifizierer müssen alle Aspekte der in Bezug genommenen Teile der Normen verifizieren.

5.6.1 Kryptographische Operation

5.6.1.1 Anforderung

Die Plattform bietet die Funktionalität < Liste der kryptographischen Vorgänge > mit < Liste der Algorithmen > entsprechend < Spezifikation > für Schlüssellängen < Liste der Schlüssellängen > und Modi < Liste der Modi > .

5.6.1.2 Wert

Evaluatoren und Entwickler von Zusammensetzungen können sich darauf verlassen, dass die kryptographischen Funktionen dem Standard entsprechen.

5.6.1.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Die Liste der kryptographischen Vorgänge definiert die in Frage kommenden Vorgänge, die in der Regel aus Verschlüsselung, Entschlüsselung, Hashing, Signierung und Signaturverifizierung ausgewählt werden.
- Die Liste der Algorithmen enthält eine Verweisung auf die verwendeten kryptographischen Algorithmen.
- Die Spezifikation verweist auf die Norm, in der der Vorgang definiert ist (einschließlich eines Abschnitts oder ähnlicher Informationen, falls zutreffend).
- Die Liste der Schlüssellängen definiert die Schlüssellängen, die für diesen kryptographischen Vorgang unterstützt werden.
- Die Liste der Modi definiert die Betriebsmodi, die für diesen kryptographischen Vorgang unterstützt werden.

Ein typisches Beispiel für eine vollständig definierte SFR wäre: Die Plattform bietet der Anwendung Verschlüsselungs- und Entschlüsselungsfunktionen nach NIST FIPS 197 (AES) mit 256-Bit-Schlüsseln im GCM-Modus.

Diese SFR sollte wiederholt werden, wenn mehr als ein Algorithmus bereitgestellt wird. Aus Gründen der Übersichtlichkeit ist es möglicherweise besser, die unterstützten Parameter in einer Tabelle wie Tabelle 5-1 zu definieren:

Tabelle 5-1 — Beispiel für kryptographische Operationen

Operationen	Algorithmus	Spezifikation	Schlüssellängen	Modi
Verschlüsselung, Entschlüsselung	AES	NIST FIPS 197	256	GCM

Die kryptographische Operation muss die Vertraulichkeit der geheimen Schlüssel gegenüber Angreifern wahren. Selbst bei dem Standard-Angreifermodell müssen Timing- und Padding-Orakel-Angriffe berücksichtigt werden, wenn sie innerhalb des Angriffspotentials liegen.

Es ist zu beachten, dass diese SFR für die der Anwendung zur Verfügung stehende kryptographische Funktionsvielfalt bestimmt ist. Diese SFR sollte nicht dazu verwendet werden, die in anderen SFR beanspruchten Kryptofunktionen (wie z. B. „Sichere verschlüsselte Speicherung“, „Sichere Kommunikationsunterstützung“, „Sichere Kommunikationserzwingung“) lediglich neu zu formulieren, es sei denn, diese Funktionsvielfalt wird der Anwendung separat zur Verfügung gestellt.

5.6.2 Generierung kryptographischer Schlüssel

5.6.2.1 Anforderung

Die Plattform bietet eine Möglichkeit, kryptographische Schlüssel zur Verwendung in <Liste der kryptographischen Algorithmen> entsprechend <Spezifikation> für Schlüssellängen <Liste der Schlüssellängen> zu generieren.

5.6.2.2 Wert

Evaluatoren und Entwickler von Zusammensetzungen können sich darauf verlassen, dass die kryptographische Schlüsselgenerierung dem Standard entspricht.

5.6.2.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Die Liste der kryptographischen Algorithmen enthält eine Verweisung auf die verwendeten Algorithmen.
- Die Spezifikation verweist auf die Norm, in der der Vorgang definiert ist (einschließlich eines Abschnitts oder ähnlicher Informationen, falls zutreffend).
- Die Liste der Schlüssellängen definiert die Schlüssellängen, die für diesen kryptographischen Vorgang unterstützt werden.

