

	DIN EN ISO/IEC 15408-2	
ICS 35.030	<div>Entwurf</div>	Einsprüche bis 2024-05-22 Vorgesehen als Ersatz für DIN EN ISO/IEC 15408-2:2020-12
<p>Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Evaluationskriterien für IT-Sicherheit – Teil 2: Sicherheitsfunktionskomponenten (ISO/IEC 15408-2:2022); Deutsche und Englische Fassung EN ISO/IEC 15408-2:2023</p> <p>Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components (ISO/IEC 15408-2:2022); German and English version EN ISO/IEC 15408-2:2023</p> <p>Sécurité de l’information, cybersécurité et protection de la vie privée – Critères d’évaluation pour la sécurité des technologies de l’information – Partie 2: Composants fonctionnels de sécurité (ISO/IEC 15408-2:2022); Version allemande et anglaise EN ISO/IEC 15408-2:2023</p> <p>Anwendungswarnvermerk</p> <p>Dieser Entwurf mit Erscheinungsdatum 2024-03-22 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.</p> <p>Weil das beabsichtigte Dokument von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.</p> <p>Stellungnahmen werden erbeten</p> <ul style="list-style-type: none">– 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. <p>Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.</p> <p>Gesamtumfang 605 Seiten</p> <p>DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)</p>		

Nationales Vorwort

Der Text von ISO/IEC 15408-2:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 15408-2:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

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

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

ISO/IEC 15408-1:2022	siehe	E DIN EN ISO/IEC 15408-1:2024-01
ISO/IEC 15408-3	siehe	DIN EN ISO/IEC 15408-3
ISO/IEC 18045	siehe	DIN EN ISO/IEC 18045
ISO/IEC 29100	siehe	DIN EN ISO/IEC 29100

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

Änderungen

Gegenüber DIN EN ISO/IEC 15408-2:2020-12 wurden folgende Änderungen vorgenommen:

- a) neue Sicherheitsfunktionskomponenten wurden eingeführt;
- b) redaktionelle Überarbeitung des Dokuments.

Nationaler Anhang NA (informativ)

Literaturhinweise

E DIN EN ISO/IEC 15408-1:2024-01, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit — Teil 1: Einführung und allgemeines Modell (ISO/IEC 15408-1:2022); Deutsche und Englische Fassung prEN ISO/IEC 15408-1:2023*

DIN EN ISO/IEC 15408-3, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit — Teil 3: Sicherheit Gewährleistungskomponenten*

DIN EN ISO/IEC 18045, *Informationstechnik — Sicherheitstechniken — Methodik für die Bewertung der IT-Sicherheit*

DIN EN ISO/IEC 29100, *Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Datenschutz*

– *Entwurf* –

E DIN EN ISO/IEC 15408-2:2024-04

– Leerseite –

**Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre –
Evaluationskriterien für IT-Sicherheit – Teil 2: Sicherheitsfunktionskomponenten
(ISO/IEC 15408-2:2022)**

Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components (ISO/IEC 15408-2:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée – Critères d'évaluation pour la sécurité des technologies de l'information – Partie 2: Composants fonctionnels de sécurité (ISO/IEC 15408-2:2022)

Inhalt

	Seite
Europäisches Vorwort	22
Vorwort	23
Einleitung	25
1 Anwendungsbereich	26
2 Normative Verweisungen	26
3 Begriffe	26
4 Abkürzungen	28
5 Übersicht	29
5.1 Allgemeines	29
5.2 Aufbau dieses Dokuments	29
6 Paradigma für Funktionsanforderungen	30
7 Sicherheitsfunktionskomponenten	34
7.1 Übersicht	34
7.1.1 Allgemeines	34
7.1.2 Klassenstruktur	34
7.1.3 Familienstruktur	35
7.1.4 Komponentenstruktur	37
7.2 Komponentenkatalog	38
8 Klasse FAU: Sicherheitsaudit	39
8.1 Klassenbeschreibung	39
8.2 Automatische Antwort beim Sicherheitsaudit (FAU_ARP)	40
8.2.1 Familienverhalten	40
8.2.2 Komponentenebenen und Beschreibung	40
8.2.3 Management von FAU_ARP.1	40
8.2.4 Audit von FAU_ARP.1	41
8.2.5 FAU_ARP.1 Sicherheitsalarme	41
8.3 Datengenerierung beim Sicherheitsaudit (FAU_GEN)	41
8.3.1 Familienverhalten	41
8.3.2 Komponentenebenen und Beschreibung	41
8.3.3 Management von FAU_GEN.1, FAU_GEN.2	41
8.3.4 Audit von FAU_GEN.1, FAU_GEN.2	41
8.3.5 FAU_GEN.1 Generierung von Auditdaten	42
8.3.6 FAU_GEN.2 Verknüpfung der Benutzeridentität	42
8.4 Sicherheitsauditanalyse (FAU_SAA)	42
8.4.1 Familienverhalten	42
8.4.2 Komponentenebenen und Beschreibung	43
8.4.3 Management von FAU_SAA.1	43
8.4.4 Management von FAU_SAA.2	43
8.4.5 Management von FAU_SAA.3	43
8.4.6 Management von FAU_SAA.4	43
8.4.7 Audit von FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4	44
8.4.8 „FAU_SAA.1 Potential violation analysis“	44
8.4.9 FAU_SAA.2 Profilbasierte Erkennung von Anomalien	44
8.4.10 FAU_SAA.3 Einfache Angriffsheuristiken	45
8.4.11 FAU_SAA.4 Komplexe Angriffsheuristiken	45
8.5 Sicherheitsauditüberprüfung (FAU_SAR)	46
8.5.1 Familienverhalten	46
8.5.2 Komponentenebenen und Beschreibung	46
8.5.3 Management von FAU_SAR.1	46
8.5.4 Management von FAU_SAR.2, FAU_SAR.3	46
8.5.5 Audit von FAU_SAR.1	46

8.5.6	Audit von FAU_SAR.2	46
8.5.7	Audit von FAU_SAR.3	47
8.5.8	FAU_SAR.1 Auditüberprüfung	47
8.5.9	FAU_SAR.2 Beschränkte Auditüberprüfung	47
8.5.10	FAU_SAR.3 Auswählbare Auditüberprüfung	47
8.6	Sicherheitsaudit Ereignisauswahl (FAU_SEL)	47
8.6.1	Familienverhalten	47
8.6.2	Komponentenebenen und Beschreibung	48
8.6.3	Management von FAU_SEL.1	48
8.6.4	Audit von FAU_SEL.1	48
8.6.5	FAU_SEL.1 Auswählbares Audit	48
8.7	Sicherheitsaudit Datenspeicherung (FAU_STG)	48
8.7.1	Familienverhalten	48
8.7.2	Komponentenebenen und Beschreibung	48
8.7.3	Management von FAU_STG.1	49
8.7.4	Management von FAU_STG.2	49
8.7.5	Management von FAU_STG.3	49
8.7.6	Management von FAU_STG.4	49
8.7.7	Management von FAU_STG.5	49
8.7.8	Audit von FAU_STG.1	50
8.7.9	Audit von FAU_STG.2, FAU_STG.3	50
8.7.10	Audit von FAU_STG.4	50
8.7.11	Audit von FAU_STG.5	50
8.7.12	FAU_STG.1 Speicherort der Auditdaten	50
8.7.13	FAU_STG.2 Geschützte Speicherung der Auditdaten	50
8.7.14	FAU_STG.3 Garantien zur Auditdatenverfügbarkeit	51
8.7.15	FAU_STG.4 Aktion bei möglichem Auditdatenverlust	51
8.7.16	FAU_STG.5 Verhinderung von Auditdatenverlust	51
9	Klasse FCO: Kommunikation	52
9.1	Klassenbeschreibung	52
9.2	Nichtabstreitbarkeit des Ursprungs (FCO_NRO)	52
9.2.1	Familienverhalten	52
9.2.2	Komponentenebenen und Beschreibung	52
9.2.3	Management von FCO_NRO.1, FCO_NRO.2	53
9.2.4	Audit von FCO_NRO.1	53
9.2.5	Audit von FCO_NRO.2	53
9.2.6	FCO_NRO.1 Auswählbarer Ursprungsnachweis	53
9.2.7	FCO_NRO.2 Erzwungener Ursprungsnachweis	54
9.3	Nichtabstreitbarkeit des Empfangs (FCO_NRR)	54
9.3.1	Familienverhalten	54
9.3.2	Komponentenebenen und Beschreibung	54
9.3.3	Management von FCO_NRR.1, FCO_NRR.2	54
9.3.4	Audit von FCO_NRR.1	55
9.3.5	Audit von FCO_NRR.2	55
9.3.6	FCO_NRR.1 Auswählbarer Empfangsnachweis	55
9.3.7	FCO_NRR.2 Erzwungener Empfangsnachweis	55
10	Klasse FCS: Kryptographische Unterstützung	56
10.1	Klassenbeschreibung	56
10.2	Verwaltung kryptographischer Schlüssel (FCS_CKM)	57
10.2.1	Familienverhalten	57
10.2.2	Komponentenebenen und Beschreibung	57
10.2.3	Management von FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6	58
10.2.4	Audit von FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6	58
10.2.5	FCS_CKM.1 Generierung kryptographischer Schlüssel	58
10.2.6	FCS_CKM.2 Verteilung kryptographischer Schlüssel	59
10.2.7	FCS_CKM.3 Zugriff auf kryptographische Schlüssel	59
10.2.8	FCS_CKM.4 Zerstörung kryptographischer Schlüssel	59

10.2.9	FCS_CKM.5 Ableitung kryptographischer Schlüssel	60
10.2.10	FCS_CKM.6 Zeitablauf und Ereignis der Zerstörung kryptographischer Schlüssel	60
10.3	Kryptographische Operation (FCS_COP)	60
10.3.1	Familienverhalten	60
10.3.2	Komponentenebenen und Beschreibung	60
10.3.3	Management von FCS_COP.1	61
10.3.4	Audit von FCS_COP.1	61
10.3.5	FCS_COP.1 Kryptographische Operation	61
10.4	Generierung von Zufallsbits (FCS_RBG)	61
10.4.1	Familienverhalten	61
10.4.2	Komponentenebenen und Beschreibung	61
10.4.3	Management von FCS_RBG.1, FCS_RBG.2, FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6	62
10.4.4	Audit von FCS_RBG.1, FCS_RBG.2	62
10.4.5	Audit von FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6	62
10.4.6	FCS_RBG.1 Generierung von Zufallsbits (RBG)	63
10.4.7	FCS_RBG.2 Generierung von Zufallsbits (externes Seeding)	63
10.4.8	FCS_RBG.3 Generierung von Zufallsbits (internal seeding – single source)	63
10.4.9	FCS_RBG.4 Generierung von Zufallsbits (internes Seeding – mehrere Quellen)	64
10.4.10	FCS_RBG.5 Generierung von Zufallsbits (Kombination von Rauschquellen)	64
10.4.11	FCS_RBG.6 Dienst zur Generierung von Zufallsbits	64
10.5	Generierung von Zufallszahlen (FCS_RNG)	64
10.5.1	Familienverhalten	64
10.5.2	Komponentenebenen und Beschreibung	65
10.5.3	Management von FCS_RNG.1	65
10.5.4	Audit von FCS_RNG.1	65
10.5.5	FCS_RNG.1 Generierung von Zufallszahlen	65
11	Klasse FDP: Schutz von Benutzerdaten	65
11.1	Klassenbeschreibung	65
11.2	Zugriffskontrollpolitik (FDP_ACC)	67
11.2.1	Familienverhalten	67
11.2.2	Komponentenebenen und Beschreibung	68
11.2.3	Management von FDP_ACC.1, FDP_ACC.2	68
11.2.4	Audit von FDP_ACC.1, FDP_ACC.2	68
11.2.5	FDP_ACC.1 Zugriffskontrolle auf Teilmengen	68
11.2.6	FDP_ACC.2 Vollständige Zugriffskontrolle	68
11.3	Funktionen zur Zugriffskontrolle (FDP_ACF)	69
11.3.1	Familienverhalten	69
11.3.2	Komponentenebenen und Beschreibung	69
11.3.3	Management von FDP_ACF.1	69
11.3.4	Audit von FDP_ACF.1	69
11.3.5	FDP_ACF.1 Zugriffskontrolle auf Grundlage von Sicherheitsattributen	70
11.4	Datenauthentifizierung (FDP_DAU)	70
11.4.1	Familienverhalten	70
11.4.2	Komponentenebenen und Beschreibung	70
11.4.3	Management von FDP_DAU.1, FDP_DAU.2	71
11.4.4	Audit von FDP_DAU.1	71
11.4.5	Audit von FDP_DAU.2	71
11.4.6	FDP_DAU.1 Einfache Datenauthentifizierung	71
11.4.7	FDP_DAU.2 Datenauthentifizierung mit Identität des Garantiegebers	71
11.5	Export aus dem TOE (FDP_ETC)	72
11.5.1	Familienverhalten	72
11.5.2	Komponentenebenen und Beschreibung	72
11.5.3	Management von FDP_ETC.1	72
11.5.4	Management von FDP_ETC.2	72
11.5.5	Audit von FDP_ETC.1, FDP_ETC.2	72
11.5.6	FDP_ETC.1 Export von Benutzerdaten ohne Sicherheitsattribute	73
11.5.7	FDP_ETC.2 Export von Benutzerdaten mit Sicherheitsattributen	73

11.6	Informationsflusskontrollpolitik (FDP_IFC)	74
11.6.1	Familienverhalten	74
11.6.2	Komponentenebenen und Beschreibung	74
11.6.3	Management von FDP_IFC.1, FDP_IFC.2	74
11.6.4	Audit von FDP_IFC.1, FDP_IFC.2	74
11.6.5	FDP_IFC.1 Informationsflusskontrolle auf Teilmengen	75
11.6.6	FDP_IFC.2 Vollständige Informationsflusskontrolle	75
11.7	Funktionen zur Informationsflusskontrolle (FDP_IFF)	75
11.7.1	Familienverhalten	75
11.7.2	Komponentenebenen und Beschreibung	75
11.7.3	Management von FDP_IFF.1, FDP_IFF.2	76
11.7.4	Management von FDP_IFF.3, FDP_IFF.4, FDP_IFF.5	76
11.7.5	Management von FDP_IFF.6	76
11.7.6	Audit von FDP_IFF.1, FDP_IFF.2, FDP_IFF.5	77
11.7.7	Audit von FDP_IFF.3, FDP_IFF.4, FDP_IFF.6	77
11.7.8	FDP_IFF.1 Einfache Sicherheitsattribute	77
11.7.9	FDP_IFF.2 Hierarchische Sicherheitsattribute	78
11.7.10	FDP_IFF.3 Eingeschränkte unerlaubte Informationsflüsse	79
11.7.11	FDP_IFF.4 Teilweise Verhinderung von unerlaubten Informationsflüssen	79
11.7.12	FDP_IFF.5 Keine unerlaubten Informationsflüsse	79
11.7.13	FDP_IFF.6 Überwachung unerlaubter Informationsflüsse	80
11.8	Kontrolle der Informationsspeicherung (FDP_IRC)	80
11.8.1	Familienverhalten	80
11.8.2	Komponentenebenen und Beschreibung	81
11.8.3	Management von FDP_IRC.1	81
11.8.4	Audit von FDP_IRC.1	81
11.8.5	FDP_IRC.1 Kontrolle der Informationsaufbewahrung	81
11.9	Import von außerhalb des TOEs (FDP_ITC)	81
11.9.1	Familienverhalten	81
11.9.2	Komponentenebenen und Beschreibung	82
11.9.3	Management von FDP_ITC.1, FDP_ITC.2	82
11.9.4	Audit von FDP_ITC.1, FDP_ITC.2	82
11.9.5	FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute	82
11.9.6	FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen	83
11.10	Interne TOE-Übertragung (FDP_ITT)	83
11.10.1	Familienverhalten	83
11.10.2	Komponentenebenen und Beschreibung	83
11.10.3	Management von FDP_ITT.1, FDP_ITT.2	84
11.10.4	Management von FDP_ITT.3, FDP_ITT.4	84
11.10.5	Audit von FDP_ITT.1, FDP_ITT.2	84
11.10.6	Audit von FDP_ITT.3, FDP_ITT.4	84
11.10.7	FDP_ITT.1 Einfacher interner Übertragungsschutz	85
11.10.8	FDP_ITT.2 Trennung der Übertragung durch Attribut	85
11.10.9	FDP_ITT.3 Integritätsüberwachung	85
11.10.10	FDP_ITT.4 Attributbasierte Integritätsüberwachung	86
11.11	Restinformationsschutz (FDP_RIP)	86
11.11.1	Familienverhalten	86
11.11.2	Komponentenebenen und Beschreibung	86
11.11.3	Management von FDP_RIP.1, FDP_RIP.2	86
11.11.4	Audit von FDP_RIP.1, FDP_RIP.2	87
11.11.5	FDP_RIP.1 Restinformationsschutz auf Teilmengen	87
11.11.6	FDP_RIP.2 Vollständiger Restinformationsschutz	87
11.12	Zurücksetzen (FDP_ROL)	87
11.12.1	Familienverhalten	87
11.12.2	Komponentenebenen und Beschreibung	87
11.12.3	Management von FDP_ROL.1, FDP_ROL.2	88
11.12.4	Audit von FDP_ROL.1, FDP_ROL.2	88

11.12.5FDP_ROL.1 Einfaches Zurücksetzen	88
11.12.6FDP_ROL.2 Erweitertes Zurücksetzen	88
11.13 Vertraulichkeit gespeicherter Daten (FDP_SDC)	89
11.13.1Familienverhalten	89
11.13.2Komponentenebenen und Beschreibung	89
11.13.3Management von FDP_SDC.1, FDP_SDC.2	89
11.13.4Audit von FDP_SDC.1, FDP_SDC.2	89
11.13.5FDP_SDC.1 Vertraulichkeit gespeicherter Daten	89
11.13.6FDP_SDC.2 Vertraulichkeit gespeicherter Daten mit zugehöriger Methode	90
11.14 Integrität gespeicherter Daten (FDP_SDI)	90
11.14.1Familienverhalten	90
11.14.2Komponentenebenen und Beschreibung	90
11.14.3Management von FDP_SDI.1	90
11.14.4Management von FDP_SDI.2	90
11.14.5Audit von FDP_SDI.1	91
11.14.6Audit von FDP_SDI.2	91
11.14.7FDP_SDI.1 Überwachung der Integrität gespeicherter Daten	91
11.14.8FDP_SDI.2 Überwachung der Integrität gespeicherter Daten und Aktionen	91
11.15 Inter-TSF-Schutz der Vertraulichkeit von Benutzerdaten bei Übertragung (FDP_UCT)	92
11.15.1Familienverhalten	92
11.15.2Komponentenebenen und Beschreibung	92
11.15.3Management von FDP_UCT.1	92
11.15.4Audit von FDP_UCT.1	92
11.15.5FDP_UCT.1 Vertraulichkeit bei einfachem Datenaustausch	92
11.16 Inter-TSF-Schutz der Benutzerdatenintegrität bei Übertragung (FDP_UIT)	93
11.16.1Familienverhalten	93
11.16.2Komponentenebenen und Beschreibung	93
11.16.3Management von FDP_UIT.1, FDP_UIT.2, FDP_UIT.3	93
11.16.4Audit von FDP_UIT.1	93
11.16.5Audit von FDP_UIT.2, FDP_UIT.3	94
11.16.6FDP_UIT.1 Datenaustauschintegrität	94
11.16.7FDP_UIT.2 Wiederherstellung bei Quelldatenaustausch	94
11.16.8FDP_UIT.3 Wiederherstellung bei Zieldatenaustausch	95
12 Klasse FIA: Identifikation und Authentifizierung	95
12.1 Klassenbeschreibung	95
12.2 Authentifizierungsfehler (FIA_AFL)	96
12.2.1 Familienverhalten	96
12.2.2 Komponentenebenen und Beschreibung	96
12.2.3 Management von FIA_AFL.1	97
12.2.4 Audit von FIA_AFL.1	97
12.2.5 FIA_AFL.1 Handhabung von Authentifizierungsfehlern	97
12.3 Authentifizierungsnachweis der Identität (FIA_API)	97
12.3.1 Familienverhalten	97
12.3.2 Komponentenebenen und Beschreibung	97
12.3.3 Management von FIA_API.1	98
12.3.4 Audit von FIA_API.1	98
12.3.5 FIA_API.1 Authentifizierungsnachweis der Identität	98
12.4 Definition von Benutzerattributen (FIA_ATD)	98
12.4.1 Familienverhalten	98
12.4.2 Komponentenebenen und Beschreibung	98
12.4.3 Management von FIA_ATD.1	98
12.4.4 Audit von FIA_ATD.1	99
12.4.5 FIA_ATD.1 Definition von Benutzerattributen	99
12.5 Spezifikation von Sicherheitsinformationen (FIA_SOS)	99
12.5.1 Familienverhalten	99
12.5.2 Komponentenebenen und Beschreibung	99
12.5.3 Management von FIA_SOS.1	99

12.5.4	Management von FIA_SOS.2	99
12.5.5	Audit von FIA_SOS.1, FIA_SOS.2	100
12.5.6	FIA_SOS.1 Verifizierung von Sicherheitsinformationen	100
12.5.7	FIA_SOS.2 Generierung von Sicherheitsinformationen durch die TSF	100
12.6	Benutzerauthentifizierung (FIA_UAU)	100
12.6.1	Familienverhalten	100
12.6.2	Komponentenebenen und Beschreibung	100
12.6.3	Management von FIA_UAU.1	101
12.6.4	Management von FIA_UAU.2	101
12.6.5	Management von FIA_UAU.3, FIA_UAU.4, FIA_UAU.7	101
12.6.6	Management von FIA_UAU.5	102
12.6.7	Management von FIA_UAU.6	102
12.6.8	Management von FIA_UAU.7	102
12.6.9	Audit von FIA_UAU.1	102
12.6.10	Audit von FIA_UAU.2	102
12.6.11	Audit von FIA_UAU.3	102
12.6.12	Audit von FIA_UAU.4	102
12.6.13	Audit von FIA_UAU.5	103
12.6.14	Audit von FIA_UAU.6	103
12.6.15	Audit von FIA_UAU.7	103
12.6.16	FIA_UAU.1 Zeitpunkt der Authentifizierung	103
12.6.17	FIA_UAU.2 Benutzerauthentifizierung vor irgendeiner anderen Aktion	103
12.6.18	FIA_UAU.3 Fälschungssichere Authentifizierung	104
12.6.19	FIA_UAU.4 Einmaliger Authentifizierungsmechanismus	104
12.6.20	FIA_UAU.5 Mehrfachauthentifizierungsmechanismen	104
12.6.21	FIA_UAU.6 Erneute Authentifizierung	104
12.6.22	FIA_UAU.7 Geschützte Authentifizierungsrückmeldung	105
12.7	Benutzeridentifizierung (FIA_UID)	105
12.7.1	Familienverhalten	105
12.7.2	Komponentenebenen und Beschreibung	105
12.7.3	Management von FIA_UID.1	105
12.7.4	Management von FIA_UID.2	105
12.7.5	Audit von FIA_UID.1, FIA_UID.2	106
12.7.6	FIA_UID.1 Zeitpunkt der Identifizierung	106
12.7.7	FIA_UID.2 Benutzeridentifizierung vor irgendeiner anderen Aktion	106
12.8	Benutzer-Subjekt-Bindung (FIA_USB)	106
12.8.1	Familienverhalten	106
12.8.2	Komponentenebenen und Beschreibung	106
12.8.3	Management von FIA_USB.1	107
12.8.4	Audit von FIA_USB.1	107
12.8.5	FIA_USB.1 Benutzer-Subjekt-Bindung	107
13	Klasse FMT: Sicherheitsmanagement	107
13.1	Klassenbeschreibung	107
13.2	Eingeschränkte Fähigkeiten und Verfügbarkeit (FMT_LIM)	108
13.2.1	Familienverhalten	108
13.2.2	Komponentenebenen und Beschreibung	109
13.2.3	Management von FMT_LIM.1, FMT_LIM.2	109
13.2.4	Audit von FMT_LIM.1	109
13.2.5	FMT_LIM.1 Eingeschränkte Fähigkeiten	109
13.2.6	FMT_LIM.2 Eingeschränkte Verfügbarkeit	109
13.3	Management von Funktionen in der TSF (FMT_MOF)	110
13.3.1	Familienverhalten	110
13.3.2	Komponentenebenen und Beschreibung	110
13.3.3	Management von FMT_MOF.1	110
13.3.4	Audit von FMT_MOF.1	110
13.3.5	FMT_MOF.1 Management des Verhaltens der Sicherheitsfunktionen	110
13.4	Management von Sicherheitsattributen (FMT_MSA)	110

13.4.1 Familienverhalten	110
13.4.2 Komponentenebenen und Beschreibung	110
13.4.3 Management von FMT_MSA.1	111
13.4.4 Management von FMT_MSA.2	111
13.4.5 Management von FMT_MSA.3	111
13.4.6 Management von FMT_MSA.4	111
13.4.7 Audit von FMT_MSA.1	111
13.4.8 Audit von FMT_MSA.2	112
13.4.9 Audit von FMT_MSA.3	112
13.4.10 Audit von FMT_MSA.4	112
13.4.11 FMT_MSA.1 Management von Sicherheitsattributen	112
13.4.12 FMT_MSA.2 Sichere Sicherheitsattribute	112
13.4.13 FMT_MSA.3 Statische Attributinitialisierung	113
13.4.14 FMT_MSA.4 Vererbung von Sicherheitsattributwerten	113
13.5 Management von TSF-Daten (FMT_MTD)	113
13.5.1 Familienverhalten	113
13.5.2 Komponentenebenen und Beschreibung	113
13.5.3 Management von FMT_MTD.1	114
13.5.4 Management von FMT_MTD.2	114
13.5.5 Management von FMT_MTD.3	114
13.5.6 Audit von FMT_MTD.1	114
13.5.7 Audit von FMT_MTD.2	114
13.5.8 Audit von FMT_MTD.3	114
13.5.9 FMT_MTD.1 Management von TSF-Daten	115
13.5.10 FMT_MTD.2 Management von Grenzen auf TSF-Daten	115
13.5.11 FMT_MTD.3 Sichere TSF-Daten	115
13.6 Widerruf (FMT_REV)	115
13.6.1 Familienverhalten	115
13.6.2 Komponentenebenen und Beschreibung	115
13.6.3 Management von FMT_REV.1	116
13.6.4 Audit von FMT_REV.1	116
13.6.5 FMT_REV.1 Widerruf	116
13.7 Ablauf von Sicherheitsattributen (FMT_SAE)	116
13.7.1 Familienverhalten	116
13.7.2 Komponentenebenen und Beschreibung	116
13.7.3 Management von FMT_SAE.1	117
13.7.4 Audit von FMT_SAE.1	117
13.7.5 FMT_SAE.1 Befristete Autorisierung	117
13.8 Spezifizierung von Managementfunktionen (FMT_SMF)	117
13.8.1 Familienverhalten	117
13.8.2 Komponentenebenen und Beschreibung	118
13.8.3 Management von FMT_SMF.1	118
13.8.4 Audit von FMT_SMF.1	118
13.8.5 FMT_SMF.1 Spezifizierung von Managementfunktionen	118
13.9 Sicherheitsmanagementrollen (FMT_SMR)	118
13.9.1 Familienverhalten	118
13.9.2 Komponentenebenen und Beschreibung	118
13.9.3 Management von FMT_SMR.1	119
13.9.4 Management von FMT_SMR.2	119
13.9.5 Management von FMT_SMR.3	119
13.9.6 Audit von FMT_SMR.1	119
13.9.7 Audit von FMT_SMR.2	119
13.9.8 Audit von FMT_SMR.3	120
13.9.9 FMT_SMR.1 Sicherheitsrollen	120
13.9.10 FMT_SMR.2 Einschränkungen zu Sicherheitsrollen	120
13.9.11 FMT_SMR.3 Übernahme von Rollen	120
14 Klasse FPR: Privatsphäre	121

14.1	Klassenbeschreibung	121
14.2	Anonymität (FPR_ANO)	121
14.2.1	Familienverhalten	121
14.2.2	Komponentenebenen und Beschreibung	121
14.2.3	Management von FPR_ANO.1, FPR_ANO.2	122
14.2.4	Audit von FPR_ANO.1, FPR_ANO.2	122
14.2.5	FPR_ANO.1 Anonymität	122
14.2.6	FPR_ANO.2 Anonymität ohne Anforderung von Informationen	122
14.3	Pseudonymität (FPR_PSE)	122
14.3.1	Familienverhalten	122
14.3.2	Komponentenebenen und Beschreibung	122
14.3.3	Management von FPR_PSE.1, FPR_PSE.2, FPR_PSE.3	123
14.3.4	Audit von FPR_PSE.1, FPR_PSE.2, FPR_PSE.3	123
14.3.5	FPR_PSE.1 Pseudonymität	123
14.3.6	FPR_PSE.2 Umkehrbare Pseudonymität	124
14.3.7	FPR_PSE.3 Alias-Pseudonymität	124
14.4	Unverknüpfbarkeit (FPR_UNL)	125
14.4.1	Familienverhalten	125
14.4.2	Komponentenebenen und Beschreibung	125
14.4.3	Management von FPR_UNL.1	125
14.4.4	Audit von FPR_UNL.1	125
14.4.5	FPR_UNL.1 Unverknüpfbarkeit von Operationen	125
14.5	Unbeobachtbarkeit (FPR_UNO)	126
14.5.1	Familienverhalten	126
14.5.2	Komponentenebenen und Beschreibung	126
14.5.3	Management von FPR_UNO.1, FPR_UNO.2	126
14.5.4	Management von FPR_UNO.3	126
14.5.5	Management von FPR_UNO.4	126
14.5.6	Audit von FPR_UNO.1, FPR_UNO.2	126
14.5.7	Audit von FPR_UNO.3	127
14.5.8	Audit von FPR_UNO.4	127
14.5.9	FPR_UNO.1 Unbeobachtbarkeit	127
14.5.10	FPR_UNO.2 Zuweisung von Informationen mit Einfluss auf Unbeobachtbarkeit	127
14.5.11	FPR_UNO.3 Unbeobachtbarkeit ohne Anforderung von Informationen	127
14.5.12	FPR_UNO.4 Autorisierte Benutzerbeobachtbarkeit	128
15	Klasse FPT: Schutz der TSF	128
15.1	Klassenbeschreibung	128
15.2	TOE-Emanation (FPT_EMS)	129
15.2.1	Familienverhalten	129
15.2.2	Komponentenebenen und Beschreibung	130
15.2.3	Management von FPT_EMS.1	130
15.2.4	Audit von FPT_EMS.1	130
15.2.5	FPT_EMS.1 Emanation der TSF und der Benutzerdaten	130
15.3	Sicherheit bei Ausfall (FPT_FLS)	131
15.3.1	Familienverhalten	131
15.3.2	Komponentenebenen und Beschreibung	131
15.3.3	Management von FPT_FLS.1	131
15.3.4	Audit von FPT_FLS.1	131
15.3.5	FPT_FLS.1 Ausfall mit Beibehaltung des sicheren Zustands	131
15.4	TSF-Initialisierung (FPT_INI)	131
15.4.1	Familienverhalten	131
15.4.2	Komponentenebenen und Beschreibung	131
15.4.3	Management von FPT_INI.1	132
15.4.4	Audit von FPT_INI.1	132
15.4.5	FPT_INI.1 TSF-Initialisierung	132
15.5	Verfügbarkeit von exportierten TSF-Daten (FPT_ITA)	133
15.5.1	Familienverhalten	133

15.5.2	Komponentenebenen und Beschreibung	133
15.5.3	Management von FPT_ITA.1	133
15.5.4	Audit von FPT_ITA.1	133
15.5.5	FPT_ITA.1 Inter-TSF-Verfügbarkeit innerhalb einer definierten Verfügbarkeitsmetrik	133
15.6	Vertraulichkeit der exportierten TSF-Daten (FPT_ITC)	134
15.6.1	Familienverhalten	134
15.6.2	Komponentenebenen und Beschreibung	134
15.6.3	Management von FPT_ITC.1	134
15.6.4	Audit von FPT_ITC.1	134
15.6.5	FPT_ITC.1 Inter-TSF-Vertraulichkeit während der Übertragung	134
15.7	Integrität exportierter TSF-Daten (FPT_ITI)	134
15.7.1	Familienverhalten	134
15.7.2	Komponentenebenen und Beschreibung	134
15.7.3	Management von FPT_ITI.1	135
15.7.4	Management von FPT_ITI.2	135
15.7.5	Audit von FPT_ITI.1	135
15.7.6	Audit von FPT_ITI.2	135
15.7.7	FPT_ITI.1 Inter-TSF-Erkennung von Änderungen	135
15.7.8	FPT_ITI.2 Inter-TSF-Erkennung und Korrektur von Änderungen	136
15.8	Interne TOE-TSF-Datenübertragung (FPT_ITT)	136
15.8.1	Familienverhalten	136
15.8.2	Komponentenebenen und Beschreibung	136
15.8.3	Management von FPT_ITT.1	137
15.8.4	Management von FPT_ITT.2	137
15.8.5	Management von FPT_ITT.3	137
15.8.6	Audit von FPT_ITT.1, FPT_ITT.2	137
15.8.7	Audit von FPT_ITT.3	137
15.8.8	FPT_ITT.1 Einfacher Schutz der TSF-Daten bei interner Übertragung	138
15.8.9	FPT_ITT.2 Trennung des TSF-Datentransfers	138
15.8.10	FPT_ITT.3 Überwachung der Integrität von TSF-Daten	138
15.9	Physischer Schutz der TSF (FPT_PHP)	138
15.9.1	Familienverhalten	138
15.9.2	Komponentenebenen und Beschreibung	139
15.9.3	Management von FPT_PHP.1	139
15.9.4	Management von FPT_PHP.2	139
15.9.5	Management von FPT_PHP.3	139
15.9.6	Audit von FPT_PHP.1	139
15.9.7	Audit von FPT_PHP.2	140
15.9.8	Audit von FPT_PHP.3	140
15.9.9	FPT_PHP.1 Passive Erkennung von physischen Angriffen	140
15.9.10	FPT_PHP.2 Mitteilung von physischen Angriffen	140
15.9.11	FPT_PHP.3 Widerstand gegen physische Angriffe	141
15.10	Vertrauenswürdige Wiederherstellung (FPT_RCV)	141
15.10.1	Familienverhalten	141
15.10.2	Komponentenebenen und Beschreibung	141
15.10.3	Management von FPT_RCV.1	141
15.10.4	Management von FPT_RCV.2, FPT_RCV.3	141
15.10.5	Management von FPT_RCV.4	142
15.10.6	Audit von FPT_RCV.1, FPT_RCV.2, FPT_RCV.3	142
15.10.7	Audit von FPT_RCV.4	142
15.10.8	FPT_RCV.1 Manuelle Wiederherstellung	142
15.10.9	FPT_RCV.2 Automatische Wiederherstellung	142
15.10.10	FPT_RCV.3 Automatische Wiederherstellung ohne übermäßigen Verlust	143
15.10.11	FPT_RCV.4 Funktionswiederherstellung	143
15.11	Erkennung von Wiederverwendung (FPT_RPL)	143
15.11.1	Familienverhalten	143
15.11.2	Komponentenebenen und Beschreibung	144

15.11.3	Management von FPT_RPL.1	144
15.11.4	Audit von FPT_RPL.1	144
15.11.5	FPT_RPL.1 Erkennung von Wiederverwendung	144
15.12	Zustandssynchronitätsprotokoll (FPT_SSP)	144
15.12.1	Familienverhalten	144
15.12.2	Komponentenebenen und Beschreibung	145
15.12.3	Management von FPT_SSP.1, FPT_SSP.2	145
15.12.4	Audit von FPT_SSP.1, FPT_SSP.2	145
15.12.5	FPT_SSP.1 Einfache vertrauenswürdige Bestätigung	145
15.12.6	FPT_SSP.2 Gegenseitige vertrauenswürdige Bestätigung	145
15.13	Zeitstempel (FPT_STM)	146
15.13.1	Familienverhalten	146
15.13.2	Komponentenebenen und Beschreibung	146
15.13.3	Management von FPT_STM.1	146
15.13.4	Management von FPT_STM.2	146
15.13.5	Audit von FPT_STM.1	146
15.13.6	Audit von FPT_STM.2	146
15.13.7	FPT_STM.1 Verlässliche Zeitstempel	147
15.13.8	FPT_STM.2 Zeitquelle	147
15.14	Inter-TSF-TSF-Datenkonsistenz (FPT_TDC)	147
15.14.1	Familienverhalten	147
15.14.2	Komponentenebenen und Beschreibung	147
15.14.3	Management von FPT_TDC.1	147
15.14.4	Audit von FPT_TDC.1	147
15.14.5	FPT_TDC.1 Einfache Inter-TSF-TSF-Datenkonsistenz	148
15.15	Prüfen von externen Entitäten (FPT_TEE)	148
15.15.1	Familienverhalten	148
15.15.2	Komponentenebenen und Beschreibung	148
15.15.3	Management von FPT_TEE.1	148
15.15.4	Audit von FPT_TEE.1	149
15.15.5	FPT_TEE.1 Prüfen von externen Entitäten	149
15.16	Interne TOE-TSF-Datenreplizierungskonsistenz (FPT_TRC)	149
15.16.1	Familienverhalten	149
15.16.2	Komponentenebenen und Beschreibung	149
15.16.3	Management von FPT_TRC.1	149
15.16.4	Audit von FPT_TRC.1	150
15.16.5	FPT_TRC.1 Interne TSF-Konsistenz	150
15.17	TSF-Selbstprüfung (FPT_TST)	150
15.17.1	Familienverhalten	150
15.17.2	Komponentenebenen und Beschreibung	150
15.17.3	Management von FPT_TST.1	151
15.17.4	Audit von FPT_TST.1	151
15.17.5	FPT_TST.1 TSF-Selbstprüfung	151
16	Klasse FRU: Verwendung von Ressourcen	151
16.1	Klassenbeschreibung	151
16.2	Fehlertoleranz (FRU_FLT)	152
16.2.1	Familienverhalten	152
16.2.2	Komponentenebenen und Beschreibung	152
16.2.3	Management von FRU_FLT.1, FRU_FLT.2	152
16.2.4	Audit von FRU_FLT.1	152
16.2.5	Audit von FRU_FLT.2	153
16.2.6	FRU_FLT.1 Verminderte Fehlertoleranz	153
16.2.7	FRU_FLT.2 Begrenzte Fehlertoleranz	153
16.3	Priorität von Diensten (FRU_PRS)	153
16.3.1	Familienverhalten	153
16.3.2	Komponentenebenen und Beschreibung	153
16.3.3	Management von FRU_PRS.1, FRU_PRS.2	154