Diese SFR sollte wiederholt werden, wenn Schlüssel für mehr als einen Algorithmus generiert werden. Aus Gründen der Übersichtlichkeit ist es möglicherweise besser, die unterstützten Parameter in einer Tabelle zu definieren.

Die Spezifikation des Algorithmus zur Schlüsselgenerierung kann für die Verwendung in spezifischen Produktevaluierungsprogrammen nützlich sein. Unabhängig vom verwendeten Algorithmus gilt für jeden Angriff innerhalb des Angriffspotentials: Auf Angriffe wie ROCA muss stets geprüft werden.

5.6.3 Kryptographischer Keystore (Schlüsselspeicher)

5.6.3.1 Anforderung

Die Plattform bietet eine Möglichkeit, < Liste von Vermögenswerten, wie kryptographische Schlüssel und Passwörter > so zu speichern, dass nicht einmal die Anwendung die < Auswahl: Vertraulichkeit, Integrität, Authentizität > dieser Daten kompromittieren kann. Diese Daten können für die kryptographischen Operationen < Liste der Operationen > verwendet werden.

5.6.3.2 Wert

Evaluatoren und Entwickler von Zusammensetzungen können sich darauf verlassen, dass Schlüssel nicht versehentlich offengelegt werden können, vorausgesetzt, die Schlüssel werden nur im Keystore gespeichert.

5.6.3.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Die Liste der Vermögenswerte definiert die Arten von Vermögenswerten, die durch den Keystore zu schützen sind.
- Die Eigenschaften Vertraulichkeit, Integrität und Authentizität definieren den Schutz, der geleistet wird.
- Die Liste der Operationen definiert die Operationen, die eine Anwendung mit den im Keystore gespeicherten Vermögenswerten durchführen kann, ohne auf die Werte der Vermögenswerte zugreifen zu müssen.

Ein Software-Schlüsselspeicher in der Plattform erfordert in der Regel entweder „Software-Angriffsabwehr“: Isolierung der Plattform“ in der Plattform oder Codeüberprüfung bzw. automatische Codeverifizierung des Produkts.

5.6.4 Kryptographische Generierung von Zufallszahlen

5.6.4.1 Anforderung

Die Plattform bietet eine Möglichkeit, auf der Grundlage von < Liste der Entropiequellen > Zufallszahlen nach <Spezifikation> zu erzeugen.

5.6.4.2 Wert

Evaluatoren und Entwickler von Zusammensetzungen können sich darauf verlassen, dass die kryptographische Schlüsselgenerierung dem Standard entspricht. Sie kann auch für andere Verwendungszwecke von starken kryptographischen Zahlen verwendet werden, z. B. für die Authentifizierung usw.

5.6.4.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Die Liste der Entropiequellen legt fest, wie die Zufälligkeit aus physischen und rechnerischen Ressourcen generiert wird.
- Die Spezifikation verweist auf die Norm, in der der Vorgang definiert ist (einschließlich eines Abschnitts oder ähnlicher Informationen, falls zutreffend).

Die Spezifikation des Algorithmus zur Zahlengenerierung kann für die Verwendung in spezifischen Produktevaluierungsprogrammen nützlich sein. Unabhängig vom verwendeten Algorithmus gilt für jeden Angriff innerhalb des Angriffspotentials: Es muss stets auf schwache Entropie und Vorhersagbarkeit geprüft werden.

5.7 Konformitätsfunktionen

5.7.1 Allgemeines

Dies sind allgemein geforderte Eigenschaften aus verschiedenen Produktomänen und -systemen.

5.7.2 Sichere vertrauenswürdige Speicherung

5.7.2.1 Anforderung

Die Plattform stellt sicher, dass alle gespeicherten Benutzerdaten, mit Ausnahme von < Liste der im Klartext gespeicherten Daten >, geschützt sind, um ihre Integrität, Authentizität und Bindung an die Plattforminstanz sicherzustellen.