16.3.4	Audit von FRU_PRS.1, FRU_PRS.2	154
16.3.5	FRU_PRS.1 Begrenzte Priorität von Diensten	154
16.3.6	FRU_PRS.2 Vollständige Priorität von Diensten	154
16.4	Ressourcenzuweisung (FRU_RSA)	154
16.4.1	Familienverhalten	154
16.4.2	Komponentenebenen und Beschreibung	155
16.4.3	Management von FRU_RSA.1	155
16.4.4	Management von FRU_RSA.2	155
16.4.5	Audit von FRU_RSA.1, FRU_RSA.2	155
16.4.6	FRU_RSA.1 Höchstquoten	155
16.4.7	FRU_RSA.2 Mindestquoten und Höchstquoten	156
17	Klasse FTA: TOE-Zugriff	156
17.1	Klassenbeschreibung	156
17.2	Einschränkung des Umfangs auswählbarer Attribute (FTA_LSA)	157
17.2.1	Familienverhalten	157
17.2.2	Komponentenebenen und Beschreibung	157
17.2.3	Management von FTA_LSA.1	157
17.2.4	Audit von FTA_LSA.1	157
17.2.5	FTA_LSA.1 Einschränkung des Umfangs auswählbarer Attribute	158
17.3	Einschränkung von mehreren gleichzeitigen Sitzungen (FTA_MCS)	158
17.3.1	Familienverhalten	158
17.3.2	Komponentenebenen und Beschreibung	158
17.3.3	Management von FTA_MCS.1	158
17.3.4	Management von FTA_MCS.2	158
17.3.5	Audit von FTA_MCS.1, FTA_MCS.2	159
17.3.6	FTA_MCS.1 Einfache Einschränkung von mehreren gleichzeitigen Sitzungen	159
17.3.7	FTA_MCS.2 Einschränkung von mehreren gleichzeitigen Sitzungen je Benutzerattribut	159
17.4	Sperren und Beenden von Sitzungen (FTA_SSL)	159
17.4.1	Familienverhalten	159
17.4.2	Komponentenebenen und Beschreibung	159
17.4.3	Management von FTA_SSL.1	160
17.4.4	Management von FTA_SSL.2	160
17.4.5	Management von FTA_SSL.3	160
17.4.6	Management von FTA_SSL.4	160
17.4.7	Audit von FTA_SSL.1, FTA_SSL.2	160
17.4.8	Audit von FTA_SSL.3	161
17.4.9	Audit von FTA_SSL.4	161
17.4.10	FTA_SSL.1 Durch die TSF ausgelöstes Sperren der Sitzung	161
17.4.11	FTA_SSL.2 Durch den Benutzer ausgelöstes Sperren	161
17.4.12	FTA_SSL.3 Durch die TSF ausgelöstes Beenden	162
17.4.13	FTA_SSL.4 Durch den Benutzer ausgelöstes Beenden	162
17.5	TOE-Zugriffsbanner (FTA_TAB)	162
17.5.1	Familienverhalten	162
17.5.2	Komponentenebenen und Beschreibung	162
17.5.3	Management von FTA_TAB.1	162
17.5.4	Audit von FTA_TAB.1	163
17.5.5	FTA_TAB.1 Standard-TOE-Zugriffsbanner	163
17.6	TOE-Zugriffsverlauf (FTA_TAH)	163
17.6.1	Familienverhalten	163
17.6.2	Komponentenebenen und Beschreibung	163
17.6.3	Management von FTA_TAH.1	163
17.6.4	Audit von FTA_TAH.1	163
17.6.5	FTA_TAH.1 TOE-Zugriffsverlauf	163
17.7	TOE-Sitzungsaufbau (FTA_TSE)	164
17.7.1	Familienverhalten	164
17.7.2	Komponentenebenen und Beschreibung	164
17.7.3	Management von FTA_TSE.1	164

17.7.4	Audit von FTA_TSE.1	164
17.7.5	FTA_TSE.1 TOE-Sitzungsaufbau	165
18	Klasse FTP: Vertrauenswürdiger Pfad/vertrauenswürdige Kanäle	165
18.1	Klassenbeschreibung	165
18.2	Vertrauenswürdiger Kanal Inter-TSF (FTP_ITC)	166
18.2.1	Familienverhalten	166
18.2.2	Komponentenebenen und Beschreibung	166
18.2.3	Management von FTP_ITC.1	166
18.2.4	Audit von FTP_ITC.1	166
18.2.5	FTP_ITC.1 Vertrauenswürdiger Kanal Inter-TSF	167
18.3	Vertrauenswürdiger Kanalprotokoll (FTP_PRO)	167
18.3.1	Familienverhalten	167
18.3.2	Komponentenebenen und Beschreibung	167
18.3.3	Management von FTP_PRO.1	167
18.3.4	Management von FTP_PRO.2	168
18.3.5	Management von FTP_PRO.3	168
18.3.6	Audit von FTP_PRO.1	168
18.3.7	Audit von FTP_PRO.2	168
18.3.8	Audit von FTP_PRO.3	168
18.3.9	FTP_PRO.1 Protokoll des vertrauenswürdigen Kanals	169
18.3.10	FTP_PRO.2 Einrichtung des vertrauenswürdigen Kanals	169
18.3.11	FTP_PRO.3 Datenschutz für den vertrauenswürdigen Kanal	170
18.4	Vertrauenswürdiger Pfad (FTP_TRP)	170
18.4.1	Familienverhalten	170
18.4.2	Komponentenebenen und Beschreibung	170
18.4.3	Management von FTP_TRP.1	171
18.4.4	Audit von FTP_TRP.1	171
18.4.5	FTP_TRP.1 Vertrauenswürdiger Pfad	171
Anhang A (informativ) Struktur der Sicherheitsfunktionsanforderungen (SFR) in den Anwendungshinweisen		172
A.1	Allgemeines	172
A.2	Aufbau der Hinweise	172
A.2.1	Allgemeines	172
A.2.2	Klassenstruktur	172
A.2.3	Familienstruktur	173
A.2.4	Komponentenstruktur	174
Anhang B (informativ) Abhängigkeitstabellen für Sicherheitsfunktionskomponenten		175
B.1	Abhängigkeitstabellen	175
Anhang C (normativ) Klasse FAU: Sicherheitsaudit — Anwendungshinweise		185
C.1	Allgemeines	185
C.1.1	Allgemeine Informationen zu Auditanforderungen	185
C.1.2	Auditanforderungen in einer verteilten Umgebung	185
C.2	Automatische Antwort beim Sicherheitsaudit (FAU_ARP)	186
C.2.1	Anwendungshinweise für Benutzer	186
C.2.2	FAU_ARP.1 Sicherheitsalarme	186
C.3	Datengenerierung beim Sicherheitsaudit (FAU_GEN)	186
C.3.1	Allgemeines	186
C.3.2	FAU_GEN.1 Generierung von Auditdaten	188
C.3.3	FAU_GEN.2 Verknüpfung der Benutzeridentität	189
C.4	Sicherheitsauditanalyse (FAU_SAA)	189
C.4.1	Anwendungshinweise für Benutzer	189
C.4.2	„FAU_SAA.1 Potential violation analysis“	189
C.4.3	FAU_SAA.2 Profilbasierte Erkennung von Anomalien	190
C.4.4	FAU_SAA.3 Einfache Angriffsheuristiken	191
C.4.5	FAU_SAA.4 Komplexe Angriffsheuristiken	192
C.5	Sicherheitsauditüberprüfung (FAU_SAR)	193
C.5.1	Anwendungshinweise für Benutzer	193

C.5.2	FAU_SAR.1 Auditüberprüfung	194
C.5.3	FAU_SAR.2 Beschränkte Auditüberprüfung	194
C.5.4	FAU_SAR.3 Auswählbare Auditüberprüfung	194
C.6	Sicherheitsaudit Ereignisauswahl (FAU_SEL)	195
C.6.1	Anwendungshinweise für Benutzer	195
C.6.2	FAU_SEL.1 Auswählbares Audit	195
C.7	Sicherheitsaudit Datenspeicherung (FAU_STG)	196
C.7.1	Anwendungshinweise für Benutzer	196
C.7.2	FAU_STG.1 Speicherort der Auditdaten	196
C.7.3	FAU_STG.2 Geschützte Speicherung der Auditdaten	196
C.7.4	FAU_STG.3 Garantien zur Auditdatenverfügbarkeit	197
C.7.5	FAU_STG.4 Verhinderung von Auditdatenverlust	197
C.7.6	FAU_STG.5 Aktionen bei möglichem Auditdatenverlust	198
Anhang D (normativ) Klasse FCO: Kommunikation — Anwendungshinweise		199
D.1	Allgemeines	199
D.2	Nichtabstreitbarkeit des Ursprungs (FCO_NRO)	199
D.2.1	Anwendungshinweise für Benutzer	199
D.2.2	FCO_NRO.1 Auswählbarer Ursprungsnachweis	200
D.2.3	FCO_NRO.2 Erzwungener Ursprungsnachweis	201
D.3	Nichtabstreitbarkeit des Empfangs (FCO_NRR)	201
D.3.1	Anwendungshinweise für Benutzer	201
D.3.2	FCO_NRR.1 Auswählbarer Empfangsnachweis	202
D.3.3	FCO_NRR.2 Erzwungener Empfangsnachweis	203
Anhang E (normativ) Klasse FCS: Kryptographische Unterstützung — Anwendungshinweise		204
E.1	Allgemeines	204
E.2	Verwaltung kryptographischer Schlüssel (FCS_CKM)	205
E.2.1	Anwendungshinweise für Benutzer	205
E.2.2	Hinweise für Evaluatoren	206
E.2.3	FCS_CKM.1 Generierung kryptographischer Schlüssel	206
E.2.4	FCS_CKM.2 Verteilung kryptographischer Schlüssel	207
E.2.5	FCS_CKM.3 Zugriff auf kryptographische Schlüssel	207
E.2.6	FCS_CKM.5 Ableitung kryptographischer Schlüssel	208
E.2.7	FCS_CKM.6 Zeitablauf und Ereignis der Zerstörung kryptographischer Schlüssel	208
E.3	Kryptographische Operation (FCS_COP)	209
E.3.1	Anwendungshinweise für Benutzer	209
E.3.2	FCS_COP.1 Kryptographische Operation	209
E.4	Generierung von Zufallsbits (FCS_RBG)	210
E.4.1	Anwendungshinweise für Benutzer	210
E.4.2	FCS_RBG.1 Generierung von Zufallsbits (RBG)	210
E.4.3	FCS_RBG.2 Generierung von Zufallsbits (externes Seeding)	211
E.4.4	FCS_RBG.3 Generierung von Zufallsbits (internal seeding — single source)	211
E.4.5	FCS_RBG.4 Generierung von Zufallsbits (internes Seeding — mehrere Quellen)	212
E.4.6	FCS_RBG.6 Dienst zur Generierung von Zufallsbits	212
E.5	Generierung von Zufallszahlen (FCS_RNG)	212
E.5.1	Anwendungshinweise für Benutzer	212
E.5.2	FCS_RNG.1 Generierung von Zufallszahlen	212
Anhang F (normativ) Klasse FDP: Schutz von Benutzerdaten — Anwendungshinweise		215
F.1	Allgemeines	215
F.2	Zugriffskontrollpolitik (FDP_ACC)	217
F.2.1	Anwendungshinweise für Benutzer	217
F.2.2	FDP_ACC.1 Zugriffskontrolle auf Teilmengen	218
F.2.3	FDP_ACC.2 Vollständige Zugriffskontrolle	218
F.3	Funktionen zur Zugriffskontrolle (FDP_ACF)	219
F.3.1	Anwendungshinweise für Benutzer	219
F.3.2	FDP_ACF.1 Zugriffskontrolle auf Grundlage von Sicherheitsattributen	219
F.4	Datenauthentifizierung (FDP_DAU)	221
F.4.1	Anwendungshinweise für Benutzer	221

F.4.2	FDP_DAU.1 Einfache Datenauthentifizierung	221
F.4.3	FDP_DAU.2 Datenauthentifizierung mit Identität des Garantiegebers	221
F.5	Export aus dem TOE (FDP_ETC)	222
F.5.1	Anwendungshinweise für Benutzer	222
F.5.2	FDP_ETC.1 Export von Benutzerdaten ohne Sicherheitsattribute	222
F.5.3	FDP_ETC.2 Export von Benutzerdaten mit Sicherheitsattributen	223
F.6	Informationsflusskontrollpolitik (FDP_IFC)	223
F.6.1	Anwendungshinweise für Benutzer	223
F.6.2	FDP_IFC.1 Informationsflusskontrolle auf Teilmengen	224
F.6.3	FDP_IFC.2 Vollständige Informationsflusskontrolle	225
F.7	Funktionen zur Informationsflusskontrolle (FDP_IFF)	225
F.7.1	Anwendungshinweise für Benutzer	225
F.7.2	FDP_IFF.1 Einfache Sicherheitsattribute	226
F.7.3	FDP_IFF.2 Hierarchische Sicherheitsattribute	227
F.7.4	FDP_IFF.3 Eingeschränkte unerlaubte Informationsflüsse	228
F.7.5	FDP_IFF.4 Teilweise Verhinderung von unerlaubten Informationsflüssen	229
F.7.6	FDP_IFF.5 Keine unerlaubten Informationsflüsse	229
F.7.7	FDP_IFF.6 Überwachung unerlaubter Informationsflüsse	230
F.8	Kontrolle der Informationsaufbewahrung (FDP_IRC)	230
F.8.1	Anwendungshinweise für Benutzer	230
F.8.2	FDP_IRC.1 Kontrolle der Informationsaufbewahrung	230
F.9	Import von außerhalb des TOEs (FDP_ITC)	231
F.9.1	Anwendungshinweise für Benutzer	231
F.9.2	FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute	232
F.9.3	FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen	232
F.10	Interne TOE-Übertragung (FDP_ITT)	233
F.10.1	Anwendungshinweise für Benutzer	233
F.10.2	FDP_ITT.1 Einfacher interner Übertragungsschutz	233
F.10.3	FDP_ITT.2 Trennung der Übertragung durch Attribut	234
F.10.4	FDP_ITT.3 Integritätsüberwachung	234
F.10.5	FDP_ITT.4 Attributbasierte Integritätsüberwachung	235
F.11	Restinformationsschutz (FDP_RIP)	236
F.11.1	Anwendungshinweise für Benutzer	236
F.11.2	FDP_RIP.1 Restinformationsschutz auf Teilmengen	237
F.11.3	FDP_RIP.2 Vollständiger Restinformationsschutz	237
F.12	Zurücksetzen (FDP_ROL)	237
F.12.1	Anwendungshinweise für Benutzer	237
F.12.2	FDP_ROL.1 Einfaches Zurücksetzen	238
F.12.3	FDP_ROL.2 Erweitertes Zurücksetzen	238
F.13	Vertraulichkeit gespeicherter Daten (FDP_SDC)	239
F.13.1	Anwendungshinweise für Benutzer	239
F.13.2	Hinweise für Evaluatoren	239
F.13.3	FDP_SDC.1 Vertraulichkeit gespeicherter Daten	239
F.13.4	FDP_SDC.2 Vertraulichkeit gespeicherter Daten mit zugehöriger Methode	239
F.14	Integrität gespeicherter Daten (FDP_SDI)	240
F.14.1	Anwendungshinweise für Benutzer	240
F.14.2	FDP_SDI.1 Überwachung der Integrität gespeicherter Daten	240
F.14.3	FDP_SDI.2 Überwachung der Integrität gespeicherter Daten und Aktionen	240
F.15	Inter-TSF-Schutz der Vertraulichkeit von Benutzerdaten bei Übertragung (FDP_UCT)	241
F.15.1	Anwendungshinweise für Benutzer	241
F.15.2	FDP_UCT.1 Vertraulichkeit bei einfachem Datenaustausch	241
F.16	Inter-TSF-Schutz der Benutzerdatenintegrität bei Übertragung (FDP_UIT)	241
F.16.1	Anwendungshinweise für Benutzer	241
F.16.2	FDP_UIT.1 Datenaustauschintegrität	241
F.16.3	FDP_UIT.2 Wiederherstellung bei Quelldatenaustausch	242
F.16.4	FDP_UIT.3 Wiederherstellung bei Zieldatenaustausch	242
Anhang G (normativ) Klasse FIA: Identifikation und Authentifizierung — Anwendungshinweise		244

G.1	Allgemeines	244
G.2	Authentifizierungsfehler (FIA_AFL)	244
G.2.1	Anwendungshinweise für Benutzer	244
G.2.2	FIA_AFL.1 Handhabung von Authentifizierungsfehlern	245
G.3	Authentifizierungsnachweis der Identität (FIA_API)	246
G.3.1	Anwendungshinweise für Benutzer	246
G.3.2	FIA_API.1 Authentifizierungsnachweis der Identität	246
G.4	Definition von Benutzerattributen (FIA_ATD)	247
G.4.1	Anwendungshinweise für Benutzer	247
G.4.2	FIA_ATD.1 Definition von Benutzerattributen	247
G.5	Spezifikation von Sicherheitsinformationen (FIA_SOS)	247
G.5.1	Anwendungshinweise für Benutzer	247
G.5.2	FIA_SOS.1 Verifizierung von Sicherheitsinformationen	248
G.5.3	FIA_SOS.2 Generierung von Sicherheitsinformationen durch die TSF	248
G.6	Benutzerauthentifizierung (FIA_UAU)	249
G.6.1	Anwendungshinweise für Benutzer	249
G.6.2	FIA_UAU.1 Zeitpunkt der Authentifizierung	249
G.6.3	FIA_UAU.2 Benutzerauthentifizierung vor irgendeiner anderen Aktion	249
G.6.4	FIA_UAU.3 Fälschungssichere Authentifizierung	249
G.6.5	FIA_UAU.4 Einmaliger Authentifizierungsmechanismus	250
G.6.6	FIA_UAU.5 Mehrfachauthentifizierungsmechanismen	250
G.6.7	FIA_UAU.6 Erneute Authentifizierung	251
G.6.8	FIA_UAU.7 Geschützte Authentifizierungsrückmeldung	251
G.7	Benutzeridentifizierung (FIA_UID)	252
G.7.1	Anwendungshinweise für Benutzer	252
G.7.2	FIA_UID.1 Zeitpunkt der Identifizierung	252
G.7.3	FIA_UID.2 Benutzeridentifizierung vor irgendeiner anderen Aktion	252
G.8	Benutzer-Subjekt-Bindung (FIA_USB)	252
G.8.1	Anwendungshinweise für Benutzer	252
G.8.2	FIA_USB.1 Benutzer-Subjekt-Bindung	252
Anhang H	(normativ) Klasse FMT: Sicherheitsmanagement — Anwendungshinweise	254
H.1	Allgemeines	254
H.2	Eingeschränkte Fähigkeiten und Verfügbarkeit (FMT_LIM)	254
H.2.1	Anwendungshinweise für Benutzer	254
H.2.2	FMT_LIM.1 Eingeschränkte Fähigkeiten	254
H.2.3	FMT_LIM.2 Eingeschränkte Verfügbarkeit	255
H.3	Management von Funktionen in der TSF (FMT_MOF)	255
H.3.1	Anwendungshinweise für Benutzer	255
H.3.2	FMT_MOF.1 Management des Verhaltens der Sicherheitsfunktionen	256
H.4	Management von Sicherheitsattributen (FMT_MSA)	256
H.4.1	Anwendungshinweise für Benutzer	256
H.4.2	FMT_MSA.1 Management von Sicherheitsattributen	256
H.4.3	FMT_MSA.2 Sichere Sicherheitsattribute	257
H.4.4	FMT_MSA.3 Statische Attributinitialisierung	257
H.4.5	FMT_MSA.4 Vererbung von Sicherheitsattributwerten	258
H.5	Management von TSF-Daten (FMT_MTD)	258
H.5.1	Anwendungshinweise für Benutzer	258
H.5.2	FMT_MTD.1 Management von TSF-Daten	258
H.5.3	FMT_MTD.2 Management von Grenzen auf TSF-Daten	259
H.5.4	FMT_MTD.3 Sichere TSF-Daten	259
H.6	Widerruf (FMT_REV)	260
H.6.1	Anwendungshinweise für Benutzer	260
H.6.2	FMT_REV.1 Widerruf	260
H.7	Ablauf von Sicherheitsattributen (FMT_SAE)	260
H.7.1	Anwendungshinweise für Benutzer	260
H.7.2	FMT_SAE.1 Befristete Autorisierung	260
H.8	Spezifizierung von Managementfunktionen (FMT_SMF)	261

H.8.1	Anwendungshinweise für Benutzer	261
H.8.2	FMT_SMF.1 Spezifizierung von Managementfunktionen	261
H.9	Sicherheitsmanagementrollen (FMT_SMR)	261
H.9.1	Anwendungshinweise für Benutzer	261
H.9.2	FMT_SMR.1 Sicherheitsrollen	262
H.9.3	FMT_SMR.2 Einschränkungen zu Sicherheitsrollen	262
H.9.4	FMT_SMR.3 Übernahme von Rollen	263
Anhang I (normativ) Klasse FPR: Privatsphäre — Anwendungshinweise		264
I.1	Allgemeines	264
I.2	Anonymität (FPR_ANO)	265
I.2.1	Anwendungshinweise für Benutzer	265
I.2.2	FPR_ANO.1 Anonymität	266
I.2.3	FPR_ANO.2 Anonymität ohne Anforderung von Informationen	266
I.3	Pseudonymität (FPR_PSE)	267
I.3.1	Anwendungshinweise für Benutzer	267
I.3.2	FPR_PSE.1 Pseudonymität	268
I.3.3	FPR_PSE.2 Umkehrbare Pseudonymität	269
I.3.4	FPR_PSE.3 Alias-Pseudonymität	270
I.4	Unverknüpfbarkeit (FPR_UNL)	270
I.4.1	Anwendungshinweise für Benutzer	270
I.4.2	FPR_UNL.1 Unverknüpfbarkeit	271
I.5	Unbeobachtbarkeit (FPR_UNO)	272
I.5.1	Anwendungshinweise für Benutzer	272
I.5.2	FPR_UNO.1 Unbeobachtbarkeit	273
I.5.3	FPR_UNO.2 Zuweisung von Informationen mit Einfluss auf Unbeobachtbarkeit	273
I.5.4	FPR_UNO.3 Unbeobachtbarkeit ohne Anforderung von Informationen	275
I.5.5	FPR_UNO.4 Autorisierte Benutzerbeobachtbarkeit	275
Anhang J (normativ) Klasse FPT: Schutz der TSF — Anwendungshinweise		276
J.1	Allgemeines	276
J.2	FPT_EMS TOE-Emanation	277
J.2.1	Anwendungshinweise für Benutzer	277
J.2.2	FPT_EMS.1 TOE-Emanation	277
J.3	Sicherheit bei Ausfall (FPT_FLS)	277
J.3.1	Anwendungshinweise für Benutzer	277
J.3.2	FPT_FLS.1 Ausfall mit Beibehaltung des sicheren Zustands	278
J.4	TSF-Initialisierung (FPT_INI)	278
J.4.1	Anwendungshinweise für Benutzer	278
J.4.2	FPT_INI.1 TSF-Initialisierung	278
J.5	Verfügbarkeit von exportierten TSF-Daten (FPT_ITA)	279
J.5.1	Anwendungshinweise für Benutzer	279
J.5.2	FPT_ITA.1 Inter-TSF-Verfügbarkeit innerhalb einer definierten Verfügbarkeitsmetrik	279
J.6	Vertraulichkeit der exportierten TSF-Daten (FPT_ITC)	279
J.6.1	Anwendungshinweise für Benutzer	279
J.6.2	Hinweise für Evaluatoren	279
J.6.3	FPT_ITC.1 Inter-TSF-Vertraulichkeit während der Übertragung	280
J.7	Integrität exportierter TSF-Daten (FPT_ITI)	280
J.7.1	Anwendungshinweise für Benutzer	280
J.7.2	FPT_ITI.1 Inter-TSF-Erkennung von Änderungen	280
J.7.3	FPT_ITI.2 Inter-TSF-Erkennung und Korrektur von Änderungen	281
J.8	Interne TOE-TSF-Datenübertragung (FPT_ITT)	281
J.8.1	Anwendungshinweise für Benutzer	281
J.8.2	Hinweise für Evaluatoren	281
J.8.3	FPT_ITT.1 Einfacher Schutz der TSF-Daten bei interner Übertragung	282
J.8.4	FPT_ITT.2 Trennung des TSF-Datentransfers	282
J.8.5	FPT_ITT.3 Überwachung der Integrität von TSF-Daten	282
J.9	Physischer Schutz der TSF (FPT_PHP)	282
J.9.1	Anwendungshinweise für Benutzer	282

J.9.2	FPT_PHP.1 Passive Erkennung von physischen Angriffen	283
J.9.3	FPT_PHP.2 Mitteilung von physischen Angriffen	283
J.9.4	FPT_PHP.3 Widerstand gegen physische Angriffe	284
J.10	Vertrauenswürdige Wiederherstellung (FPT_RCV)	284
J.10.1	Anwendungshinweise für Benutzer	284
J.10.2	FPT_RCV.1 Manuelle Wiederherstellung	286
J.10.3	FPT_RCV.2 Automatische Wiederherstellung	287
J.10.4	FPT_RCV.3 Automatische Wiederherstellung ohne übermäßigen Verlust	287
J.10.5	FPT_RCV.4 Funktionswiederherstellung	288
J.11	Erkennung von Wiederverwendung (FPT_RPL)	288
J.11.1	Anwendungshinweise für Benutzer	288
J.11.2	FPT_RPL.1 Erkennung von Wiederverwendung	288
J.12	Zustandssynchronitätsprotokoll (FPT_SSP)	288
J.12.1	Anwendungshinweise für Benutzer	288
J.12.2	FPT_SSP.1 Einfache vertrauenswürdige Bestätigung	289
J.12.3	FPT_SSP.2 Gegenseitige vertrauenswürdige Bestätigung	289
J.13	Zeitstempel (FPT_STM)	289
J.13.1	Anwendungshinweise für Benutzer	289
J.13.2	FPT_STM.1 Verlässliche Zeitstempel	290
J.14	Inter-TSF-TSF-Datenkonsistenz (FPT_TDC)	290
J.14.1	Anwendungshinweise für Benutzer	290
J.14.2	FPT_TDC.1 Einfache Inter-TSF-TSF-Datenkonsistenz	290
J.15	Prüfen von externen Entitäten (FPT_TEE)	291
J.15.1	Anwendungshinweise für Benutzer	291
J.15.2	Hinweise für Evaluatoren	291
J.15.3	FPT_TEE.1 Prüfen von externen Entitäten	291
J.16	Interne TOE-TSF-Datenreplizierungskonsistenz (FPT_TRC)	292
J.16.1	Anwendungshinweise für Benutzer	292
J.16.2	FPT_TRC.1 Interne TSF-Konsistenz	292
J.17	TSF-Selbstprüfung (FPT_TST)	292
J.17.1	Anwendungshinweise für Benutzer	292
J.17.2	Hinweise für Evaluatoren	293
J.17.3	FPT_TST.1 TSF-Prüfung	293
Anhang K (normativ) Klasse FRU: Verwendung von Ressourcen — Anwendungshinweise		295
K.1	Allgemeines	295
K.2	Fehlertoleranz (FRU_FLT)	295
K.2.1	Anwendungshinweise für Benutzer	295
K.2.2	FRU_FLT.1 Verminderte Fehlertoleranz	295
K.2.3	FRU_FLT.2 Begrenzte Fehlertoleranz	296
K.3	Priorität von Diensten (FRU_PRS)	296
K.3.1	Anwendungshinweise für Benutzer	296
K.3.2	FRU_PRS.1 Begrenzte Priorität von Diensten	296
K.3.3	FRU_PRS.2 Vollständige Priorität von Diensten	297
K.4	Ressourcenzuweisung (FRU_RSA)	297
K.4.1	Anwendungshinweise für Benutzer	297
K.4.2	FRU_RSA.1 Höchstquoten	298
K.4.3	FRU_RSA.2 Mindestquoten und Höchstquoten	298
Anhang L (normativ) Klasse FTA: TOE-Zugriff — Anwendungshinweise		300
L.1	Allgemeines	300
L.2	Einschränkung des Umfangs auswählbarer Attribute (FTA_LSA)	300
L.2.1	Anwendungshinweise für Benutzer	300
L.2.2	FTA_LSA.1 Einschränkung des Umfangs auswählbarer Attribute	301
L.3	Einschränkung von mehreren gleichzeitigen Sitzungen (FTA_MCS)	301
L.3.1	Anwendungshinweise für Benutzer	301
L.3.2	FTA_MCS.1 Einfache Einschränkung von mehreren gleichzeitigen Sitzungen	301
L.3.3	FTA_MCS.2 Einschränkung von mehreren gleichzeitigen Sitzungen je Benutzerattribut	301
L.4	Sperren und Beenden von Sitzungen (FTA_SSL)	302

L.4.1	Anwendungshinweise für Benutzer	302
L.4.2	FTA_SSL.1 Durch die TSF ausgelöstes Sperren der Sitzung	302
L.4.3	FTA_SSL.2 Durch den Benutzer ausgelöstes Sperren	303
L.4.4	FTA_SSL.3 Durch die TSF ausgelöstes Beenden	303
L.4.5	FTA_SSL.4 Durch den Benutzer ausgelöstes Beenden	303
L.5	TOE-Zugriffsbanner (FTA_TAB)	304
L.5.1	Anwendungshinweise für Benutzer	304
L.5.2	FTA_TAB.1 Standard-TOE-Zugriffsbanner	304
L.6	TOE-Zugriffsverlauf (FTA_TAH)	304
L.6.1	Anwendungshinweise für Benutzer	304
L.6.2	FTA_TAH.1 TOE-Zugriffsverlauf	304
L.7	TOE-Sitzungsaufbau (FTA_TSE)	305
L.7.1	Anwendungshinweise für Benutzer	305
L.7.2	FTA_TSE.1 TOE-Sitzungsaufbau	305
Anhang M (normativ) Klasse FTP: Vertrauenswürdiger Pfad/vertrauenswürdige Kanäle —		
	Anwendungshinweise	307
M.1	Allgemeines	307
M.2	Vertrauenswürdiger Kanal Inter-TSF (FTP_ITC)	307
M.2.1	Anwendungshinweise für Benutzer	307
M.2.2	FTP_ITC.1 Vertrauenswürdiger Kanal Inter-TSF	307
M.3	Vertrauenswürdiges Kanalprotokoll (FTP_PRO)	308
M.3.1	Anwendungshinweise für Benutzer	308
M.3.2	FTP_PRO.1 Protokoll des vertrauenswürdigen Kanals	308
M.3.3	FTP_PRO.2 Einrichtung des vertrauenswürdigen Kanals	309
M.3.4	FTP_PRO.3 Datenschutz für den vertrauenswürdigen Kanal	309
M.4	Vertrauenswürdiger Pfad (FTP_TRP)	310
M.4.1	Anwendungshinweise für Benutzer	310
M.4.2	FTP_TRP.1 Vertrauenswürdiger Pfad	310
	Literaturhinweise	311

Bilder

Bild 1	— Beziehung zwischen Benutzerdaten und TSF-Daten	33
Bild 2	— Beziehung zwischen „Authentisierungsdaten“ und „Sicherheitsinformationen“	34
Bild 3	— Struktur der Funktionsklassen	34
Bild 4	— Struktur der Funktionsfamilien	35
Bild 5	— Struktur der Funktionskomponenten	37
Bild 6	— Muster eines Klassenaufbaudiagramms	39
Bild 7	— FAU: Klassenaufbau Sicherheitsaudit	40
Bild 8	— FAU_ARP: Komponentenebenen	40
Bild 9	— FAU_GEN: Komponentenebenen	41
Bild 10	— FAU_SAA: Komponentenebenen	43
Bild 11	— FAU_SAR: Komponentenebenen	46
Bild 12	— FAU_SEL: Komponentenebenen	48
Bild 13	— FAU_STG: Komponentenebenen	49
Bild 14	— FCO: Klassenaufbau Kommunikation	52
Bild 15	— FCO_NRO: Komponentenebenen	52
Bild 16	— FCO_NRR: Komponentenebenen	54
Bild 17	— FCS: Klassenaufbau Kryptographische Unterstützung	57
Bild 18	— FCS_CKM: Komponentenebenen	58
Bild 19	— FCS_COP: Komponentenebenen	61
Bild 20	— FCS_RBG: Komponentenebenen	62
Bild 21	— FCS_RNG: Komponentenebenen	65
Bild 22	— FDP: Klassenaufbau Schutz von Benutzerdaten	67
Bild 23	— FDP_ACC: Komponentenebenen	68

Bild 24 — FDP_ACF: Komponentenebenen	69
Bild 25 — FDP_DAU: Komponentenebenen	70
Bild 26 — FDP_ETC: Komponentenebenen	72
Bild 27 — FDP_IFC: Komponentenebenen	74
Bild 28 — FDP_IFF: Komponentenebenen	76
Bild 29 — FDP_IRC: Komponentenebenen	81
Bild 30 — FDP_ITC: Komponentenebenen	82
Bild 31 — FDP_ITT: Komponentenebenen	84
Bild 32 — FDP_RIP: Komponentenebenen	86
Bild 33 — FDP_ROL: Komponentenebenen	87
Bild 34 — FDP_SDC: Komponentenebenen	89
Bild 35 — FDP_SDI: Komponentenebenen	90
Bild 36 — FDP_UCT: Komponentenebenen	92
Bild 37 — FDP_UIT: Komponentenebenen	93
Bild 38 — FIA: Klassenaufbau Identifikation und Authentifizierung	96
Bild 39 — FIA_AFL: Komponentenebenen	96
Bild 40 — FIA_API: Komponentenebenen	97
Bild 41 — FIA_ATD: Komponentenebenen	98
Bild 42 — FIA_SOS: Komponentenebenen	99
Bild 43 — FIA_UAU: Komponentenebenen	101
Bild 44 — FIA_UID: Komponentenebenen	105
Bild 45 — FIA_USB: Komponentenebenen	106
Bild 46 — FMT: Klassenaufbau Sicherheitsmanagement	108
Bild 47 — FMT_LIM: Komponentenebenen	109
Bild 48 — FMT_MOF: Komponentenebenen	110
Bild 49 — FMT_MSA: Komponentenebenen	111
Bild 50 — FMT_MTD: Komponentenebenen	114
Bild 51 — FMT_REV: Komponentenebenen	116
Bild 52 — FMT_SAE: Komponentenebenen	117
Bild 53 — FMT_SMF: Komponentenebenen	118
Bild 54 — FMT_SMR: Komponentenebenen	119
Bild 55 — FPR: Klassenaufbau Privatsphäre	121
Bild 56 — FPR_ANO: Komponentenebenen	121
Bild 57 — FPR_PSE: Komponentenebenen	123
Bild 58 — FPR_UNL: Komponentenebenen	125
Bild 59 — FPR_UNO: Komponentenebenen	126
Bild 60 — FPT: Klassenaufbau Schutz der TSF	129
Bild 61 — FPT_EMS: Komponentenebenen	130
Bild 62 — FPT_FLS: Komponentenebenen	131
Bild 63 — FPT_INI: Komponentenebenen	132
Bild 64 — FPT_ITA: Komponentenebenen	133
Bild 65 — FPT_ITC: Komponentenebenen	134
Bild 66 — FPT_ITI: Komponentenebenen	135
Bild 67 — FPT_ITT: Komponentenebenen	136
Bild 68 — FPT_PHP: Komponentenebenen	139
Bild 69 — FPT_RCV: Komponentenebenen	141
Bild 70 — FPT_RPL: Komponentenebenen	144
Bild 71 — FPT_SSP: Komponentenebenen	145
Bild 72 — FPR_STM: Komponentenebenen	146
Bild 73 — FPT_TDC: Komponentenebenen	147
Bild 74 — FPT_TEE: Komponentenebenen	148
Bild 75 — FPT_TRC: Komponentenebenen	149
Bild 76 — FPT_TST: Komponentenebenen	150
Bild 77 — FRU: Klassenaufbau Verwendung von Ressourcen	152
Bild 78 — FRU_FLT: Komponentenebenen	152
Bild 79 — FRU_PRS: Komponentenebenen	153
Bild 80 — FRU_RSA: Komponentenebenen	155