5.7.2.2 Wert

Evaluatoren und Entwickler von Zusammensetzungen können sich auf die Integrität und Authentizität der gespeicherten Daten verlassen.

5.7.2.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- In der Liste der im Klartext gespeicherten Daten sind die Kategorien aufgeführt, die von der sicheren verschlüsselten Speicherung ausgeschlossen sind, die für alle anderen Daten verwendet werden sollte.

Der verwendete Mechanismus muss sowohl die Integrität als auch die Authentizität der gespeicherten Daten schützen.

Es ist zu beachten, dass, wenn der Speicher gegen das Auslesen durch physische Angreifer geschützt werden muss, „Physische Angreiferabwehr“ verwendet werden sollte.

5.7.3 Sichere vertrauliche Speicherung

5.7.3.1 Anforderung

Die Plattform stellt sicher, dass alle von der Anwendung gespeicherten Daten, mit Ausnahme von <Liste der gespeicherten Daten>, geschützt sind, um ihre Vertraulichkeit, Integrität, Authentizität und Bindung an die Plattforminstanz sicherzustellen.

5.7.3.2 Wert

Evaluatoren und Entwickler von Zusammensetzungen können sich auf die Vertraulichkeit, Integrität und Authentizität der gespeicherten Daten verlassen.

5.7.3.3 Überlegungen

Kann in Situationen verwendet werden, in denen der Speicher durch nicht verschlüsselte Mittel geschützt ist.

5.7.4 Sichere verschlüsselte Speicherung

5.7.4.1 Anforderung

Die Plattform stellt sicher, dass alle gespeicherten Benutzerdaten, mit Ausnahme von < Liste der im Klartext gespeicherten Daten >, wie in <Spezifikation> angegeben, mit einem eindeutigen Schlüssel der Plattforminstanz der Schlüssellänge < Schlüssellänge > verschlüsselt werden.

5.7.4.2 Wert

Evaluatoren und Entwickler von Zusammensetzungen können sich ohne weitere Aktivitäten darauf verlassen, dass (implizit) gespeicherte Daten verschlüsselt sind.

5.7.4.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- In der Liste der im Klartext gespeicherten Daten sind die Kategorien aufgeführt, die von der sicheren verschlüsselten Speicherung ausgeschlossen sind, die für alle anderen Daten verwendet werden sollte.
- Die Spezifikation verweist auf die Norm, in der der Verschlüsselungsmechanismus definiert ist (einschließlich eines Abschnitts oder ähnlicher Informationen, falls zutreffend).
- Die Schlüssellänge ist die Größe des für die Verschlüsselung verwendeten Schlüssels.

Der verwendete Verschlüsselungsmechanismus muss sowohl die Vertraulichkeit als auch die Integrität der gespeicherten Daten schützen.

Der zur Verschlüsselung der Daten verwendete Schlüssel muss so generiert werden, dass eine Kompromittierung des Schlüssels einer Produktinstanz keine leichtere Kompromittierung einer anderen Produktinstanz ermöglicht; außerdem muss die Vertraulichkeit dieses Schlüssels geschützt werden.

Dies kann mit Hilfe der Funktionalität „Kryptographische Operation“ implementiert werden, aber diese SFR sollte nur in Anspruch genommen werden, wenn die Funktionalität dieser SFR dem Benutzer (z. B. der Anwendung) direkt zur Verfügung steht.

5.7.5 Sichere Datenserialisierung

5.7.5.1 Anforderung

Die Plattform stellt sicher, dass alle außerhalb der direkten Kontrolle der Plattform gespeicherten Daten, mit Ausnahme von < Liste der außerhalb der direkten Kontrolle der Plattform gespeicherten Daten >, so geschützt werden, dass die < Auswahl: Vertraulichkeit, Integrität, Authentizität, Bindung an die Plattforminstanz, Versionierung > sichergestellt ist.