Bild 81 — FTA: Klassenaufbau TOE-Zugriff	157
Bild 82 — FTA_LSA: Komponentenebenen	157
Bild 83 — FTA_MCS: Komponentenebenen	158
Bild 84 — FTA_SSL: Komponentenebenen	160
Bild 85 — FTA_TAB: Komponentenebenen	162
Bild 86 — FTA_TAH: Komponentenebenen	163
Bild 87 — FTA_TSE: Komponentenebenen	164
Bild 88 — FTP: Klassenaufbau Vertrauenswürdiger Pfad/vertrauenswürdige Kanäle	166
Bild 89 — FTP_ITC: Komponentenebenen	166
Bild 90 — FTP_PRO: Komponentenebenen	167
Bild 91 — FTP_TRP: Komponentenebenen	170
Bild A.1 — Struktur der Funktionsklassen	172
Bild A.2 — Struktur der Funktionsfamilien für Anwendungshinweise	173
Bild A.3 — Struktur der Funktionskomponenten	174

Tabellen

Tabelle 1 — FPT_EMS.1.1 Tabelle	130
Tabelle 2 — FPT_INI.1.2 Tabelle	132
Tabelle B.1 — Abhängigkeitstabelle für Klasse FAU: Sicherheitsaudit	175
Tabelle B.2 — Abhängigkeitstabelle für Klasse FCO: Kommunikation	176
Tabelle B.3 — Abhängigkeitstabelle für Klasse FCS: Kryptographische Unterstützung	177
Tabelle B.4 — Abhängigkeitstabelle für Klasse FDP: Schutz von Benutzerdaten	177
Tabelle B.5 — Abhängigkeitstabelle für Klasse FIA: Identifikation und Authentifizierung	180
Tabelle B.6 — Abhängigkeitstabelle für Klasse FMT: Sicherheitsmanagement	180
Tabelle B.7 — Abhängigkeitstabelle für Klasse FPR: Privatsphäre	181
Tabelle B.8 — Abhängigkeitstabelle für Klasse FPT: Schutz der TSF	181
Tabelle B.9 — Abhängigkeitstabelle für Klasse FRU: Verwendung von Ressourcen	182
Tabelle B.10 — Abhängigkeitstabelle für Klasse FTA: TOE-Zugriff	182
Tabelle B.11 — Abhängigkeitstabelle für Klasse FTP: Vertrauenswürdiger Pfad/vertrauenswürdige Kanäle	184

Europäisches Vorwort

Der Text von ISO/IEC 15408-2:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 15408-2:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird EN ISO/IEC 15408-2:2020 ersetzen.

Anerkennungsnotiz

Der Text von ISO/IEC 15408-2:2022 wurde von CEN als EN ISO/IEC 15408-2:2023 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Directives, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Directives, Teil 2 erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe <https://patents.iec.ch>).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html. In der IEC, siehe www.iec.ch/understanding-standards.

Dieses Dokument wurde vom Technischen Komitee ISO/TC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection* erarbeitet.

Diese vierte Ausgabe ersetzt die dritte Ausgabe (ISO 15408-2:2008^{N1}), die technisch überarbeitet wurde.

Die wesentlichen Änderungen sind folgende:

— Es wurden neue Sicherheitsfunktionskomponenten eingeführt.

Eine Auflistung aller Teile der Normenreihe ISO/IEC 15408 kann auf der ISO-Internetseite abgerufen werden.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html und www.iec.ch/national-committees zu finden.

N1 Nationale Fußnote: Gemeint ist: ISO/IEC 15408-2:2008.

Rechtliche Hinweise

Die unten aufgeführten Regierungsorganisationen haben zu der Entwicklung dieser Version der Common Criteria for Information Technology Security Evaluations beigetragen. Als gemeinsame Urheberrechtsinhaber an den Common Criteria for Information Technology Security Evaluations (kurz CC) erteilen sie hiermit der ISO/IEC die nicht-exklusive Lizenz zur Verwendung der CC für die weitere Entwicklung/Pflege der Normenreihe ISO/IEC 15408. Diese Regierungsorganisationen behalten sich allerdings das Recht zur Nutzung, Vervielfältigung, zum Vertrieb sowie zur Übersetzung und Änderung der CC nach Belieben vor.

Australien	Australian Signals Directorate
Kanada	Communications Security Establishment
Frankreich	Agence Nationale de la Sécurité des Systèmes d'Information
Deutschland	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Niederlande	Netherlands National Communications Security Agency
Neuseeland	Government Communications Security Bureau
Republik Korea	National Security Research Institute
Spanien	Ministerio de Asuntos Económicos y Transformación Digital
Schweden	FMV, Swedish Defence Materiel Administration
Vereinigtes Königreich	National Cyber Security Centre
USA	National Security Agency

Einleitung

Die in diesem Dokument definierten Sicherheitsfunktionskomponenten sind die Grundlage für in einem Schutzprofil (PP), PP-Modul, Funktionspaket oder einer Sicherheitsvorgabe (ST) ausgedrückten Sicherheitsfunktionsanforderungen (SFR). Diese Anforderungen beschreiben das von einem Evaluierungsgegenstand (TOE) erwartete, gewünschte Sicherheitsverhalten und sind dafür ausgelegt, die in einem PP, einem PP-Modul, einem Funktionspaket oder einer ST angegebenen Sicherheitszielsetzungen zu erfüllen. Diese Anforderungen beschreiben Sicherheitseigenschaften, die Benutzer durch direkte Interaktion (d. h. Eingaben, Ausgaben) mit der IT oder durch die IT-Antwort ermitteln können.

Sicherheitsfunktionskomponenten ermöglichen die Formulierung der SFR zur Abwehr von Bedrohungen in der angenommenen Betriebsumgebung des TOEs und/oder decken alle identifizierten organisatorischen Sicherheitspolitiken ab.

Zur Zielgruppe dieses Dokuments gehören Verbraucher, Entwickler und Evaluatoren von sicheren IT-Produkten. ISO/IEC 15408-1:2022, 5.2 enthält zusätzliche Informationen zur Zielgruppe der Normenreihe ISO/IEC 15408 und zur Verwendung der Normenreihe ISO/IEC 15408 durch entsprechende Gruppen. Diese Gruppen verwenden dieses Dokument wie folgt:

- a) Verbraucher, die dieses Dokument beim Auswählen von Komponenten in der Formulierung von Funktionsanforderungen verwenden, die die in einem PP, PP-Modul, Funktionspaket oder einer ST formulierten Sicherheitszielsetzungen erfüllen. ISO/IEC 15408-1:20—, Abschnitt 7 enthält weitere detaillierte Informationen zur Beziehung zwischen Sicherheitszielsetzungen und Sicherheitsanforderungen;
- b) Entwickler, die mit der Erstellung eines TOEs auf tatsächliche oder angenommene Sicherheitsanforderungen von Verbrauchern reagieren, finden in diesem Dokument eine genormte Methode zum Verständnis dieser Anforderungen. Sie verwenden auch den Inhalt dieses Dokuments als Grundlage für die weitere Definition der Sicherheitsfunktionalität und von Sicherheitsmechanismen des TOEs zur Konformität mit diesen Anforderungen;
- c) Evaluatoren, die die in diesem Dokument definierten SFR dazu nutzen, zu verifizieren, dass die im PP, PP-Modul, Funktionspaket oder in der ST definierten Funktionsanforderungen des TOEs die IT-Sicherheitszielsetzungen erfüllen und die alle Abhängigkeiten erfassen und als erfüllt nachweisen. Evaluatoren verwenden dieses Dokument unterstützend dazu, um festzustellen, ob ein TOE die angegebenen Anforderungen erfüllt.

ANMERKUNG Im vorliegenden Dokument werden einige Begriffe fett und kursiv gedruckt, um sie vom übrigen Text abzuheben. Die Beziehung zwischen den Komponenten einer Familie wird durch Fettmarkierung hervorgehoben. Diese Konvention erfordert die Verwendung von Fettdruck für alle neuen Anforderungen. Für hierarchische Komponenten werden Anforderungen fett hervorgehoben, wenn sie über die Anforderungen der vorherigen Komponente hinaus erweitert oder geändert werden. Zusätzlich werden alle neuen oder erweiterten zulässigen über die vorherige Komponente hinausgehenden Operationen auch fett hervorgehoben.

Die Verwendung von Kursivschrift weist auf einen Text hin, der eine genaue Bedeutung hat. Für die Vertrauenswürdigkeitsanforderungen gilt die Konvention für spezielle Verben, die sich auf die Evaluierung beziehen.

1 Anwendungsbereich

Dieses Dokument definiert die Anforderungen an Struktur und Inhalt der Sicherheitsfunktionskomponenten für die Sicherheitsevaluierung. Es enthält einen Katalog an Funktionskomponenten, der die häufigsten Sicherheitsfunktionsanforderungen vieler IT-Produkte abdeckt.

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 15408-1:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-3, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 15408-1, ISO/IEC 15408-3, ISO/IEC 18045 und die folgenden Begriffe.

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

- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>
- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>

3.1

Identität

Darstellung, die eine Entität im Kontext des Evaluierungsgegenstandes (TOE) eindeutig identifiziert

BEISPIEL Ein Beispiel für eine solche Repräsentation ist eine Zeichenkette.

Anmerkung 1 zum Begriff: Entitäten können unterschiedlicher Art sein, z. B. ein Benutzer, ein Prozess oder ein Datenträger. Bei einem menschlichen Benutzer kann die Repräsentation der vollständige oder abgekürzte Name oder ein eindeutiges Pseudonym sein.

Anmerkung 2 zum Begriff: Eine Entität kann mehr als eine Identität aufweisen.

3.2

Inter-TSF-Übertragung

Kommunikation zwischen dem Evaluierungsgegenstand (TOE) und den Sicherheitsfunktionen anderer vertrauenswürdiger IT-Produkte

3.3

interner Kommunikationskanal

Kommunikationskanal zwischen getrennten Teilen des Evaluierungsgegenstands (TOE)

3.4

interne TOE-Übertragung

Kommunikation von Daten zwischen getrennten Teilen des Evaluierungsgegenstands (TOE)

3.5

Betrieb

<an einer Komponente von ISO/IEC 15408-2> Modifikation oder Wiederholung einer Komponente durch Zuweisung, Iteration, Präzisierung oder Auswahl

3.6

Geheimnis

Informationen, die nur autorisierten Benutzern und/oder der TOE-Sicherheitsfunktionalität (TSF) bekannt sind, um eine spezifische *Sicherheitsfunktionsrichtlinie* (SFP) (3.8) durchzusetzen

3.7

sicherer Zustand

Zustand, in dem die Daten der TOE-Sicherheitsfunktionalität (TSF) konsistent sind und die TSF die ordnungsgemäße Durchsetzung der Sicherheitsfunktionsanforderungen (SFR) fortlaufend wahrnimmt

3.8

Sicherheitsfunktionsrichtlinie

SFP, en: Security Function Policy

Regelsatz, der ein bestimmtes Sicherheitsverhalten beschreibt, das von der TOE-Sicherheitsfunktionalität (TSF) durchgesetzt wird und sich als ein Satz von Sicherheitsfunktionsanforderungen (SFR) beschreiben lässt

3.9

TOE-Ressource

alles, was innerhalb des Evaluierungsgegenstands (TOE) nutzbar oder verwertbar ist

3.10

Übertragung außerhalb des TOEs

durch die Sicherheitsfunktionalität (TSF) des Evaluationsgegenstands (TOE) vermittelte Kommunikation von Daten an Entitäten, die nicht der Kontrolle der TSF unterliegen

3.11

vertrauenswürdiger Kanal

Weg, über den eine TOE-Sicherheitsfunktionalität (TSF) und ein anderes vertrauenswürdigen IT-Produkt mit dem notwendigen Vertrauensgrad kommunizieren können

3.12

vertrauenswürdiger Pfad

Weg, über den ein Anwender und eine TSF mit dem notwendigen Vertrauensgrad kommunizieren können

Anmerkung 1 zum Begriff: Die Kommunikation setzt in der Regel die Identifizierung und Authentifizierung beider Parteien sowie das Konzept einer benutzerspezifischen Sitzung voraus, die durch Integrität geschützt ist.

Anmerkung 2 zum Begriff: Handelt es sich bei der externen Entität um ein vertrauenswürdigen IT-Produkt, wird anstelle des vertrauenswürdigen Pfades der Begriff *vertrauenswürdiger Kanal* (3.11) verwendet.

Anmerkung 3 zum Begriff: Sowohl die physischen als auch die logischen Aspekte der sicheren Kommunikation können als Mechanismen zur Vertrauensbildung betrachtet werden.

3.13

TSF-Daten

Daten für den *Betrieb* (3.5) des Evaluierungsgegenstands (TOE), welche für die Durchsetzung der Sicherheitsanforderung (SFR) benötigt werden

3.14

Benutzerdaten

vom Evaluierungsgegenstand (TOE) empfangene oder erzeugte Daten, die für eine externe Entität von Bedeutung sind, aber die *Operation* (3.5) der TOE-Sicherheitsfunktionalität (TSF) nicht beeinflussen

Anmerkung 1 zum Begriff: Je nach Konzept geht diese Definition davon aus, dass dieselben Daten, die von den Benutzern erstellt werden und sich tatsächlich auf den Betrieb der TSF auswirken, als *TSF-Daten* (3.13) betrachtet werden können.

4 Abkürzungen

API	Anwendungsprogrammierschnittstelle (en: Application Programming Interface)
CD	Compact Disc
DAC	benutzerbestimmbare Zugriffskontrolle (en: Discretionary Access Control)
DRBG	deterministischer Zufallsbitgenerator (en: Deterministic Random Bit Generator)
EMS	elektromagnetisches Spektrum
GB	Gigabyte
GHz	Gigahertz
GUI	grafische Benutzungsschnittstelle (en: Graphical User Interface)
HSM	Hardware-Sicherheitsmodul
HTTPS	Hypertext-Übertragungsprotokoll sicher (en: Hypertext Transfer Protocol Secure)
IOCTL	Eingabe-Ausgabe-Steuerung (en: Input Output Control)
IP	Internet-Protokoll
IPsec	IP-Sicherheit (Protokoll) (en: IP security (protocol))
LDAP	vereinfachtes Verzeichniszugriffsprotokoll (en: Lightweight Directory Access Protocol)
MAC	systembestimmte Zugriffskontrolle (en: Mandatory Access Control)
MB	Megabyte
MBps	Megabytes je Sekunde
OS	Betriebssystem (en: Operating System)
OTP	einmalig programmierbar (en: One-Time Programmable)
PC	Personal Computer
PCI	Peripheral Component Interconnect
PKI	Public-Key-Infrastruktur (en: Public Key Infrastructure)
PP	Schutzprofil (en: Protection Profile)
RAM	Direktzugriffsspeicher (en: Random Access Memory)
RBG	Zufallsbitgenerator (en: Random Bit Generator)
RNG	Zufallszahlengenerator (en: Random Number Generator)
RPC	Remote Procedure Call
SFP	Sicherheitsfunktionsrichtlinie (en: security function policy)
SFR	Sicherheitsfunktionsanforderung (en: Security Functional Requirement)
SSH	Secure Shell
ST	Sicherheitsvorgabe (en: Security Target)
TCP	Transmission Control Protocol
TLS	Transportschichtsicherheit (en: Transport Layer Security)
TOE	Evaluierungsgegenstand (en: Target of Evaluation)
TSF	TOE-Sicherheitsfunktionalität (en: TOE Security Functionality)
TSFI	TSF-Schnittstelle (en: TSF Interface)

USB universeller serieller Bus
VPN Virtual Private Network

5 Übersicht

5.1 Allgemeines

Die Normenreihe ISO/IEC 15408 und die zugehörigen, in diesem Dokument beschriebenen Sicherheitsfunktionsanforderungen (SFR) sind nicht dazu ausgelegt, eine endgültige Antwort auf alle Probleme der IT-Sicherheit zu geben. Dieses Dokument bietet eine Reihe wohlverstandener Sicherheitsfunktionskomponenten, die zur Spezifizierung vertrauenswürdiger Produkte mit Blick auf die Markterfordernisse verwendet werden können. Diese Sicherheitsfunktionskomponenten werden als derzeitiger Stand der Technik bei der Sicherheitsanforderungsspezifikation dargestellt.

Dieses Dokument schließt nicht alle erdenklichen Sicherheitsfunktionskomponenten ein, sondern enthält die den an diesem Dokument Mitwirkenden bekannten und von ihnen als sinnvoll erachteten Komponenten.

Da sich das Verständnis und die Bedürfnisse von Verbrauchern ändern können, müssen die Funktionskomponenten dieses Dokuments gepflegt werden. Es ist vorgesehen, dass einige Autoren der PP, PP-Module, Funktionspakete und ST Sicherheitsbedürfnisse haben können, die nicht von den Sicherheitsfunktionskomponenten in diesem Dokument abgedeckt werden. In diesen Fällen kann der Autor eines PP, PP-Moduls, Funktionspakets oder einer ST die Verwendung von Funktionskomponenten und Anforderungen in Betracht ziehen, die nicht in diesem Dokument angegeben sind. Die Konzepte der Erweiterbarkeit werden in ISO/IEC 15408-1:2022, 8.4 erläutert.

5.2 Aufbau dieses Dokuments

Abschnitt 5 beschreibt das in den SFR dieses Dokuments verwendete Paradigma.

Abschnitt 7 stellt den Katalog der Funktionskomponenten vor, während Abschnitt 8 bis Abschnitt 18 die Funktionsklassen beschreiben.

Anhang A liefert Erklärungen für potentielle Benutzer der Funktionskomponenten.

Anhang B liefert eine vollständige Tabelle mit Querverweisungen zu den Abhängigkeiten der Funktionskomponenten.

Anhang C bis Anhang M liefern Erklärungen zu den Funktionsklassen. Dieses Material muss als normative Anweisungen zur Anwendung relevanter Operationen und Auswahl entsprechender Informationen zu Audit und Dokumentation betrachtet werden. Bei verschiedenen Optionen kann der Autor eines PP, PP-Moduls, Funktionspakets und einer ST frei wählen.

Autoren von PPs, PP-Modulen, Funktionspaketen oder STs müssen insbesondere für die entsprechenden Strukturen, Regeln und Leitlinien ISO/IEC 15408-1:2022 zu Rate ziehen:

- ISO/IEC 15408-1:2022, Abschnitt 3 definiert die in der Normenreihe ISO/IEC 15408 verwendeten Begriffe;
- ISO/IEC 15408-1:2022, Abschnitt 7 beschreibt, wie die SFR unter Verwendung der Sicherheitsfunktionskomponenten spezifiziert werden können;
- ISO/IEC 15408-1:2022, Abschnitt 8 beschreibt, wie die Sicherheitsfunktionskomponenten organisiert sind und welche Operationen an ihnen angewendet werden können;
- ISO/IEC 15408-1:2022, Anhang A liefert weitere Informationen zur Struktur für Sicherheitsfunktionspakete;

- e) ISO/IEC 15408-1:2022, Anhang B liefert weitere Informationen zur Struktur für PPs;
- f) ISO/IEC 15408-1:2022, Anhang C liefert weitere Informationen zur Struktur der PP-Module und PP-Konfigurationen;
- g) ISO/IEC 15408-1:2022, Anhang D liefert weitere Informationen zur Struktur für STs.

6 Paradigma für Funktionsanforderungen

Dieser Abschnitt beschreibt das in den Sicherheitsfunktionskomponenten verwendete Paradigma und die Ableitung der SFR.

Dieses Dokument ist ein Katalog an Sicherheitsfunktionskomponenten, die für die Spezifikation der einen TOE beschreibenden SFR verwendet werden dürfen.

Die TOE-Evaluierung beschäftigt sich hauptsächlich mit der Sicherstellung, dass eine definierte Reihe von SFRs über die TOE-Ressourcen durchgesetzt wird. Die SFRs definieren die Regeln, über die der TOE den Zugriff auf und die Nutzung seiner Ressourcen steuert und somit die vom TOE geregelten Informationen und Dienste.

Die SFRs können mehrere Sicherheitsfunktionspolitiken (SFPs) definieren, um die von den TOEs durchzusetzenden Regeln darzustellen. Jede SFP legt über die Definition von Subjekten, Objekten, Ressourcen oder Informationen und Operationen, für die diese SFP gültig ist, ihren Anwendungsbereich der Kontrolle fest. Alle SFPs werden über die TOE-Sicherheitsfunktionalität (TSF) (siehe unten) implementiert, deren Mechanismen die in den SFRs definierten Regeln durchsetzen und die erforderlichen Fähigkeiten bereitstellen.

Die von einem TOE für die korrekte Durchsetzung der SFRs erforderlichen Bestandteile werden in ihrer Gesamtheit als TSF bezeichnet. Die TSF besteht aus der gesamten Hardware, Software und Firmware eines TOEs, auf die sich entweder direkt oder indirekt für die Durchsetzung der Sicherheit verlassen wird.

Der TOE kann ein monolithisches Produkt sein, das Hardware, Firmware und Software enthält. Der TOE kann alternativ auch ein mehrteiliges Produkt sein, das intern aus mehreren, getrennten Teilen besteht. Jedes dieser Teile des TOEs bietet einen bestimmten Dienst für den TOE und ist mit den anderen Teilen des TOEs über einen internen Kommunikationskanal verbunden. Dieser kann so klein sein wie ein Prozessorbus oder darf ein internes Netzwerk für den TOE umfassen.

Wenn der TOE aus mehreren Teilen besteht, dann kann jeder Teil seinen eigenen Teil der TSF haben, der wiederum Benutzerdaten und TSF-Daten über interne Kommunikationskanäle mit anderen Teilen der TSF austauscht. Diese Interaktion wird als interne TOE-Übertragung bezeichnet. In solch einem Fall bilden die einzelnen Teile der TSF abstrahiert die zusammengesetzte TSF, die die SFRs durchsetzt.

Die Schnittstellen eines TOEs können für den bestimmten TOE lokalisiert sein oder sie können über externe Kommunikationskanäle mit anderen IT-Produkten interagieren. Diese externen Interaktionen mit anderen IT-Produkten können zwei Formen annehmen.

- a) Die SFRs des anderen „vertrauenswürdigen IT-Produkts“ und die SFRs des TOEs wurden verwaltungstechnisch abgestimmt und von dem anderen vertrauenswürdigen IT-Produkt wird angenommen, dass es seine SFRs korrekt durchsetzt (z. B. durch gesonderte Evaluierung). Informationsaustausche in dieser Situation werden Inter-TSF-Übertragungen genannt, da sie zwischen den TSFs einzelner vertrauenswürdiger Produkte stattfinden.
- b) Das andere IT-Produkt ist möglicherweise nicht vertrauenswürdig und kann als „nicht vertrauenswürdiges IT-Produkt“ bezeichnet werden. Seine SFRs sind daher entweder unbekannt oder deren Implementation wird als nicht vertrauenswürdig erachtet. In dieser Situation werden durch die TSF vermittelte Informationsaustausche als Übertragungen außerhalb des TOEs bezeichnet, da es entweder keine TSFs gibt oder deren politische Merkmale für das andere IT-Produkt unbekannt sind.

Die Reihe von Schnittstellen, ob interaktiv (Mensch-Maschine-Schnittstelle) oder programmatisch (Anwendungsprogrammierschnittstelle (API)), durch die auf Ressourcen zugegriffen wird, die über die TSF vermittelt werden, oder durch die Informationen vom TSF abgerufen werden, wird als TSF-Schnittstelle (TSFI) bezeichnet. Die TSFI definiert die Grenzen der TOE-Funktionalität, welche für die Durchsetzung der SFRs bereitgestellt wird.

Benutzer befinden sich außerhalb des TOEs. Allerdings interagieren Benutzer mit dem TOE über die TSFIs, um die Ausführung von Diensten durch den TOE anzufragen, die den in den SFRs definierten Regeln entsprechen. Es gibt zwei Arten von Benutzern, die für dieses Dokument von Interesse sind: menschliche Benutzer und externe IT-Entitäten. Menschliche Benutzer können noch weiter unterschieden werden in lokale menschliche Benutzer, also Benutzer, die direkt mit dem TOE über TOE-Geräte interagieren oder entfernte menschliche Benutzer, also Benutzer, die indirekt über ein anderes IT-Produkt mit dem TOE interagieren.

BEISPIEL 1 Ein Beispiel für ein TOE-Gerät ist eine Arbeitsstation.

Eine Zeitspanne der Interaktion zwischen Benutzern und der TSF wird als Sitzung bezeichnet. Der Aufbau von Benutzersitzungen kann auf der Grundlage einer Vielzahl an Überlegungen gesteuert werden.

BEISPIEL 2 Benutzerauthentifizierung, Tageszeit, Zugriffsmethode auf den TOE und Anzahl der erlaubten gleichzeitigen Sitzungen (je Benutzer oder insgesamt).

Dieses Dokument verwendet den Begriff „autorisiert“, um einen Benutzer zu kennzeichnen, der entweder die zur Durchführung einer Operation erforderlichen Rechte oder Privilegien oder beides besitzt. Der Begriff „autorisierter Benutzer“ bedeutet also, dass für diesen Benutzer die Ausführung einer bestimmten Operation oder einer Reihe von Operationen, entsprechend der Definition in den SFRs, erlaubt ist.

Um Anforderungen zu formulieren, die eine Trennung von Administratöraufgaben verlangen, besagen die relevanten Sicherheitsfunktionskomponenten (der Familie FMT_SMR) explizit, dass administrative Rollen erforderlich sind. Eine Rolle ist ein vordefinierter Regelwerk, das die zulässigen Interaktionen zwischen einem Benutzer in dieser Rolle und dem TOE festlegt. Ein TOE kann die Definition einer beliebigen Anzahl an Rollen unterstützen.

BEISPIEL 3 Zu den Rollen für einen sicheren Betrieb eines TOEs können „Auditadministrator“ und „Benutzerkontenadministrator“ gehören.

TOEs enthalten Ressourcen, die zur Verarbeitung und Speicherung von Informationen verwendet werden können. Das wichtigste Ziel der TSF ist die vollständige und korrekte Durchsetzung der SFRs über die vom TOE gesteuerten Ressourcen und Informationen.

TOE-Ressourcen können auf viele unterschiedliche Arten aufgebaut und verwendet werden. Allerdings trifft dieses Dokument eine bestimmte Unterscheidung, die die Spezifizierung gewünschter Sicherheitseigenschaften ermöglicht. Alle Entitäten die aus Ressourcen hergestellt werden können, können auf eine von zwei Arten gekennzeichnet werden. Die Entitäten können aktiv sein, also der Grund für Aktionen innerhalb des TOEs sein, und sie können der Grund für Operationen sein, die auf der Grundlage von Informationen ausgeführt werden. Alternativ können Entitäten auch passiv sein und sind dann entweder der Container, aus dem die Informationen kommen oder in dem die Informationen gespeichert werden.

Aktive Entitäten im TOE, die Operationen an Objekten ausführen, werden als Subjekte bezeichnet. Innerhalb eines TOEs können mehrere Subjekttypen bestehen:

- a) solche, die im Namen eines autorisierten Benutzers agieren;

BEISPIEL 4 UNIX-Prozesse.

- b) solche, die als ein spezifischer Funktionsprozess agieren, der wiederum im Namen mehrerer Benutzer handeln kann;

BEISPIEL 5 Funktionen, wie sie in Client/Server-Architekturen zu finden sind.

c) solche, die als Teil des TOEs selbst agieren.

BEISPIEL 6 Prozesse, die nicht im Namen eines Benutzers agieren.

Dieses Dokument behandelt die Durchsetzung der SFRs über die oben aufgeführten Subjekttypen.

Passive Entitäten im TOE, die Informationen enthalten oder empfangen und an denen Subjekte Operationen durchführen, werden als Objekte bezeichnet. Wenn ein Subjekt (eine aktive Entität) das Ziel einer Operation ist, kann ein Subjekt auch wie ein Objekt behandelt werden.

BEISPIEL 7 Ein Beispiel für ein Subjekt ist eine Interprozesskommunikation.

Objekte können Informationen enthalten. Dieses Konzept ist zur Spezifizierung von Richtlinien zur Informationsflusssteuerung in der Klasse FDP erforderlich.

Von Regeln in den SFRs kontrollierte Benutzer, Subjekte, Information, Objekte, Sitzungen und Ressourcen können gewisse Attribute aufweisen, die Informationen zur Verwendung durch den TOE für seinen korrekten Betrieb enthalten. Einige Attribute, wie Dateinamen, dürfen informativ oder zur Identifizierung individueller Ressourcen ausgelegt sein, während andere Attribute, wie Informationen zur Zugriffskontrolle spezifisch für die Durchsetzung der SFRs existieren können. Diese letztgenannten Attribute werden allgemein als „Sicherheitsattribute“ bezeichnet. Das Wort Attribut wird in diesem Dokument an einigen Stellen als Kurzform für den Begriff „Sicherheitsattribut“ verwendet. Unabhängig von der bestimmungsgemäßen Verwendung der Attributinformation können Kontrollen der Attribute entsprechend den Vorgaben der SFRs erforderlich sein.

Daten in einem TOE werden entweder als Benutzerdaten oder TSF-Daten eingestuft. Bild 1 stellt diese Beziehung dar. Benutzerdaten sind in TOEs gespeicherte Informationen, die von Benutzern in Übereinstimmung mit den SFRs bedient werden können und die für die TSF keine besondere Bedeutung haben. TSF-Daten sind Informationen, die TSFs bei der Entscheidungsfindung gemäß den Anforderungen der SFRs verwenden. TSF-Daten dürfen von Benutzern beeinflusst werden, wenn dies von den SFRs erlaubt wird.

BEISPIEL 8 Benutzerdaten:

— Der Inhalt einer E-Mail kann zu den Benutzerdaten gehören.

TSF-Daten:

— Sicherheitsattribute, Authentisierungsdaten, interne TSF-Statusvariablen, die von den in den SFRs definierten Regeln oder zum Schutz der TSFs verwendet werden, und Einträge in Zugriffskontrolllisten sind Beispiele für TSF-Daten.

Es gibt mehrere für den Datenschutz anwendbare SFPs wie SFPs zur Zugriffskontrolle und SFPs zur Informationsflusskontrolle. Die Mechanismen zur Implementation von SFPs zur Zugriffskontrolle stützen ihre Politikentscheidungen auf Attribute der Benutzer, Ressourcen, Subjekte, Objekte, Sitzungen, TSF-Statusdaten und Operationen im Anwendungsbereich der Kontrolle. Diese Attribute werden im Regelwerk verwendet, das die zulässigen Operationen der Subjekte an den Objekten steuert.

Die Mechanismen zur Implementation der SFPs zur Informationsflusskontrolle stützen ihre Politikentscheidungen auf die Attribute der Subjekte, auf Informationen im Anwendungsbereich der Kontrolle und auf das Regelwerk, das die Operationen der Subjekte an den Informationen steuert. Die Attribute der Informationen, die mit den Attributen des Containers verbunden oder von den Daten im Container abgeleitet werden können, verbleiben während der Verarbeitung durch die TSF bei der Information.

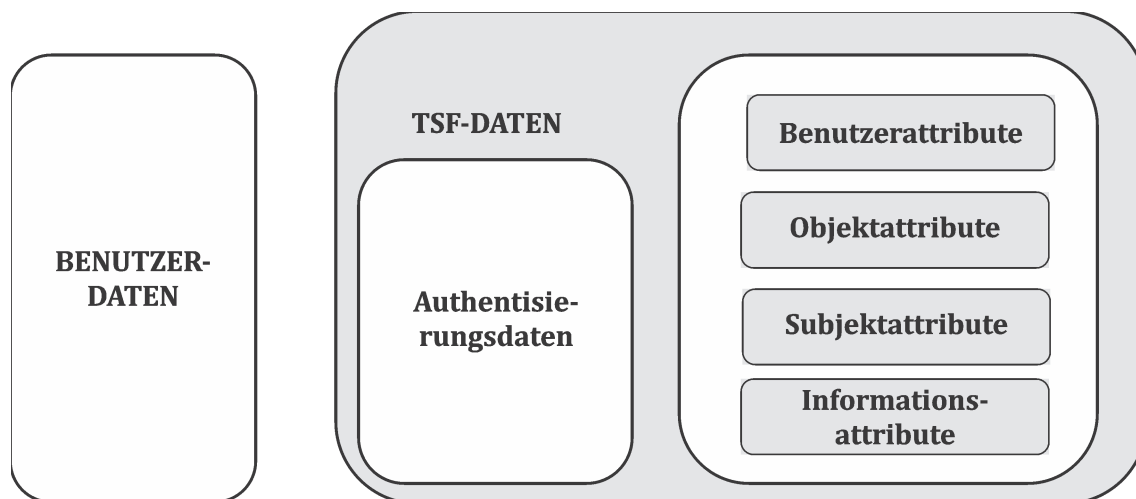


Bild 1 — Beziehung zwischen Benutzerdaten und TSF-Daten

Zwei bestimmte, in diesem Dokument behandelte Arten von TSF-Daten können identisch sein, müssen es aber nicht. Dabei handelt es sich um Authentisierungsdaten und Sicherheitsinformationen.

Authentisierungsdaten werden zur Verifizierung der durch einen Benutzer beanspruchten Identität bei der Anfrage von Diensten des TOEs verwendet. Die üblichste Form von Authentisierungsdaten ist das Passwort, das als wirksamer Sicherheitsmechanismus darauf angewiesen ist, geheim gehalten zu werden. Es brauchen allerdings nicht alle Formen von Authentisierungsdaten geheim gehalten werden. Geräte zur biometrischen Authentisierung erfordern keine Geheimhaltung der Daten, sondern verlassen sich auf die Tatsache, dass nur ein Benutzer über diese Daten verfügt und sie nicht verfälscht werden können.

BEISPIEL 9 Beispiele für Geräte zur biometrischen Authentisierung sind Fingerabdruckleser und Netzhautscanner.

Der in diesem Dokument verwendete Begriff Sicherheitsinformationen ist zwar auf Authentisierungsdaten anwendbar, soll aber auch auf andere Arten von Daten anwendbar sein, die geheim gehalten werden müssen, um eine spezifische SFP durchzusetzen.

Daher müssen einige, aber nicht alle, Authentisierungsdaten geheim gehalten werden und einige, aber nicht alle, Sicherheitsinformationen werden als Authentisierungsdaten verwendet. Bild 2 zeigt diese Beziehung zwischen Sicherheitsinformationen und Authentisierungsdaten. Im Bild werden die üblichen Datentypen von Authentisierungsdaten und Sicherheitsinformationen in Unterabschnitten aufgezeigt.

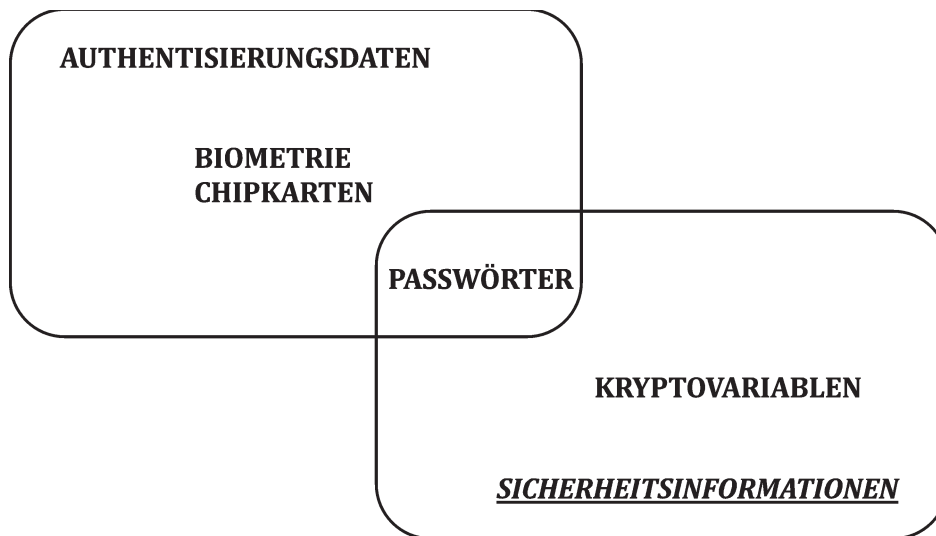


Bild 2 — Beziehung zwischen „Authentisierungsdaten“ und „Sicherheitsinformationen“

7 Sicherheitsfunktionskomponenten

7.1 Übersicht

7.1.1 Allgemeines

Dieser Abschnitt definiert Inhalt und Darstellung der Funktionsanforderungen dieses Dokuments und bietet Leitlinien zur Organisation der Anforderungen an neue, erweiterte Komponenten, die in ein PP, PP-Modul, Funktionspaket oder eine ST aufgenommen werden dürfen. Wie in ISO/IEC 15408-1:2022, Abschnitt 8 beschrieben, werden die Funktionskomponenten und Anforderungen in Klassen, Familien, Komponenten und Elementen ausgedrückt.