5.7.5.2 Wert

Evaluatoren und Entwickler von Zusammensetzungen können sich darauf verlassen, dass die Daten außerhalb der Plattform gespeichert werden können, ohne dass sie verändert oder offengelegt werden.

5.7.5.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Die Liste der außerhalb der direkten Kontrolle der Plattform gespeicherten Daten.
- Die durch den Mechanismus sichergestellten Schutzmaßnahmen.

Falls kryptographische Algorithmen verwendet werden, sind ebenfalls anzugeben:

- Die Spezifikation verweist auf die Norm, in der die für die Datenverschlüsselung verwendeten kryptographischen Algorithmen definiert sind (einschließlich eines Abschnitts oder ähnlicher Informationen, falls zutreffend).
- Die Schlüssellänge ist die Größe der Schlüssel, die von den für die Datenverschlüsselung verwendeten kryptographischen Algorithmen verwendet werden.

Der im Verschlüsselungsmechanismus verwendete Schlüssel muss so generiert werden, dass eine Kompromittierung des Schlüssels einer Produktinstanz keine leichtere Kompromittierung einer anderen Produktinstanz ermöglicht.

Dies kann mit Hilfe der Funktionalität „Kryptographische Operation“ implementiert werden, aber diese SFR sollte nur in Anspruch genommen werden, wenn die Funktionalität dieser SFR dem Benutzer (z. B. der Anwendung) direkt zur Verfügung steht.

Es ist zu beachten, dass, wenn der Speicher gegen das Auslesen durch physische Angreifer geschützt werden muss, „Physische Angreiferabwehr“ verwendet werden sollte.

5.7.6 Bereinigung von Restinformationen

5.7.6.1 Anforderung

Die Plattform stellt sicher, dass < Liste der Daten >, mit Ausnahme von < Liste der Daten, die nicht automatisch gelöscht werden >, mit dem in < Spezifikation > angegebenen Verfahren gelöscht wird, bevor der Speicher von der Plattform oder Anwendung erneut verwendet wird und bevor ein Angreifer darauf zugreifen kann.

5.7.6.2 Wert

Evaluatoren und Entwickler von Zusammensetzungen können sich darauf verlassen, dass (implizit) gespeicherte und kopierte Daten automatisch, ohne weitere Aktivitäten, gelöscht werden.

5.7.6.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Die Liste der Daten definiert die Kategorien der automatisch zu löschenden Daten und dürfte sehr umfangreich sein (siehe unten).
- Die Liste der Ausnahmen von Daten, die nicht automatisch gelöscht werden, definiert die Kategorien, von denen nicht erwartet wird, dass sie automatisch gelöscht werden.
- Die Spezifikation verweist auf die Norm, in der der Verschlüsselungsmechanismus definiert ist (einschließlich eines Abschnitts oder ähnlicher Informationen, falls zutreffend).

In der Regel würde die Liste der Daten „alle Daten der Anwendung, die von der Anwendung nicht mehr verwendet werden“ lauten, so dass ein „Lazy Erasure“ nur bei der Wiederverwendung des Speichers und nicht sofort bei der Freigabe des Speichers erfolgt, um den üblichen Softwareimplementierungen zu entsprechen.

Angriffe wie der Kaltstartangriff müssen in Betracht gezogen werden.

5.7.7 Erstellung und Speicherung von Auditprotokollen

5.7.7.1 Anforderung

Die Plattform erstellt und verwaltet ein Auditprotokoll von <Liste der bedeutenden Sicherheitsereignisse> und ermöglicht den Zugriff und die Analyse dieser Protokolle nach einer bestimmten <Zugriffskontrollregelung>.

5.7.7.2 Wert

Evaluatoren und Entwickler von Zusammensetzungen können sich darauf verlassen, dass (implizit) gespeicherte und kopierte Daten automatisch, ohne weitere Aktivitäten, gelöscht werden.

5.7.7.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Die Liste der bedeutenden Sicherheitsereignisse definiert die Ereignisse im Protokoll, von denen erwartet wird, dass sie eine breite Abdeckung der möglichen Ereignisse der Plattform bieten.
- Die Zugriffskontrollregelung legt die Bedingungen fest, unter denen die Protokolle eingesehen werden dürfen, in der Regel von bestimmten privilegierten Benutzern nach der Authentifizierung.

Auch die „Software-Angriffsabwehr: Isolierung der Plattform“ könnte als Beleg für diese Behauptung angeführt werden.

5.7.8 Zuverlässiger Index

5.7.8.1 Anforderung

Die Plattform implementiert eine streng ansteigende Funktion.

5.7.8.2 Wert

Dieses Merkmal kann verwendet werden, um Versionen oder sogar die Zeit zu verfolgen.

5.7.8.3 Überlegungen

Ein nur ansteigender Zähler von Ereignissen oder Timer-Ticks erfüllt diese Anforderung ebenso wie eine geschützte Zeitmessung.

5.7.9 Sicheres Debugging

5.7.9.1 Anforderung

Die Plattform bietet Debug-Funktionalität nur für < Liste der Endpunkte > , die nach <Spezifikation> authentifiziert sind.

Die Plattform stellt sicher, dass alle gespeicherten Benutzerdaten, mit Ausnahme von < Liste der Ausnahmen > , unzugänglich gemacht werden.

5.7.9.2 Wert

Die Entwickler von Zusammensetzungen können ihre Produkte debuggen, ohne die Sicherheit der Daten ihrer Benutzer zu kompromittieren.

5.7.9.3 Überlegungen

Die variablen Teile dieser SFR werden folgendermaßen ausgefüllt:

- Die Liste der Endpunkte führt die Endpunkte auf (möglicherweise mit ihrer physischen Verbindung und den erforderlichen Authentifizierungsdaten), die die Plattform in den Debug-Modus versetzen dürfen.
- Die Spezifikation verweist auf die Norm, in der der Authentifizierungsmechanismus definiert ist (einschließlich eines Abschnitts oder ähnlicher Informationen, falls zutreffend).
- In der Liste der Ausnahmen sind die Daten aufgeführt, die während des Debugging vom Schutz ausgeschlossen sind. Dazu sollten keine Benutzerdaten gehören, bei denen die begründete Erwartung besteht, dass sie personenbezogene Daten des Benutzers enthalten.

Dies kann über die Funktion „Unterstützung der sicheren Kommunikation“ erfolgen.

5.7.10 Sichere Wiederherstellung

5.7.10.1 Anforderung

Die Plattform erkennt die Anomalien < Liste der Anomalien > und kehrt zu einem bekannten Zustand < Liste der kontrollierten Zustände > zurück.

5.7.10.2 Wert

Um die Ausfallsicherheit sicherzustellen, könnte die Plattform einen Mechanismus bereitstellen, der die Rückkehr zu einem bestimmten kontrollierten Zustand ermöglicht, z. B. zu einem Aktualisierungs- oder Wiederherstellungszustand.

5.7.10.3 Überlegungen

Dies kann ein gefährlicher Mechanismus sein, da z. B. ein Rollback gewisse Sicherheitsnachteile mit sich bringen kann, was bei der Bewertung berücksichtigt werden muss. Es sollte darauf geachtet werden, dass kein unangemessener Zustand wiederhergestellt wird, z. B. sollten monoton inkrementierende Zähler und Angriffszähler nicht dekrementiert werden.

5.7.11 Sicheres Backup und Wiederherstellung

5.7.11.1 Anforderung

Die Plattform stellt sicher, dass Benutzerdaten < Liste der Daten >, mit Ausnahme von < Liste der Ausnahmen >, so gesichert und wiederhergestellt werden können, dass die < Vertraulichkeit, > Integrität und Authentizität geschützt ist.

5.7.11.2 Wert

Dies kann genutzt werden, um die Anforderungen der IoT-Gerätenormen zu unterstützen, wie z. B. IEC 62443 CR 7.3 Control system backup.

5.7.11.3 Überlegungen

Wird die Vertraulichkeit nicht beansprucht, müssen die Auswirkungen auf andere SFR berücksichtigt werden: Alle Daten, die ohne Vertraulichkeit gesichert werden können, sollten bei der Analyse der SFR als dem Angreifer bekannt betrachtet werden.

Es sollte darauf geachtet werden, dass kein unangemessener Zustand wiederhergestellt wird, z. B. sollten monoton inkrementierende Zähler und Angriffszähler nicht dekrementiert werden.

5.7.12 Allgemeines Sicherheitsmerkmal der Plattform

5.7.12.1 Anforderung

Die Plattform bietet die < Sicherheitsoperation(en) > nach < Spezifikation(en) > .

5.7.12.2 Wert

Die Plattform implementiert ein spezielles Sicherheitsmerkmal, das nicht zu den in diesem Katalog aufgeführten allgemeinen IoT-Merkmalen gehört, und seine Ausführung muss speziell bewertet werden.

Dies könnte z. B. zur Abdeckung der Anforderungen der IEC 62443 CR 3.4 über „Software- und Informationsintegrität“ verwendet werden.

5.7.12.3 Überlegungen

Diese SFR darf nur verwendet werden, wenn die von der Plattform implementierte Funktionalität nicht bereits durch eine SFR im Katalog abgedeckt ist.

5.8 Zugriffskontrolle

Dies sind allgemein geforderte Eigenschaften aus verschiedenen Produktomänen und -systemen.

5.8.1 Privilegierte Zugriffskontrolle

5.8.1.1 Anforderung

Die Plattform ermöglicht den Zugriff auf < Liste der zulässigen Ressourcen/Operationen > ausschließlich auf der Grundlage von < Liste der Privilegien > .

5.8.1.2 Wert

Diese SFR kann verwendet werden, um Zugriffskontrollmechanismen zu verlangen, die nicht auf der regulären Benutzerauthentifizierung beruhen, wie zum Beispiel die Zugriffskontrolle auf der Grundlage von:

- einem physischen Zugang zu einer Schaltfläche;
- der physischen/virtuellen Adresse der Anfrage;
- dem Anforderungskontext, z. B. Root/User-Modus, NSPE/SPE-Modus, Benutzer-/Prozess-ID usw.;
- der Herkunft aus dem Netzwerk, z. B. von einem internen oder externen Port.

5.8.1.3 Überlegungen

Die Implementierung, die dieses Merkmal erfüllt, kann mit derjenigen, die die Isolierungsanforderung erfüllt, gemeinsam oder teilweise gemeinsam sein, z. B. kann die Implementierung von ARM TrustZone verwendet werden, um die Plattform (z. B. SPE) von der Anwendung (z. B. NSPE) zu isolieren und eine Zugriffskontrolle auf der Grundlage des NSPE/SPE-Ursprungs durchzuführen.

5.8.2 Authentifizierte Zugriffskontrolle

5.8.2.1 Anforderung

Die Plattform ermöglicht nur < Liste der Rolle(n) > , die identifiziert, authentifiziert und autorisiert sind, die Durchführung von < Liste der zulässigen Ressourcen/Operationen > zu ermöglichen.

5.8.2.2 Wert

Diese SFR kann verwendet werden, um eine Authentifizierung für eingeschränkte Operationen zu verlangen, so dass Computer- oder menschliche Rollen den Zugang zu eingeschränkten Funktionen ermöglichen, z. B. um die Übereinstimmung mit EN 303645 Bestimmung 5.1-2, 5.2-4, 5.5-4 und 5.5-5, oder IEC 62443 CR 1.1 Identifizierung und Authentifizierung menschlicher Benutzer, CR 1.3 Kontoverwaltung, CR 2.1 Durchsetzung von Berechtigungen und CR 2.12 Nichtabstreitbarkeit zu zeigen.

5.8.2.3 Überlegungen

Das Management der den Rollen zugewiesenen Zugangsentsitäten, die Rollen, die Berechtigungen der Rollen und die zulässigen Operationen sollten ebenfalls als Operation betrachtet und in die kodierte Spezifikation aufgenommen werden. Zur besseren Lesbarkeit ist es möglicherweise sinnvoll, diese SFR zu wiederholen.

5.9 Verfügbarkeit

5.9.1 Allgemeines

Dies sind allgemein geforderte Eigenschaften aus verschiedenen Produktomänen und -systemen.

5.9.2 Eingeschränkte Anforderungen an die Umgebungsfähigkeit

5.9.2.1 Anforderung

Die Plattform begrenzt ihre Anforderungen an ihre Umgebung entsprechend: < Liste der Regeln > .

5.9.2.2 Wert

Die Plattform könnte sich in Situationen befinden, in denen die Umgebung darauf angewiesen ist, dass die Plattform keine unangemessenen Anforderungen an die Umgebung stellt, um Denial-of-Service-Angriffe oder eine Überlastung dieser Infrastruktur zu verhindern, d. h. dass die Plattform keine Quelle eines (unbeabsichtigten) Denial-of-Service-Angriffs auf die Umgebung ist.

In einem Stromnetz kann ein Angreifer beispielsweise versuchen, den Strombedarf vieler Geräte böswillig zu manipulieren und so den Ausfall von Systemkomponenten oder Kraftwerken zu verursachen. Diese SFR kann verwendet werden, um sicherzustellen, dass die Plattform ihre Übergangsgeschwindigkeit begrenzt (z. B. Abkopplung von Lasten höchstens einmal je Stunde)

5.9.2.3 Überlegungen

Diese SFR beschreibt die Beschränkungen der Plattform, die vermeiden sollen, dass sie die Ursache für einen Denial-of-Service-Angriff auf die Umgebung ist. Wenn die Plattform gegen Denial-of-Service-Angriffe geschützt werden muss, ist die SFR in 5.9.2 zu verwenden.

5.9.3 Unterstützung der Verfügbarkeit

5.9.3.1 Anforderung

Die Plattform stellt die Verfügbarkeit und den ordnungsgemäßen Betrieb von < Liste der Sicherheitsfunktionsanforderungen > für die folgenden Situationen < Liste der Situation > sicher.

5.9.3.2 Wert

Dies kann verwendet werden, um die Abwehr von Denial-of-Service-Angriffen auf die Plattform zu demonstrieren, wie z. B. die Anforderungen der IEC 62443 CR 7.1 Denial-of-Service-Schutz und CR 7.2 Ressourcenmanagement.

5.9.3.3 Überlegungen

Alle Angriffe innerhalb des Angriffspotentials und jede zusätzliche Abwehr des Angreifers gehören zum Anwendungsbereich.

Diese SFR beschreibt die Abwehr der Plattform von Denial-of-Service-Angriffen. Wenn die Beschränkungen der Plattform zur Vermeidung eines selbst verursachten Denial-of-Service-Angriffs auf die Umgebung erforderlich sind, ist die SFR in 5.9.1 zu verwenden.

5.10 Mindestsatz an Sicherheitsfunktionsanforderungen

Die folgenden SFR sind, sofern zutreffend, obligatorisch und müssen Teil aller Sicherheitsvorgaben sein:

- „Verifizierung der Plattformidentität“: Diese Funktion ist für den Evaluators wichtig, um sicherzustellen, dass die Sicherheitsevaluierung auf dem erwarteten Plattfortmtyp und der erwarteten Version durchgeführt wird, und für den Benutzer, um zu überprüfen, ob die verwendete Plattform die erwartete ist.
- „Sichere Aktualisierung der Plattform“ oder die Begründung unter ALC_FLR.SESIP, warum Aktualisierungen nicht anwendbar sind: Diese Funktion ist für Sicherheitszwecke unerlässlich, wenn möglich, um die Korrektur von Sicherheitsproblemen zu ermöglichen, die in der Praxis festgestellt werden könnten.

6 Sicherheitsprozesspakete (SPP)

6.1 Allgemeines

IoT-Normen verlangen nicht nur, dass die zugrunde liegende Plattform (SFR) Sicherheitsfunktionen implementiert, sondern auch, dass spezifische Sicherheitsprozesse von den Entwicklern implementiert und auf den Fall der zu evaluierenden Plattform angewandt werden; solche Prozesse könnten sich auf alle Phasen des Lebenszyklus der Plattform beziehen (z. B. Entwicklung, Produktion, Betrieb).

Um die Verifizierung der Anwendung solcher Sicherheitsprozesse zu ermöglichen, was dann den Nachweis der Konformität mit IoT-Normen unterstützen kann, definiert dieser Abschnitt das Konzept des Sicherheitsprozesspakets und einen Basiskatalog von SPP, die in SESIP-Sicherheitsvorgaben und -Profilen beansprucht werden können.

ANMERKUNG 1 Dies ist von ALC-Komponenten zu unterscheiden, bei denen es sich um Evaluierungsaufgaben handelt, die darauf abzielen, durch die Bewertung des Umgangs des Entwicklers mit der Plattform (Entwicklung, Produktion, Auslieferung und Management der Mängelbeseitigung) die Vertrauenswürdigkeit der Plattform und der mit ihr verbundenen Vermögenswerte zu erhöhen, die aber nicht den Anspruch auf die Anwendung eines spezifischen Sicherheitsprozesses auf die Plattform zulassen.

ANMERKUNG 2 Zielsetzungen für die Umgebung können diesen Bedarf nicht decken, da es sich zwar um Anforderungen handelt, die jedoch vom Evaluator nicht verifiziert werden.

Der Begriff Paket wird verwendet, da die Anforderungen an die Prozessimplementierung mit den folgenden spezifischen Evaluierungsanforderungen verbunden sind:

- Der Entwickler muss die Spezifikationen des beanspruchten Sicherheitsprozesses und Beweise für die Anwendung dieses Prozesses auf die zu evaluierende Plattform vorlegen.
- Der Evaluator muss die Korrektheit der Anforderung und ihre Anwendung für den Plattformfall auf der Grundlage der Eingaben des Entwicklers verifizieren; wenn das Ergebnis des Prozesses auf der Plattformimplementierung sichtbar ist, darf die Verifizierung auch auf der Überprüfung des Quellcodes (falls zutreffend) und/oder auf den Prüfergebnissen basieren.

Für die Beanspruchung von SPP gelten die gleichen Regeln wie für SFR in 5.1.

6.2 Sichere Entwicklung

6.2.1 Anforderung

Bei der Entwicklung der Plattform wurde der in <Norm/Spezifikation> beschriebene sichere Entwicklungsprozess auf die Plattform angewandt.

6.2.2 Wert

Die Aufnahme dieses Paketanspruchs in ein(e) SESIP-Sicherheitsvorgabe oder -Profil ermöglicht das Erstellen von Nachweisen, dass die Anforderungen an die sichere Entwicklung aus einer referenzierten Spezifikation/Norm auf die zu evaluierende Plattform angewandt wurden.

Beispiel: Anwendung des Security-by-Design-Prozesses aus einer Spezifikation/Norm, z. B. ISO/SAE 21434:2021.