7.1.2 Klassenstruktur

7.1.2.1 Allgemeines

Bild 3 stellt die Struktur der Funktionsklassen schematisch dar. Jede Funktionsklasse enthält einen Klassennamen, eine Klasseneinleitung und eine oder mehrere Funktionsfamilien.

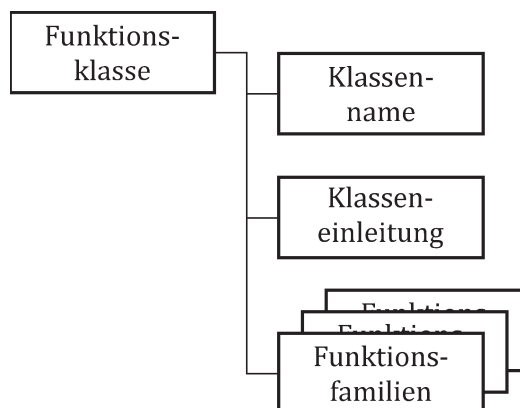


Bild 3 — Struktur der Funktionsklassen

ANMERKUNG Eine Funktionsklasse kann mehrere Funktionsfamilien enthalten.

7.1.2.2 Klassenname

Der Unterabschnitt Klassenname liefert erforderliche Informationen zur Identifizierung und Einstufung einer Funktionsklasse. Jede Funktionsklasse hat einen eindeutigen Namen. Die kategorische Information zur Einstufung besteht aus einem Kurznamen mit drei Zeichen. Der Kurzname der Klasse wird bei der Spezifikation der Kurznamen der Familien für diese Klasse verwendet.

7.1.2.3 Klasseneinleitung

Die Klasseneinleitung erfasst den gemeinsamen Zweck oder Ansatz dieser Familien zur Erfüllung der Sicherheitszielsetzungen. Die Definition der Funktionsklassen spiegelt keinerlei formale Taxonomien in der Spezifikation der Anforderungen wider.

Die Klasseneinleitung umfasst ein Bild mit der Beschreibung der Familien dieser Klasse und der Komponentenhierarchie in jeder Familie entsprechend der Erklärungen in 7.2.

7.1.3 Familienstruktur

7.1.3.1 Allgemeines

Bild 4 stellt die Struktur der Funktionsfamilien schematisch dar.

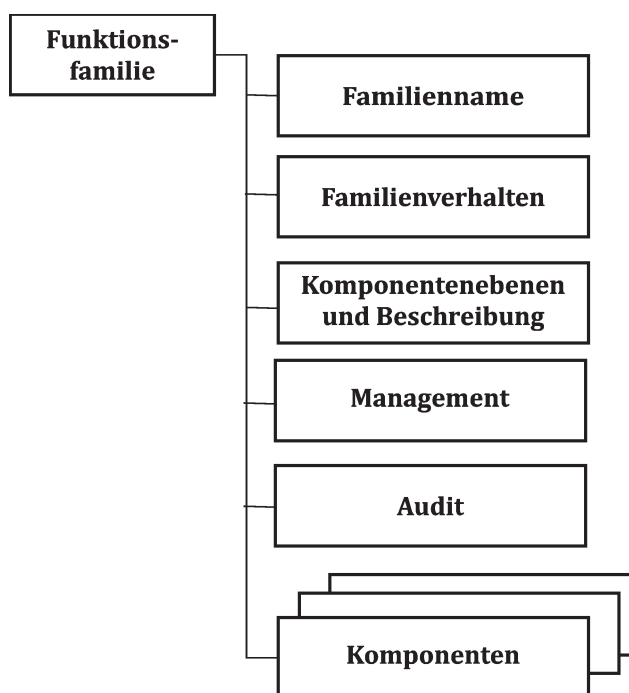


Bild 4 — Struktur der Funktionsfamilien

7.1.3.2 Familienname

Der Unterabschnitt Familienname liefert kategorische und beschreibende Informationen zum Identifizieren und Einstufen einer Funktionsfamilie. Jede Funktionsfamilie hat einen eindeutigen Namen. Die Information zur Einstufung besteht aus einem Kurznamen mit sieben Zeichen, wobei die ersten drei Zeichen dem Kurznamen der Klasse entsprechen, gefolgt von einem Unterstrich und dem Kurznamen der Familie wie folgt: XXX_YYY. Die eindeutige Kurzform des Familiennamens liefert den Hauptreferenznamen der Sicherheitskomponenten.

7.1.3.3 Familienverhalten

Der Unterabschnitt über das Familienverhalten liefert die ausformulierte Beschreibung der Funktionsfamilie mit Angabe der Sicherheitszielsetzungen und einer allgemeinen Beschreibung der Funktionsanforderungen. Diese werden im Folgenden ausführlicher beschrieben:

- a) Die Sicherheitszielsetzungen der Familie behandeln ein Sicherheitsproblem, das mithilfe eines TOEs gelöst werden kann, der von einer Komponente dieser Familie abgeleitete SFRs enthält;
- b) die Beschreibung der *Funktionsanforderungen* fasst alle in dieser Komponente (bzw. in diesen Komponenten) enthaltenen Anforderungen zusammen. Die Beschreibung richtet sich an Autoren von ST, PP, PP-Modulen oder Sicherheitsfunktionspaketen, die bewerten möchten, ob die Familie für ihre spezifischen Anforderungen relevant ist.

7.1.3.4 Komponentenebenen und Beschreibung

Funktionsfamilien enthalten eine oder mehrere Komponenten, von denen jede zur Einbindung in ST, PP, PP-Module oder Sicherheitsfunktionspakete ausgewählt werden darf. Das Ziel des Unterabschnitts über die Komponentenebenen und der Beschreibung ist die Bereitstellung von Informationen für Benutzer zur Auswahl passender Funktionskomponenten, sobald die Familie als erforderlicher oder sinnvoller Teil ihrer Sicherheitsanforderungen identifiziert wurde.

Die Beschreibung von Funktionsfamilien beschreibt die verfügbaren Komponenten und ihre Begründung. Die genauen Einzelheiten der Komponenten sind in jeder Komponente enthalten.

Die Beziehungen zwischen Komponenten in einer Funktionsfamilie können hierarchisch sein. Eine Komponente ist hierarchisch zu einer anderen, wenn sie eine höhere Sicherheit bietet.

Die Beschreibungen der Familien bieten, wie in 7.2 erklärt, eine grafische Übersicht der Komponentenhierarchie in einer Familie.

7.1.3.5 Management

Die Unterabschnitte Management enthalten Informationen für die Autoren von ST, PP, PP-Modulen oder Sicherheitsfunktionspaketen, die bei Managementaktivitäten zu einer bestimmten Komponente zu beachten sind. Die Abschnitte verweisen auf Komponenten der Klasse Management (FMT) und bieten Leitlinien für potentielle Managementaktivitäten, die durch Operationen an diesen Komponenten angewendet werden dürfen.

Ein Autor darf die angezeigten Managementkomponenten auswählen oder andere, nicht aufgeführte Managementanforderungen zur Ausgestaltung der Managementaktivitäten einbinden. Von daher sollten diese Informationen als informativ betrachtet werden.

7.1.3.6 Audit

Die Unterabschnitte für Anforderungen zum Audit enthalten auditierfähige Ereignisse zur Auswahl durch die Autoren, wenn Anforderungen der Klasse FAU in dem/der ST, PP, PP-Modul oder Sicherheitsfunktionspaket enthalten sind. Diese Anforderungen enthalten sicherheitsrelevante Ereignisse in Bezug auf die verschiedenen Detailebenen, die durch die Komponenten der Familie „Security audit data generation“ (FAU_GEN) unterstützt werden.

Es kann beobachtet werden, dass die Einstufung von auditierfähigen Ereignissen hierarchisch ist.

BEISPIEL 1 Eine Auditanmerkung kann folgende Aktionen enthalten:

- minimal: erfolgreiche Verwendung des Sicherheitsmechanismus;
- einfach: jede Verwendung des Sicherheitsmechanismus sowie relevante Informationen zu den beteiligten Sicherheitsattributen;

- detailliert: jede am Mechanismus durchgeführte Konfigurationsänderung einschließlich der Konfigurationsistwerte vor und nach der Änderung.

BEISPIEL 2 Wenn einfache Auditgenerierung erforderlich ist, werden alle als minimal und zugleich einfach identifizierten auditierfähigen Ereignisse über die entsprechende Zuweisungsoperation in das PP, PP-Modul, Funktionspaket oder in die ST eingebunden; ausgenommen, wenn die höhere Ebene lediglich mehr Details als die niedrigere Ebene bereitstellt. Wenn detaillierte Auditgenerierung erforderlich ist, werden alle auditierfähigen Ereignisse (minimal, einfach und detailliert) in das PP, PP-Modul, Funktionspaket oder in die ST eingebunden.

In der Klasse FAU werden die Regeln zum Steuern des Audits ausführlicher erklärt.

7.1.4 Komponentenstruktur

7.1.4.1 Allgemeines

Bild 5 stellt die Struktur der Funktionskomponenten dar.

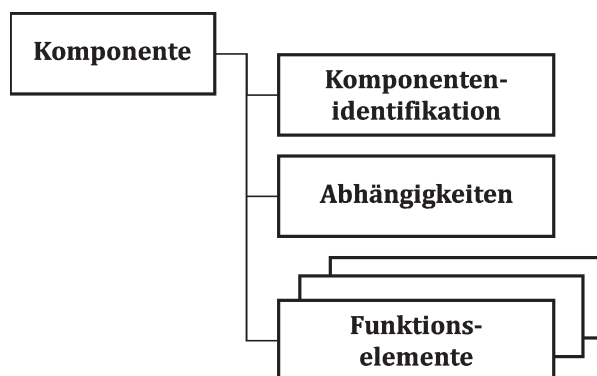


Bild 5 — Struktur der Funktionskomponenten

7.1.4.2 Komponentenidentifikation

Der/Die Unterabschnitt(e) Komponentenidentifikation liefert/liefern beschreibende Informationen, die zur Identifizierung, Einstufung, Registrierung und Querverweisung einer Komponente erforderlich sind. Folgendes wird als Teil jeder Funktionskomponente bereitgestellt:

- ein *eindeutiger Name*. Der Name spiegelt den Zweck der Komponente wider;
- ein *eindeutiger Kurzname*. Eine eindeutige Kurzform des Namens der Funktionskomponente. Dieser Kurzname dient als Hauptreferenzname zur Einstufung, Registrierung und Querverweisung der Komponente. Dieser Kurzname spiegelt die zugehörige Klasse und Familie der Komponente und die Komponentenummer innerhalb der Familie wider;
- eine *hierarchisch-zu-Liste*. Eine Liste anderer Komponenten, zu denen diese Komponente in einer hierarchischen Beziehung steht, und für die diese Komponente verwendet werden kann, Abhängigkeiten zu den aufgeführten Komponenten zu erfüllen.

7.1.4.3 Funktionselemente

Für jede Komponente wird eine Reihe von Elementen bereitgestellt. Jedes Element ist einzeln definiert und eigenständig.

Beim Aufbau von Paketen, PPs und/oder STs ist die Auswahl von nur einem oder mehreren Elementen einer Komponente nicht zulässig. Für die Einbindung in ein PP, PP-Modul, ein Sicherheitsfunktionspaket oder eine ST muss stets die gesamte Reihe von Elementen einer Komponente ausgewählt werden.

Es wird eine eindeutige Kurzform des Namens des Funktionselements bereitgestellt.

BEISPIEL Der Komponentennamen FDP_IFF.4.2 ist wie folgt zu interpretieren:

- F: Funktionsanforderung;
- DP: Klasse „User data protection“;
- _IFF: Familie „Information flow control functions“;
- .4: 4. Komponente namens „Partial elimination of illicit information flows“;
- .2: 2. Element der Komponente.

7.1.4.4 Abhängigkeiten

Wenn eine Komponente für sich genommen nicht ausreichend ist und auf das Vorhandensein oder die Interaktion mit einer anderen Komponente angewiesen ist, um selbst korrekt zu funktionieren, entstehen Abhängigkeiten zwischen Funktionskomponenten.

Jede Funktionskomponente bietet eine vollständige Liste der Abhängigkeiten von anderen Funktions- und Sicherheitskomponenten. Einige Komponenten können auch „keine Abhängigkeiten“ auflisten. Die Komponenten, zu denen Abhängigkeiten bestehen, können wiederum selbst Abhängigkeiten zu anderen Komponenten haben. Bei der Liste der Komponenten handelt es sich um die direkten Abhängigkeiten, d. h., es gibt nur Verweisungen zu den für die korrekte Aufgabenausführung dieser Komponente erforderlichen anderen Funktionskomponenten. Die indirekten Abhängigkeiten, also die aus den Abhängigkeiten anderer Komponenten entstehenden Abhängigkeiten, werden in Anhang B dieses Dokuments aufgeführt. Es wird darauf hingewiesen, dass die Abhängigkeit in einigen Fällen insofern optional ist, dass mehrere Funktionskomponenten bereitgestellt werden, bei denen jede einzelne zur Erfüllung der Abhängigkeit ausreichen würde.

BEISPIEL FDP_UIT.1 „Data exchange integrity“.

Die Abhängigkeitsliste bestimmt die minimal erforderlichen Funktions- oder Sicherheitskomponenten zur Erfüllung der mit einer identifizierten Komponente verknüpften Sicherheitsanforderungen. Zur Erfüllung der Abhängigkeit dürfen auch Komponenten verwendet werden, die hierarchisch zur identifizierten Komponente sind.

Die in diesem Dokument angegebenen Abhängigkeiten sind normativ und müssen innerhalb eines Pakets, PP oder einer ST erfüllt werden. In Situationen, in denen die angegebenen Abhängigkeiten nicht anwendbar sind, muss der Autor die Abhängigkeit erfüllen, indem er begründet, warum sie nicht anwendbar ist, und er darf die abhängige Komponente aus dem Paket, PP oder der ST unberücksichtigt lassen.

7.2 Komponentenkatalog

Die Gruppierung von Komponenten in diesem Dokument stellt keinerlei formale Taxonomie dar.

Dieses Dokument enthält Klassen von Familien und Komponenten, die auf der Grundlage zusammenhängender Funktionen oder Zwecke grob gruppiert und in alphabetischer Reihenfolge dargestellt werden. Am Anfang jeder Klasse gibt es ein informatives Bild, das die Taxonomie jeder Klasse mit Darstellung der Familien jeder Klasse und den Komponenten jeder Familie aufzeigt. Bild 6 ist ein sinnvoller Indikator der hierarchischen Beziehung, die zwischen den Komponenten bestehen kann.

In der Beschreibung der Funktionskomponenten werden durch einen Unterabschnitt die Abhängigkeiten zwischen der Komponente und anderen Komponenten identifiziert.

In jeder Klasse beschreibt ein Bild ähnlich dem Bild 6 die Hierarchie der Familie. Im Bild 6 enthält die erste Familie, Familie 1, drei hierarchische Komponenten, wobei Komponente 2 und Komponente 3 beide zur Erfül-

lung der Abhängigkeiten zu Komponente 1 verwendet werden können. Komponente 3 ist hierarchisch zu Komponente 2 und kann auch zur Erfüllung der Abhängigkeiten zu Komponente 2 verwendet werden.

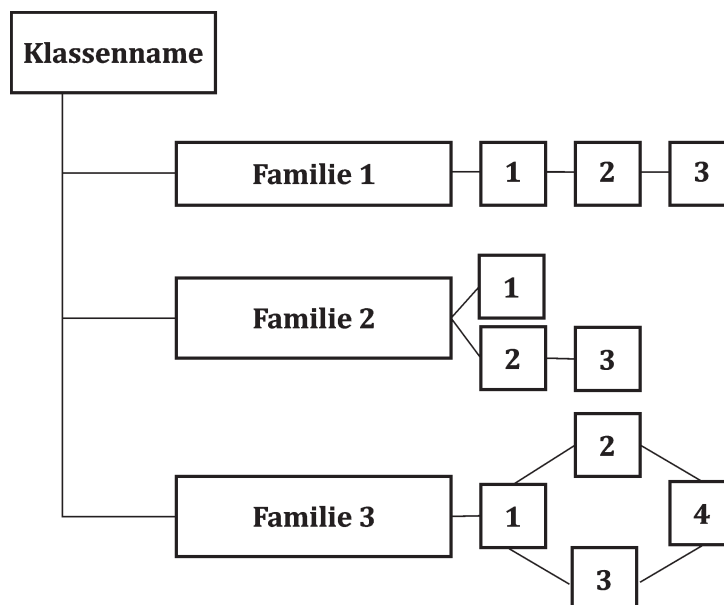


Bild 6 — Muster eines Klassenaufbaudiagramms

In Familie 2 gibt es drei Komponenten, die nicht alle hierarchisch sind. Die Komponenten 1 und 2 sind zu keiner anderen Komponente hierarchisch. Komponente 3 ist hierarchisch zu Komponente 2 und kann auch zur Erfüllung der Abhängigkeiten zu Komponente 2 verwendet werden, aber nicht zur Erfüllung der Abhängigkeiten zu Komponente 1.

In Familie 3 sind die Komponenten 2, 3 und 4 hierarchisch zu Komponente 1. Die Komponenten 2 und 3 sind beide hierarchisch zu Komponente 1, aber nicht vergleichbar. Komponente 4 ist hierarchisch zu den Komponenten 2 und 3.

Diese Diagramme sind als Ergänzung des Textes zu den Familien gedacht und erleichtern die Identifizierung von Beziehungen. Sie ersetzen nicht die Anmerkung „Hierarchisch zu:“ jeder Komponente, die einen verpflichtenden Hierarchieanspruch für jede Komponente darstellt.

8 Klasse FAU: Sicherheitsaudit

8.1 Klassenbeschreibung

Sicherheitsaudits umfassen das Erkennen, Aufzeichnen, Speichern und Analysieren von Informationen zu sicherheitsrelevanten Aktivitäten (d. h. von der TSF gesteuerte Aktivitäten). Die sich daraus ergebenden Auditaufzeichnungen können untersucht werden, um zu ermitteln, welche sicherheitsrelevanten Aktivitäten stattgefunden haben und wer (welcher Benutzer) für sie verantwortlich ist.

Bild 7 zeigt den Aufbau dieser Klasse, ihrer Familien und Komponenten. Elemente sind in dem Bild nicht dargestellt.

Anhang C liefert Erklärungen zu dieser Klasse und sollte bei der Verwendung der in dieser Klasse ausgewiesenen Komponenten herangezogen werden.

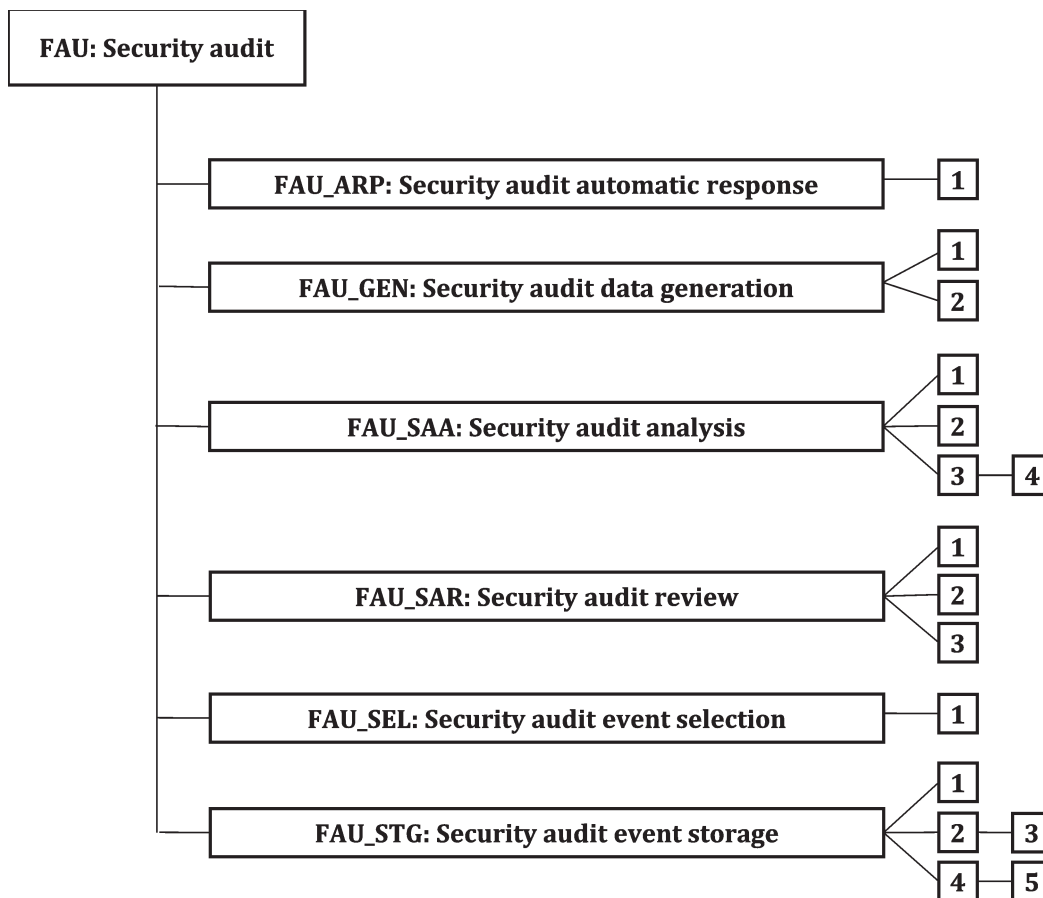


Bild 7 — FAU: Klassenaufbau Sicherheitsaudit

8.2 Automatische Antwort beim Sicherheitsaudit (FAU_ARP)

8.2.1 Familienverhalten

Diese Familie definiert die zu verwendende Antwort für den Fall, dass erkannte Ereignisse auf einen potentiellen Sicherheitsverstoß hindeuten.

8.2.2 Komponentenebenen und Beschreibung

Bild 8 zeigt die Komponentenebenen für diese Familie.



Bild 8 — FAU_ARP: Komponentenebenen

Bei „FAU_ARP.1 Security alarms“ muss die TSF Maßnahmen ergreifen für den Fall, dass ein potentieller Sicherheitsverstoß erkannt wurde.

8.2.3 Management von FAU_ARP.1

Die folgenden Aktionen können für die Managementfunktionen in FMT berücksichtigt werden:

- a) das Management (Hinzufügen, Entfernen oder Anpassung) von Aktionen.

8.2.4 Audit von FAU_ARP.1

Wenn „FAU_GEN Security audit data generation“ in das PP, PP-Modul, Funktionspaket, oder in die ST eingebunden ist, sollten folgende Aktionen auditierfähig sein:

- a) minimal: Aktionen aufgrund von potentiellen Sicherheitsverstößen.

8.2.5 FAU_ARP.1 Sicherheitsalarme

Komponentenbeziehungen

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_SAA.1 Potential violation analysis“

FAU_ARP.1.1

Die TSF muss beim Erkennen eines potentiellen Sicherheitsverstößes [Zuweisung: Liste der Aktionen] durchführen.

8.3 Datengenerierung beim Sicherheitsaudit (FAU_GEN)

8.3.1 Familienverhalten

Diese Familie definiert Anforderungen an die Aufzeichnung beim Eintreten von sicherheitsrelevanten Ereignissen, die unter TSF-Kontrolle erfolgen. Diese Familie identifiziert die Ebene des Audits, spezifiziert die Arten von Ereignissen, die durch die TSF auditierfähig sein müssen, und identifiziert den minimalen Satz an auditbezogenen Informationen, die von den verschiedenen Arten von Auditaufzeichnungen bereitgestellt werden sollten.

8.3.2 Komponentenebenen und Beschreibung

Bild 9 zeigt die Komponentenebenen für diese Familie.



Bild 9 — FAU_GEN: Komponentenebenen

„FAU_GEN.1 Audit data generation“ definiert die Ebene der auditierfähigen Ereignisse und spezifiziert die Datenliste, die in jeder Aufzeichnung aufgenommen werden muss.

In „FAU_GEN.2 User identity association“ muss die TSF auditierfähige Ereignisse mit einzelnen Benutzeridentitäten verknüpfen.

8.3.3 Management von FAU_GEN.1, FAU_GEN.2

Die folgenden Aktionen können für die Managementfunktionen in FMT berücksichtigt werden:

- a) Managementaktivitäten sind nicht vorgesehen.

8.3.4 Audit von FAU_GEN.1, FAU_GEN.2

Wenn „FAU_GEN Security audit data generation“ in das PP, PP-Modul, Funktionspaket, oder in die ST eingebunden ist, sollten folgende Aktionen auditierfähig sein:

- a) Auditierfähige Ereignisse sind nicht vorgesehen.

8.3.5 FAU_GEN.1 Generierung von Auditdaten

Komponentenbeziehungen

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FPT_STM.1 Reliable time stamps“

FAU_GEN.1.1

Die TSF muss in der Lage sein, Auditdaten zu folgenden auditierfähigen Ereignissen zu generieren:

- a) Einschaltung und Abschaltung der Auditfunktionen;
- b) alle auditierfähigen Ereignisse für [Auswahl, eine auswählen: *minimale, einfache, detaillierte, nicht spezifizierte*] Auditebene;
- c) [Zuweisung: andere spezifisch definierte auditierfähige Ereignisse].

FAU_GEN.1.2

Die TSF muss im Rahmen der Auditdaten mindestens folgende Informationen aufzeichnen:

- a) Datum und Uhrzeit des auditierfähigen Ereignisses, Ereignisart, Subjektidentität (falls zutreffend) und Ergebnis (Erfolg oder Scheitern) des Ereignisses;
- b) für jede auditierfähige Ereignisart auf der Grundlage der auditierfähigen Ereignisdefinitionen der in das PP, PP-Modul, Funktionspaket oder die ST eingebundenen Funktionskomponenten, [Zuweisung: *andere auditrelevante Informationen*].

8.3.6 FAU_GEN.2 Verknüpfung der Benutzeridentität

Komponentenbeziehungen

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_GEN.1 Audit data generation“

„FIA_UID.1 Timing of identification“

FAU_GEN.2.1

Für Auditereignisse, die aus Aktionen identifizierter Benutzer resultieren, muss die TSF in der Lage sein, jedes auditierfähige Ereignis mit der Identität des Benutzers zu verknüpfen, der das Ereignis ausgelöst hat.

8.4 Sicherheitsauditanalyse (FAU_SAA)

8.4.1 Familienverhalten

Diese Familie definiert Anforderungen an automatisierte Mittel, die Systemaktivitäten und Auditdaten analysieren und auf mögliche oder reale Sicherheitsverstöße prüfen. Diese Analyse kann zur Unterstützung bei der Angriffserkennung oder der automatischen Antwort auf einen potentiellen Sicherheitsverstoß eingesetzt werden.

Die auf der Grundlage der Erkennung zu ergreifenden Aktionen können auf Wunsch über die Familie „Security audit automatic response“ (FAU_ARP) festgelegt werden.

8.4.2 Komponentenebenen und Beschreibung

Bild 10 zeigt die Komponentenebenen für diese Familie.

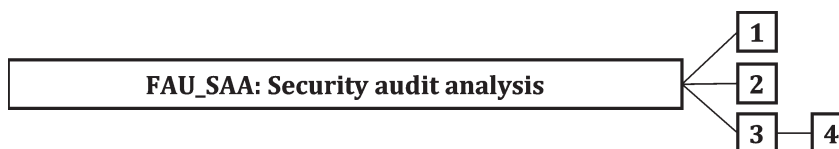


Bild 10 — FAU_SAA: Komponentenebenen

Bei „FAU_SAA.1 Potential violation analysis“ ist grundsätzliche Schwellwerterkennung auf der Grundlage eines festen Satzes von Regeln erforderlich.

Bei „FAU_SAA.2 Profile based anomaly detection“ enthält die TSF einzelne Profile zur Systemverwendung, wobei ein Profil die historischen Verwendungsmuster repräsentiert, die von Mitgliedern der Profilzielgruppe durchgeführt wurden. Eine Profilzielgruppe bezieht sich auf eine Gruppe von einer oder mehreren mit der TSF interagierenden Einzelpersonen. Jedes Mitglied einer Profilzielgruppe bekommt eine individuelle Verdachtswertung, die darstellt, wie gut die aktuelle Aktivität des Mitglieds mit den bekannten Verwendungsmustern im Profil übereinstimmt. Diese Analyse kann zur Laufzeit ausgeführt werden oder bei einer nachgelagerten Analyse im Batch-Modus.

Bei „FAU_SAA.3 Simple attack heuristics“ muss die TSF in der Lage sein, das Eintreten von Schlüsselereignissen zu erkennen, die eine wesentliche Bedrohung für die Durchsetzung der SFRs darstellen. Diese Suche nach Schlüsselereignissen kann in Echtzeit ablaufen oder bei einer nachgelagerten Analyse im Batch-Modus.

Bei „FAU_SAA.4 Complex attack heuristics“ muss die TSF in der Lage sein, mehrstufige Angriffsszenarien darzustellen und zu erkennen. Die TSF ist in der Lage, (möglicherweise von mehreren Einzelpersonen ausgeführte) Systemereignisse mit Ereignisabfolgen zu vergleichen, die als Gesamtangriffsszenarien bekannt sind. Die TSF muss in der Lage sein anzuzeigen, wenn ein Schlüsselereignis oder eine Ereignisabfolge gefunden wurde, die auf einen potentiellen Verstoß bei der Durchsetzung der SFRs hindeutet.

8.4.3 Management von FAU_SAA.1

Die folgenden Aktionen können für die Managementfunktionen in FMT berücksichtigt werden:

- a) Pflege der Regeln durch (Hinzufügen, Anpassen, Löschen) von Regeln aus dem Regelwerk.

8.4.4 Management von FAU_SAA.2

Die folgenden Aktionen können für die Managementfunktionen in FMT berücksichtigt werden:

- a) Pflege (Löschen, Anpassen, Hinzufügen) von Benutzergruppen in den Profilzielgruppen.

8.4.5 Management von FAU_SAA.3

Die folgenden Aktionen können für die Managementfunktionen in FMT berücksichtigt werden:

- a) Pflege (Löschen, Anpassen, Hinzufügen) der Teilmenge von Systemereignissen.

8.4.6 Management von FAU_SAA.4

Die folgenden Aktionen können für die Managementfunktionen in FMT berücksichtigt werden:

- a) Pflege (Löschen, Anpassen, Hinzufügen) der Teilmenge von Systemereignissen;
- b) Pflege (Löschen, Anpassen, Hinzufügen) der Menge von Systemereignisabfolgen.

8.4.7 Audit von FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4

Wenn „FAU_GEN Security audit data generation“ in das PP, PP-Modul, Funktionspaket, oder in die ST eingebunden ist, sollten folgende Aktionen auditierfähig sein:

- a) minimal: Aktivieren und Deaktivieren eines der Analysemechanismen;
- b) minimal: vom Tool automatisch ausgeführte Antworten.

8.4.8 „FAU_SAA.1 Potential violation analysis“

Komponentenbeziehungen

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_GEN.1 Audit data generation“

FAU_SAA.1.1

Die TSF muss in der Lage sein, bei der Überwachung der auditierten Ereignisse einen Regelsatz anzuwenden, und auf dessen Grundlage auf einen potentiellen Verstoß bei der Durchsetzung der SFRs hinzuweisen.

FAU_SAA.1.2

Die TSF muss folgende Regeln für die Überwachung auditierter Ereignisse durchsetzen:

- a) Akkumulation oder Kombination von [Zuweisung: *Teilmenge der definierten auditierfähigen Ereignisse*], von denen bekannt ist, dass sie auf einen potentiellen Sicherheitsverstoß hinweisen;
- b) [Zuweisung: *jede andere Regel*].

8.4.9 FAU_SAA.2 Profilbasierte Erkennung von Anomalien

Komponentenbeziehungen

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FIA_UID.1 Timing of identification“

FAU_SAA.2.1

Die TSF muss in der Lage sein, Profile der Systemverwendung zu pflegen, wobei ein einzelnes Profil den historischen Verwendungsmustern von Mitgliedern der [Zuweisung: *Profilzielgruppe*] entspricht.

FAU_SAA.2.2

Die TSF muss in der Lage sein, eine Verdachtswertung zu pflegen, die mit jedem Benutzer, dessen Aktivität in einem Profil aufgezeichnet wird, verknüpft ist, wobei diese Verdachtswertung darstellt, wie stark die aktuelle Aktivität des Benutzers als unvereinbar mit den im Profil dargestellten etablierten Nutzungsmustern angesehen wird.

FAU_SAA.2.3

Die TSF muss in der Lage sein, einen möglichen Verstoß bei der Durchsetzung der SFRs anzuzeigen, wenn die Verdachtswertung eines Benutzers die folgenden Schwellwertbedingungen überschreitet [Zuweisung: *Bedingungen, bei denen von der TSF eine anomale Aktivität berichtet wird*].

8.4.10 FAU_SAA.3 Einfache Angriffsheuristiken

Komponentenbeziehungen

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: keine Abhängigkeiten.

FAU_SAA.3.1

Die TSF muss in der Lage sein, eine interne Darstellung folgender Schlüsselereignisse [Zuweisung: *eine Teilmenge an Systemereignissen*] zu pflegen, die möglicherweise auf einen Verstoß bei der Durchsetzung der SFRs hindeuten.

FAU_SAA.3.2

Die TSF muss in der Lage sein, Schlüsselereignisse mit den aufgezeichneten, bei einer Untersuchung von [Zuweisung: *die zur Bestimmung der Systemaktivität zu verwendende Information*] erkennbaren Systemaktivitäten zu vergleichen.

FAU_SAA.3.3

Die TSF muss in der Lage sein, einen potentiellen Verstoß bei der Durchsetzung der SFRs anzuzeigen, wenn ein Systemereignis gefunden wurde, das mit einem Schlüsselereignis für einen potentiellen Verstoß bei der Durchsetzung der SFRs übereinstimmt.

8.4.11 FAU_SAA.4 Komplexe Angriffsheuristiken

Komponentenbeziehungen

Hierarchisch zu: „FAU_SAA.3 Simple attack heuristics“

Abhängigkeiten: keine Abhängigkeiten.

FAU_SAA.4.1

Die TSF muss in der Lage sein, eine interne Darstellung folgender **Ereignisabfolgen bekannter Angriffsszenarien** [Zuweisung: *Liste von Abfolgen von Systemereignissen, deren Auftreten für bekannte Penetrationsszenarien repräsentativ ist*] und der folgenden Schlüsselereignisse [Zuweisung: *eine Teilmenge an Systemereignissen*] zu pflegen, die möglicherweise auf einen **potentiellen** Verstoß bei der Durchsetzung der SFRs hindeuten.

FAU_SAA.4.2

Die TSF muss in der Lage sein, Schlüsselereignisse **und Ereignisabfolgen** mit den aufgezeichneten, bei einer Untersuchung von [Zuweisung: *die zur Bestimmung der Systemaktivität zu verwendende Information*] erkennbaren Systemaktivitäten zu vergleichen.

FAU_SAA.4.3

Die TSF muss in der Lage sein, einen potentiellen Verstoß bei der Durchsetzung der SFRs anzuzeigen, wenn eine System**aktivität** gefunden wurde, die mit einem Schlüsselereignis **oder einer Ereignisabfolge** für einen potentiellen Verstoß bei der Durchsetzung der SFRs übereinstimmt.

8.5 Sicherheitsauditüberprüfung (FAU_SAR)

8.5.1 Familienverhalten

Diese Familie definiert die Anforderungen an Tools, die für autorisierte Benutzer zur Unterstützung bei der Überprüfung von Auditdaten verfügbar gemacht werden.

8.5.2 Komponentenebenen und Beschreibung

Bild 11 zeigt die Komponentenebenen für diese Familie.



Bild 11 — FAU_SAR: Komponentenebenen

„FAU_SAR.1 Audit review“ bietet die Möglichkeit zum Lesen von Informationen aus Auditdaten.

„FAU_SAR.2 Restricted audit review“ erfordert, dass, außer den in „FAU_SAR.1 Audit review“ identifizierten Benutzern, keine weiteren Benutzer die Informationen lesen können.

„FAU_SAR.3 Selectable audit review“ erfordert Tools zur Auditüberprüfung, um die zu überprüfenden Auditdaten auf der Grundlage von Kriterien auszuwählen.

8.5.3 Management von FAU_SAR.1

Die folgenden Aktionen können für die Managementfunktionen in FMT berücksichtigt werden:

- a) Pflege (Löschen, Anpassen, Hinzufügen) von Benutzergruppen mit Lesezugriffsrechten auf die Auditaufzeichnungen.

8.5.4 Management von FAU_SAR.2, FAU_SAR.3

Die folgenden Aktionen können für die Managementfunktionen in FMT berücksichtigt werden:

- a) Managementaktivitäten sind nicht vorgesehen.

8.5.5 Audit von FAU_SAR.1

Wenn „FAU_GEN Security audit data generation“ in das PP, PP-Modul, Funktionspaket, oder in die ST eingebunden ist, sollten folgende Aktionen auditierfähig sein:

- a) einfach: Lesen von Informationen aus den Auditaufzeichnungen.

8.5.6 Audit von FAU_SAR.2

Wenn „FAU_GEN Security audit data generation“ in das PP, PP-Modul, Funktionspaket, oder in die ST eingebunden ist, sollten folgende Aktionen auditierfähig sein: