

	DIN EN ISO/IEC 15408-3	
ICS 35.030	<div>Entwurf</div>	Einsprüche bis 2024-04-16 Vorgesehen als Ersatz für DIN EN ISO/IEC 15408-3:2021-06
<p>Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Evaluationskriterien für IT-Sicherheit – Teil 3: Sicherheit Gewährleistungskomponenten (ISO/IEC 15408-3:2022); Deutsche und Englische Fassung EN ISO/IEC 15408-3:2023</p> <p>Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components (ISO/IEC 15408-3:2022); German and English version EN ISO/IEC 15408-3:2023</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 3: Composants d’assurance de sécurité (ISO/IEC 15408-3:2022); Version allemande et anglaise EN ISO/IEC 15408-3:2023</p> <p>Anwendungswarnvermerk</p> <p>Dieser Entwurf mit Erscheinungsdatum 2024-02-16 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 431 Seiten</p> <p>DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)</p>		

Nationales Vorwort

Der Text von ISO/IEC 15408-3:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 15408-3:2023 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 10007:2017	siehe	DIN ISO 10007:2020-10
ISO/IEC 18045:2022	siehe	DIN EN ISO/IEC 18045:2021-02

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 15408-3:2021-06 wurden folgende Änderungen vorgenommen:

- a) Terminologie überprüft und aktualisiert;
- b) genauer Konformitätstyp eingeführt;
- c) Schutzprofile (PPs) mit geringer Sicherheit entfernt und PPs mit direkter Begründung eingeführt;
- d) PP-Module und PP-Konfigurationen für modulare Evaluierungen eingeführt;
- e) Mehrfachsicherungsbewertung eingeführt;
- f) redaktionelle Überarbeitung des Dokuments.

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO/IEC 18045:2021-02, *Informationstechnik — Sicherheitstechniken — Methodik für die Bewertung der IT-Sicherheit (ISO/IEC 18045:2008)*; Deutsche Fassung EN ISO/IEC 18045:2020, nur auf CD-ROM

DIN ISO 10007:2020-10, *Qualitätsmanagement — Leitfaden für Konfigurationsmanagement (ISO 10007:2017)*

– *Entwurf* –

E DIN EN ISO/IEC 15408-3:2024-03

– Leerseite –

**Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre –
Evaluationskriterien für IT-Sicherheit – Teil 3: Sicherheit
Gewährleistungskomponenten (ISO/IEC 15408-3:2022)**

Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components (ISO/IEC 15408-3:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée – Critères d'évaluation pour la sécurité des technologies de l'information – Partie 3: Composants d'assurance de sécurité (ISO/IEC 15408-3:2022)

Inhalt

	Seite
Europäisches Vorwort	10
Vorwort	11
Einleitung	14
1 Anwendungsbereich	15
2 Normative Verweisungen	15
3 Begriffe	15
4 Übersicht	20
5 Paradigma für Vertrauenswürdigkeit	20
5.1 Allgemeines	20
5.2 Ansatz der Normenreihe ISO/IEC 15408	20
5.3 Ansatz für Vertrauenswürdigkeit	21
5.3.1 Allgemeines	21
5.3.2 Bedeutung von Anfälligkeiten	21
5.3.3 Ursachen von Anfälligkeiten	21
5.3.4 Vertrauenswürdigkeit der Normenreihe ISO/IEC 15408	22
5.3.5 Vertrauenswürdigkeit durch Evaluierung	22
5.4 Vertrauenswürdigkeitsskala der Normenreihe ISO/IEC 15408	23
6 Vertrauenswürdigkeitskomponenten	23
6.1 Allgemeines	23
6.2 Struktur der Vertrauenswürdigkeitsklassen	23
6.2.1 Allgemeines	23
6.2.2 Klassenname	23
6.2.3 Klasseneinleitung	23
6.2.4 Vertrauenswürdigkeitsfamilien	23
6.3 Struktur der Vertrauenswürdigkeitsfamilien	24
6.3.1 Familienname	24
6.3.2 Ziele	24
6.3.3 Komponentenebenen	25
6.3.4 Anwendungshinweise	25
6.3.5 Vertrauenswürdigkeitskomponenten	25
6.4 Struktur der Vertrauenswürdigkeitskomponenten	25
6.4.1 Allgemeines	25
6.4.2 Komponentenidentifikation	26
6.4.3 Ziele	26
6.4.4 Anwendungshinweise	26
6.4.5 Abhängigkeiten	26
6.4.6 Vertrauenswürdigkeitselemente	26
6.5 Vertrauenswürdigkeitselemente	27
6.6 Komponententaxonomie	27
7 Klasse APE: Evaluierung des Schutzprofils (PP)	28
7.1 Allgemeines	28
7.2 PP-Einleitung (APE_INT)	28
7.2.1 Ziele	28
7.2.2 APE_INT.1 PP-Einleitung	28
7.3 Konformitätsansprüche (APE_CCL)	29
7.3.1 Ziele	29
7.3.2 APE_CCL.1 Konformitätsansprüche	29
7.4 Sicherheitsproblemdefinition (APE_SPD)	31
7.4.1 Ziele	31
7.4.2 APE_SPD.1 Sicherheitsproblemdefinition	32
7.5 Sicherheitszielsetzungen (APE_OBJ)	32

7.5.1	Ziele	32
7.5.2	Komponentenebenen	32
7.5.3	APE_OBJ.1 Sicherheitszielsetzungen für die Betriebsumgebung	32
7.5.4	APE_OBJ.2 Sicherheitszielsetzungen	33
7.6	Erweiterte Komponentendefinition (APE_ECD)	34
7.6.1	Ziele	34
7.6.2	APE_ECD.1 Erweiterte Komponentendefinition	34
7.7	Sicherheitsanforderungen (APE_REQ)	35
7.7.1	Ziele	35
7.7.2	Komponentenebenen	36
7.7.3	APE_REQ.1 Sicherheitsanforderungen des PP-Moduls mit direkter Begründung	36
7.7.4	APE_REQ.2 Abgeleitete Sicherheitsanforderungen	37
8	Klasse ACE: Evaluierung der Schutzprofilkonfiguration	38
8.1	Allgemeines	38
8.2	Einleitung für PP-Module (ACE_INT)	39
8.2.1	Ziele	39
8.2.2	ACE_INT.1 Einleitung für PP-Module	39
8.3	Konformitätsansprüche des PP-Moduls (ACE_CCL)	40
8.3.1	Ziele	40
8.3.2	ACE_CCL.1 Konformitätsansprüche des PP-Moduls	40
8.4	Sicherheitsproblemdefinition des PP-Moduls (ACE_SPD)	42
8.4.1	Ziele	42
8.4.2	ACE_SPD.1 Sicherheitsproblemdefinition des PP-Moduls	42
8.5	Sicherheitszielsetzungen des PP-Moduls (ACE_OBJ)	43
8.5.1	Ziele	43
8.5.2	Komponentenebenen	43
8.5.3	ACE_OBJ.1 Sicherheitszielsetzungen des PP-Moduls für die Betriebsumgebung	43
8.5.4	ACE_OBJ.2 Sicherheitszielsetzungen des PP-Moduls	44
8.6	Erweiterte Komponentendefinition des PP-Moduls (ACE_ECD)	45
8.6.1	Ziele	45
8.6.2	ACE_ECD.1 Erweiterte Komponentendefinition des PP-Moduls	45
8.7	Sicherheitsanforderungen des PP-Moduls (ACE_REQ)	46
8.7.1	Ziele	46
8.7.2	Komponentenebenen	46
8.7.3	ACE_REQ.1 Festgelegte Sicherheitsanforderungen des PP-Moduls	46
8.7.4	ACE_REQ.2 Abgeleitete Sicherheitsanforderungen des PP-Moduls	48
8.8	Konsistenz des PP-Moduls (ACE_MCO)	49
8.8.1	Ziele	49
8.8.2	ACE_MCO.1 Konsistenz des PP-Moduls	49
8.9	Konsistenz der PP-Konfiguration (ACE_CCO)	50
8.9.1	Ziele	50
8.9.2	ACE_CCO.1 Konsistenz der PP-Konfiguration	51
9	Klasse ASE: Evaluierung der Sicherheitsvorgabe (ST)	54
9.1	Allgemeines	54
9.2	ST-Einleitung (ASE_INT)	55
9.2.1	Ziele	55
9.2.2	ASE_INT.1 ST-Einleitung	55
9.3	Konformitätsansprüche (ASE_CCL)	56
9.3.1	Ziele	56
9.3.2	ASE_CCL.1 Konformitätsansprüche	56
9.4	Sicherheitsproblemdefinition (ASE_SPD)	58
9.4.1	Ziele	58
9.4.2	ASE_SPD.1 Sicherheitsproblemdefinition	59
9.5	Sicherheitszielsetzungen (ASE_OBJ)	59
9.5.1	Ziele	59
9.5.2	Komponentenebenen	59
9.5.3	ASE_OBJ.1 Sicherheitszielsetzungen für die Betriebsumgebung	59

9.5.4	ASE_OBJ.2 Sicherheitszielsetzungen	60
9.6	Erweiterte Komponentendefinition (ASE_ECD)	61
9.6.1	Ziele	61
9.6.2	ASE_ECD.1 Erweiterte Komponentendefinition	61
9.7	Sicherheitsanforderungen (ASE_REQ)	62
9.7.1	Ziele	62
9.7.2	Komponentenebenen	63
9.7.3	ASE_REQ.1 Direkte Begründung für die Sicherheitsanforderungen	63
9.7.4	ASE_REQ.2 Abgeleitete Sicherheitsanforderungen	64
9.8	Zusammenfassende Spezifikation des TOE (ASE_TSS)	66
9.8.1	Ziele	66
9.8.2	Komponentenebenen	66
9.8.3	ASE_TSS.1 Zusammenfassende Spezifikation des TOE	66
9.8.4	ASE_TSS.2 Zusammenfassende Spezifikation des TOE mit zusammenfassendem Architekturdesign	67
9.9	Konsistenz der Sicherheitsvorgaben des Verbundprodukts (ASE_COMP)	68
9.9.1	Ziele	68
9.9.2	Komponentenebenen	68
9.9.3	Anwendungshinweise	68
9.9.4	ASE_COMP.1 Konsistenz der Sicherheitsvorgabe (ST)	69
10	Klasse ADV: Entwicklung	70
10.1	Allgemeines	70
10.2	Sicherheitsarchitektur (ADV_ARC)	74
10.2.1	Ziele	74
10.2.2	Komponentenebenen	75
10.2.3	Anwendungshinweise	75
10.2.4	ADV_ARC.1 Beschreibung der Sicherheitsarchitektur	75
10.3	Funktionsspezifikation (ADV_FSP)	76
10.3.1	Ziele	76
10.3.2	Komponentenebenen	77
10.3.3	Anwendungshinweise	77
10.3.4	ADV_FSP.1 Grundlegende Funktionsanforderungen	79
10.3.5	ADV_FSP.2 Sicherheit durchsetzende Funktionsspezifikation	80
10.3.6	ADV_FSP.3 Funktionsspezifikation mit vollständiger Zusammenfassung	81
10.3.7	ADV_FSP.4 Vollständige Funktionsspezifikation	82
10.3.8	ADV_FSP.5 Vollständige semiformale Funktionsspezifikation mit zusätzlichen Fehlerinformationen	83
10.3.9	ADV_FSP.6 Vollständige semiformale Funktionsspezifikation mit zusätzlicher formaler Spezifikation	85
10.4	Darstellung der Implementierung (ADV_IMP)	86
10.4.1	Ziele	86
10.4.2	Komponentenebenen	86
10.4.3	Anwendungshinweise	86
10.4.4	ADV_IMP.1 Darstellung der Implementierung der TSF	87
10.4.5	ADV_IMP.2 Vollständige Zuordnung der Darstellung der Implementierung der TSF	88
10.5	TSF-Interna (ADV_INT)	89
10.5.1	Ziele	89
10.5.2	Komponentenebenen	89
10.5.3	Anwendungshinweise	89
10.5.4	ADV_INT.1 Wohlstrukturierte Teilmengen von TSF-Interna	90
10.5.5	ADV_INT.2 Wohlstrukturierte Interna	91
10.5.6	ADV_INT.3 Minimal komplexe Interna	92
10.6	Modellierung der Sicherheitspolitik (ADV_SPM)	93
10.6.1	Ziele	93
10.6.2	Komponentenebenen	93
10.6.3	Anwendungshinweise	93
10.6.4	ADV_SPM.1 Formales TOE-Sicherheitspolitikmodell	94

10.7	TOE-Design (ADV_TDS)	95
10.7.1	Ziele	95
10.7.2	Komponentenebenen	96
10.7.3	Anwendungshinweise	96
10.7.4	ADV_TDS.1 Grundsätzliches Design	97
10.7.5	ADV_TDS.2 Architekturdesign	98
10.7.6	ADV_TDS.3 Grundsätzliches modulares Design	99
10.7.7	ADV_TDS.4 Semiformales modulares Design	101
10.7.8	ADV_TDS.5 Vollständiges semiformales modulares Design	102
10.7.9	ADV_TDS.6 Vollständiges semiformales modulares Design mit formaler allgemeiner Design Darstellung	103
10.8	Compliance mit dem Verbunddesign (ADV_COMP)	105
10.8.1	Ziele	105
10.8.2	Komponentenebenen	105
10.8.3	Anwendungshinweise	105
10.8.4	ADV_COMP.1 Design-Compliance mit den basiskomponentenbezogenen Leitlinien für Benutzer, dem ETR für Verbundevaluierung und dem Bericht der Evaluierungsinstanz der Basiskomponente	106
11	Klasse AGD: Leitliniendokumente	107
11.1	Allgemeines	107
11.2	Operative Leitlinien für Benutzer (AGD_OPE)	107
11.2.1	Ziele	107
11.2.2	Komponentenebenen	107
11.2.3	Anwendungshinweise	108
11.2.4	AGD_OPE.1 Operative Leitlinien für Benutzer	108
11.3	Vorbereitende Verfahren (AGD_PRE)	109
11.3.1	Ziele	109
11.3.2	Komponentenebenen	109
11.3.3	Anwendungshinweise	109
11.3.4	AGD_PRE.1 Vorbereitende Verfahren	110
12	Klasse ALC: Unterstützung des Lebenszyklus	110
12.1	Allgemeines	110
12.2	CM-Funktionen (ALC_CMC)	112
12.2.1	Ziele	112
12.2.2	Komponentenebenen	112
12.2.3	Anwendungshinweise	113
12.2.4	ALC_CMC.1 Kennzeichnung des TOE	113
12.2.5	ALC_CMC.2 Verwendung des CM-Systems	114
12.2.6	ALC_CMC.3 Autorisierungskontrollen	115
12.2.7	ALC_CMC.4 Herstellungsunterstützung, Abnahmeverfahren und Automatisierung	117
12.2.8	ALC_CMC.5 Erweiterte Unterstützung	120
12.3	CM-Umfang (ALC_CMS)	123
12.3.1	Ziele	123
12.3.2	Komponentenebenen	123
12.3.3	Anwendungshinweise	123
12.3.4	ALC_CMS.1 CM-Abdeckung des TOE	124
12.3.5	ALC_CMS.2 CM-Abdeckung für Teile des TOE	124
12.3.6	ALC_CMS.3 CM-Abdeckung für die Darstellung der Implementierung	125
12.3.7	ALC_CMS.4 CM-Abdeckung für die Problemverfolgung	126
12.3.8	ALC_CMS.5 CM-Abdeckung für Entwicklungswerkzeuge	127
12.4	Lieferung (ALC_DEL)	128
12.4.1	Ziele	128
12.4.2	Komponentenebenen	128
12.4.3	Anwendungshinweise	128
12.4.4	ALC_DEL.1 Lieferverfahren	129
12.5	Sicherheit in der Entwicklungsumgebung (ALC_DVS)	129
12.5.1	Ziele	129

12.5.2	Komponentenebenen	130
12.5.3	Anwendungshinweise	130
12.5.4	ALC_DVS.1 Identifikation von Sicherheitsmaßnahmen	130
12.5.5	ALC_DVS.2 Angemessenheit von Sicherheitsmaßnahmen	131
12.6	Mängelbeseitigung (ALC_FLR)	131
12.6.1	Ziele	131
12.6.2	Komponentenebenen	131
12.6.3	Anwendungshinweise	131
12.6.4	ALC_FLR.1 Grundlegende Mängelbeseitigung	132
12.6.5	ALC_FLR.2 Verfahren zu Mängelberichten	133
12.6.6	ALC_FLR.3 Systematische Mängelbeseitigung	134
12.7	Entwicklung des Lebenszyklus (ALC_LCD)	136
12.7.1	Ziele	136
12.7.2	Komponentenebenen	136
12.7.3	Anwendungshinweise	136
12.7.4	ALC_LCD.1 Vom Entwickler definierte Lebenszyklusprozesse	137
12.7.5	ALC_LCD.2 Messbares Lebenszyklusmodell	138
12.8	Artefakte der TOE-Entwicklung (ALC_TDA)	139
12.8.1	Ziele	139
12.8.2	Komponentenebenen	139
12.8.3	Anwendungshinweise	139
12.8.4	ALC_TDA.1 Eindeutig identifizierende Implementierungsrepräsentation	140
12.8.5	ALC_TDA.2 Abgleich des Umfangs der Darstellung der Implementierung mit dem CMS	142
12.8.6	ALC_TDA.3 Neugenerierung des TOE mit genau definierten Entwicklungswerkzeugen	144
12.9	Werkzeuge und Techniken (ALC_TAT)	147
12.9.1	Ziele	147
12.9.2	Komponentenebenen	147
12.9.3	Anwendungshinweise	147
12.9.4	ALC_TAT.1 Genau festgelegte Entwicklungswerkzeuge	148
12.9.5	ALC_TAT.2 Konformität mit Implementierungsstandards	148
12.9.6	ALC_TAT.3 Konformität mit Implementierungsstandards – alle Teile	149
12.10	Integration von Zusammensetzungsteilen und Konsistenzprüfung von Lieferverfahren (ALC_COMP)	150
12.10.1	Ziele	150
12.10.2	Komponentenebenen	150
12.10.3	Anwendungshinweise	151
12.10.4	ALC_COMP.1 Integration der abhängigen Komponente in die zugehörige Basiskomponente und Konsistenzprüfung für Auslieferungs- und Abnahmeverfahren	151
13	Klasse ATE: Prüfungen	152
13.1	Allgemeines	152
13.2	Abdeckung (ATE_COV)	153
13.2.1	Ziele	153
13.2.2	Komponentenebenen	153
13.2.3	Anwendungshinweise	153
13.2.4	ATE_COV.1 Nachweis der Abdeckung	153
13.2.5	ATE_COV.2 Analyse der Abdeckung	154
13.2.6	ATE_COV.3 Strenge Analyse der Abdeckung	154
13.3	Tiefe (ATE_DPT)	155
13.3.1	Ziele	155
13.3.2	Komponentenebenen	156
13.3.3	Anwendungshinweise	156
13.3.4	ATE_DPT.1 Prüfung: grundlegendes Design	156
13.3.5	ATE_DPT.2 Prüfung: Sicherheit-durchsetzende Module	157
13.3.6	ATE_DPT.3 Prüfung: modulares Design	157
13.3.7	ATE_DPT.4 Prüfung: Darstellung der Implementierung	158
13.4	Funktionsprüfungen (ATE_FUN)	159
13.4.1	Ziele	159

13.4.2	Komponentenebenen	159
13.4.3	Anwendungshinweise	159
13.4.4	ATE_FUN.1 Funktionsprüfung	160
13.4.5	ATE_FUN.2 Geordnete Funktionsprüfungen	161
13.5	Unabhängiges Prüfen (ATE_IND)	162
13.5.1	Ziele	162
13.5.2	Komponentenebenen	162
13.5.3	Anwendungshinweise	162
13.5.4	ATE_IND.1 Unabhängige Prüfungen – Konformität	163
13.5.5	ATE_IND.2 Unabhängige Prüfungen – Stichprobe	164
13.5.6	ATE_IND.3 Unabhängige Prüfungen – vollständig	165
13.6	Prüfung von Verbundprodukten (ATE_COMP)	166
13.6.1	Ziele	166
13.6.2	Komponentenebenen	166
13.6.3	Anwendungshinweise	166
13.6.4	ATE_COMP.1 Funktionsprüfung des Verbundprodukts	167
14	Klasse AVA: Anfälligkeitsbewertung	168
14.1	Allgemeines	168
14.2	Anwendungshinweise	168
14.3	Anfälligkeitsanalyse (AVA_VAN)	168
14.3.1	Ziele	168
14.3.2	Komponentenebenen	169
14.3.3	AVA_VAN.1 Anfälligkeitsuntersuchung	169
14.3.4	AVA_VAN.2 Anfälligkeitsanalyse	170
14.3.5	AVA_VAN.3 Konzentrierte Anfälligkeitsanalyse	171
14.3.6	AVA_VAN.4 Methodische Anfälligkeitsanalyse	172
14.3.7	AVA_VAN.5 Erweiterte methodische Anfälligkeitsanalyse	173
14.4	Anfälligkeitsbewertung für Verbundprodukte (AVA_COMP)	175
14.4.1	Ziele	175
14.4.2	Komponentenebenen	175
14.4.3	Anwendungshinweise	175
14.4.4	AVA_COMP.1 Anfälligkeitsbewertung für Verbundprodukte	176
15	Klasse ACO: Zusammensetzung	176
15.1	Allgemeines	176
15.2	Begründung der Zusammensetzung (ACO_COR)	179
15.2.1	Ziele	179
15.2.2	Komponentenebenen	179
15.2.3	ACO_COR.1 Begründung der Zusammensetzung	179
15.3	Entwicklungsnachweis (ACO_DEV)	180
15.3.1	Ziele	180
15.3.2	Komponentenebenen	180
15.3.3	Anwendungshinweise	180
15.3.4	ACO_DEV.1 Funktionsbeschreibung	181
15.3.5	ACO_DEV.2 Einfacher Nachweis des Designs	181
15.3.6	ACO_DEV.3 Detaillierter Nachweis des Designs	182
15.4	Verlässlichkeit der abhängigen Komponente (ACO_REL)	183
15.4.1	Ziele	183
15.4.2	Komponentenebenen	184
15.4.3	Anwendungshinweise	184
15.4.4	ACO_REL.1 Einfache Verlässlichkeitsinformation	184
15.4.5	ACO_REL.2 Verlässlichkeitsinformationen	185
15.5	Prüfen des zusammengesetzten TOEs (ACO_CTT)	185
15.5.1	Ziele	185
15.5.2	Komponentenebenen	185
15.5.3	Anwendungshinweise	186
15.5.4	ACO_CTT.1 Schnittstellenprüfung	186
15.5.5	ACO_CTT.2 Strenge Schnittstellenprüfung	187

15.6	Anfälligkeitsanalyse der Zusammensetzung (ACO_VUL)	189
15.6.1	Ziele	189
15.6.2	Komponentenebenen	189
15.6.3	Anwendungshinweise	189
15.6.4	ACO_VUL.1 Anfälligkeitsüberprüfung der Zusammensetzung	189
15.6.5	ACO_VUL.2 Anfälligkeitsanalyse der Zusammensetzung	190
15.6.6	ACO_VUL.3 Erweitert-einfache Anfälligkeitsanalyse der Zusammensetzung	191
Anhang A	(informativ) Entwicklung (ADV)	193
A.1	Ergänzende Informationen zu ADV_ARC: Sicherheitsarchitekturen	193
A.1.1	Allgemeines	193
A.1.2	Sicherheitsarchitektureigenschaften	193
A.1.3	Sicherheitsarchitekturbeschreibungen	194
A.2	ADV_FSP: Ergänzende Informationen zur Funktionsspezifikation	196
A.2.1	Allgemeines	196
A.2.2	Nicht-TSF-Teil des TOE	197
A.2.3	Bestimmen der TSFI	198
A.2.4	Beispiel: Ein komplexes DBMS	201
A.2.5	Beispiel-Funktionsspezifikation	202
A.3	ADV_INT: Ergänzende Informationen zu TSF-Intern	204
A.3.1	Allgemeines	204
A.3.2	Struktur von prozeduraler Software	204
A.3.3	Komplexität von prozeduraler Software	206
A.4	ADV_TDS: Teilsysteme und Module	207
A.4.1	Allgemeines	207
A.4.2	Teilsysteme	207
A.4.3	Module	208
A.4.4	Ansatz zur Einstufung	210
A.4.5	Sicherheitsrelevanz	212
A.5	Ergänzende Informationen zu formalen Methoden	213
Anhang B	(informativ) Zusammensetzung (ACO)	215
B.1	Allgemeines	215
B.2	Notwendigkeit für Evaluierungen zusammengesetzter TOEs	215
B.3	Durchführung der Evaluierung von Sicherheitsvorgaben (ST) für einen zusammengesetzten TOE	216
B.4	Interaktionen zwischen zusammengesetzten IT-Entitäten	217
Anhang C	(informativ) Querverweisung von Abhängigkeiten der Vertrauenswürdigkeitskomponenten	223
	Literaturhinweise	228

Bilder

Bild 1	Hierarchie von Vertrauenswürdigkeitsklasse/-familie/-komponente/-element	24
Bild 2	Struktur der Vertrauenswürdigkeitskomponenten	25
Bild 3	Muster eines Klassenaufbaudiagramms	27
Bild 4	APE: Evaluierung des Schutzprofils (PP), Klassenaufbau	28
Bild 5	ACE: Evaluierung der Schutzprofilkonfiguration, Klassenaufbau	39
Bild 6	ASE: Evaluierung der Sicherheitsvorgabe (ST), Klassenaufbau	55
Bild 7	Beziehungen von ADV-Konstrukten zueinander und zu anderen Familien	71
Bild 8	ADV: Entwicklung, Klassenaufbau	74
Bild 9	AGD: Leitliniendokumente, Klassenaufbau	107
Bild 10	ALC: Unterstützung des Lebenszyklus, Klassenaufbau	112
Bild 11	ATE: Prüfungen, Klassenaufbau	153
Bild 12	AVA: Anfälligkeitsbewertung, Klassenaufbau	168
Bild 13	Beziehung zwischen ACO-Familien und Interaktionen zwischen den Komponenten	177
Bild 14	Beziehung zwischen ACO-Familien	179

Bild 15 — ACO: Zusammensetzung, Klassenaufbau	179
Bild A.1 — Wrapper	200
Bild A.2 — Schnittstellen in einem DBMS-System	201
Bild A.3 — Teilsysteme und Module	207
Bild A.4 — Beziehung von ADV_SPM zu anderen Familien und Konstrukten	213
Bild B.1 — Abstraktion der Basiskomponente	218
Bild B.2 — Abstraktion der abhängigen Komponente	219
Bild B.3 — Abstraktion des zusammengesetzten TOEs	220
Bild B.4 — Schnittstellen zusammengesetzter Komponenten	220

Tabellen

Tabelle A.1 — Einstufung der Beschreibungsdetails	211
Tabelle C.1 — Abhängigkeitstabelle für Klasse ADV: Entwicklung	223
Tabelle C.2 — Abhängigkeitstabelle für Klasse AGD: Leitliniendokumente	224
Tabelle C.3 — Abhängigkeitstabelle für Klasse ALC: Unterstützung des Lebenszyklus	224
Tabelle C.4 — Abhängigkeitstabelle für Klasse APE: Evaluierung des Schutzprofils	225
Tabelle C.5 — Abhängigkeitstabelle für Klasse ACE: Evaluierung der PP-Konfiguration	225
Tabelle C.6 — Abhängigkeitstabelle für Klasse ASE: Evaluierung der Sicherheitsvorgabe (ST)	225
Tabelle C.7 — Abhängigkeitstabelle für Klasse ATE: Prüfungen	226
Tabelle C.8 — Abhängigkeitstabelle für Klasse AVA: Anfälligkeitsbewertung	226
Tabelle C.9 — Abhängigkeitstabelle für Klasse ACO: Zusammensetzung	227

Europäisches Vorwort

Der Text von ISO/IEC 15408-3:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 15408-3:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument wird EN ISO/IEC 15408-3:2021 ersetzen.

Anerkennungsnotiz

Der Text von ISO/IEC 15408-3:2022 wurde von CEN als EN ISO/IEC 15408-3:2023 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/IEC 15408-3:2008), die technisch überarbeitet wurde.

Die wesentlichen Änderungen sind folgende:

- die Terminologie wurde überprüft und aktualisiert;
- der genaue Konformitätstyp wurde aufgenommen;
- die PP mit niedriger Vertrauenswürdigkeit wurden entfernt und die PP mit direkter Begründung aufgenommen;
- PP-Module und PP-Konfigurationen für modulare Evaluierungen wurden aufgenommen;
- eine Evaluierung mit Mehrfach-Vertrauenswürdigkeit wurde aufgenommen.

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

- Entwurf -

**E DIN EN ISO/IEC 15408-3:2024-03
EN ISO/IEC 15408-3:2023 (D)**

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.

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

Einleitung

Die in diesem Dokument definierten Vertrauenswürdigkeitskomponenten sind die Grundlage für die in einem Vertrauenswürdigkeitspaket, Schutzprofil (PP), PP-Modul, einer PP-Konfiguration oder einer Sicherheitsvorgabe (ST) ausgedrückten Vertrauenswürdigkeitsanforderungen.

Diese Anforderungen schaffen eine einheitliche Methode zur Formulierung von Vertrauenswürdigkeitsanforderungen für TOEs. Dieses Dokument katalogisiert den Satz an Vertrauenswürdigkeitskomponenten, -familien und -klassen. Es definiert auch Evaluationskriterien für die PP, PP-Konfigurationen, PP-Module und die ST.

Die Zielgruppe für dieses Dokument schließt Verbraucher, Entwickler, technische Arbeitsgruppen, Evaluatoren von sicheren IT-Produkten und andere ein. ISO/IEC 15408-1:2022, Abschnitt 5, enthält zusätzliche Informationen zur Zielgruppe der Normenreihe ISO/IEC 15408 und zur Verwendung der Normenreihe ISO/IEC 15408 durch entsprechende Gruppen, die die Zielgruppe umfassen. Diese Gruppen können dieses Dokument wie folgt verwenden:

- a) Verbraucher, die dieses Dokument beim Auswählen von Komponenten in der Formulierung von Vertrauenswürdigkeitsanforderungen zur Erfüllung von in einem PP oder einer ST ausgedrückten Sicherheitszielsetzungen verwenden, um den erforderlichen Grad der Vertrauenswürdigkeit des TOE zu bestimmen.
- b) Entwickler, die mit der Erstellung eines TOE auf tatsächliche oder angenommene Sicherheitsanforderungen von Verbrauchern reagieren, verweisen auf dieses Dokument bei der Interpretation von Aussagen zu Vertrauenswürdigkeitsanforderungen und der Bestimmung von Ansätzen zur Vertrauenswürdigkeit von TOEs.
- c) Evaluatoren, die die in diesem Dokument definierten Vertrauenswürdigkeitsanforderungen als eine verpflichtende Aussage ihrer Evaluierungskriterien bei der Bestimmung der Vertrauenswürdigkeit der TOEs und bei der Evaluierung von PPs und STs verwenden.

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 Vertrauenswürdigkeitsanforderungen der Normenreihe ISO/IEC 15408. Es beinhaltet die einzelnen Vertrauenswürdigkeitskomponenten, aus denen sich die in ISO/IEC 15408-5 enthaltenen Vertrauenswürdigkeitsstufen und andere Pakete zusammensetzen, sowie die Kriterien für die Evaluierung von Schutzprofilen (PP), PP-Konfigurationen, PP-Modulen und Sicherheitsvorgaben (ST).

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 — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information security — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-4, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 15408-5, *Information security — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

ISO/IEC 18045:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

ISO/IEC IEEE 24765, *Systems and software engineering — Vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-4, ISO/IEC 15408-5, ISO/IEC 18045 und ISO/IEC IEEE 24765 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

Abnahmeverfahren

Verfahren, das durchgeführt wird, um neu erstellte oder geänderte *Konfigurationselemente* (3.3) als Teil des Evaluierungsgegenstands (TOE) abzunehmen oder in den nächsten Lebenszyklusschritt zu überführen

Anmerkung 1 zum Begriff: Diese Verfahren identifizieren die Rollen oder Einzelpersonen, die für die Abnahme verantwortlich sind, sowie die anzuwendenden Kriterien, die für die Entscheidung über die Abnahme herangezogen werden.

Anmerkung 2 zum Begriff: Es gibt mehrere Arten von Abnahmesituationen; manche können sich überschneiden:

- a) erstmalige Übernahme eines Elements in das Konfigurationsmanagementsystem, insbesondere als Teil eines Integrationsprozesses;
- b) Überführung von Konfigurationselementen in die nächste Lebenszyklusphase in allen Entwurfsphasen des TOE

BEISPIEL 1 Modul, Teilsystem, Qualitätskontrolle des fertiggestellten TOE;

c) im Anschluss an den Transport von Konfigurationselementen

BEISPIEL 2 Teile des TOE oder vorläufige Produkte zwischen verschiedenen Standorten der *Entwicklung* (3.15);

d) im Anschluss an die *Auslieferung* (3.14) des TOE an den Verbraucher;

e) im Anschluss an die Integration des TOE

BEISPIEL 3 Aufnahme von Software-, Firmware- und Hardware-Komponenten aus anderen Quellen in den TOE.

3.2

Aktion

Evaluatoren- oder Entwickleraktionselement von ISO/IEC 15408-3

Anmerkung 1 zum Begriff: Diese Aktionen werden entweder explizit als Evaluatorenaktionen angegeben oder implizit aus Entwickleraktionen (implizite Evaluatorenaktionen) innerhalb der Vertrauenswürdigkeitskomponenten von ISO/IEC 15408-3 abgeleitet.

3.3

Konfigurationselement

Element oder Aggregation von Hardware, Software oder beidem, das bzw. die für das Konfigurationsmanagement vorgesehen ist und während der *Entwicklung* (3.15) des Evaluierungsgegenstands (TOE) als eine einzige Entität im Rahmen des Konfigurationsmanagementprozesses behandelt wird

Anmerkung 1 zum Begriff: Es kann sich dabei entweder um Teile des TOE oder um Objekte handeln, die mit der Entwicklung des TOE in Zusammenhang stehen, z. B. Evaluierungsdokumente oder Entwicklungswerkzeuge. Konfigurationsmanagement-Elemente können, zusammen mit ihrer Version, entweder direkt im Konfigurationsmanagementsystem gespeichert sein (zum Beispiel Dateien) oder referenziert werden (zum Beispiel Hardware-Bauteile).

3.4

Konfigurationsliste

Dokument der *Konfigurationsmanagementausgabe* (3.8), das alle *Konfigurationselemente* (3.3) für ein spezifisches Produkt zusammen mit der genauen Version aller Konfigurationsmanagementelemente auflistet, die für eine bestimmte Version des Gesamtprodukts relevant sind

Anmerkung 1 zum Begriff: Diese Liste ermöglicht die Unterscheidung der Elemente, die zur evaluierten Version des Produkts gehören, von anderen Versionen dieser Elemente, die zu anderen Versionen des Produkts gehören. Die finale Konfigurationsmanagementliste ist ein spezifisches Dokument für eine spezifische Version des spezifischen Produkts. (Bei der Liste kann es sich natürlich um ein elektronisches Dokument innerhalb eines *Konfigurationsmanagementwerkzeugs* (3.12) handeln. In diesem Fall kann sie als spezifischer Einblick in das System oder einen Teil des Systems angesehen werden und nicht als eine Ausgabe des Systems. Allerdings wird die Konfigurationsliste im praktischen Einsatz während einer Evaluierung vermutlich als Teil der Evaluierungsdokumentation bereitgestellt werden.) Die Konfigurationsliste definiert die Elemente, die unter die Konfigurationsmanagementanforderungen von ALC_CMC fallen.

3.5

Konfigurationsmanagement

CM, en: Configuration Management

Fachgebiet, in dem technische und administrative Anleitung und Überwachung eingesetzt werden, um die funktionellen und physikalischen Merkmale eines *Konfigurationselements* (3.3) zu identifizieren und zu dokumentieren, Änderungen dieser Merkmale zu kontrollieren, die Umsetzung von Änderungen sowie den Implementierungsstatus aufzuzeichnen und zu berichten und die Compliance der festgelegten Anforderungen zu überprüfen

[QUELLE: ISO/IEC IEEE 24765:2017, 3.779 1]

3.6

Konfigurationsmanagementdokumentation

CM-Dokumentation

Dokumentation einschließlich *Konfigurationsmanagementausgabe* (3.8), *Konfigurationsmanagementliste(n)*, *Konfigurationsmanagementsystem-Datensätzen* (3.11), *Konfigurationsmanagementplan* (3.9) und *Konfigurationsmanagement-Nutzungsdokumentation* (3.13)

3.7

Konfigurationsmanagementnachweis

alles was verwendet werden kann, um Vertrauen in den ordnungsgemäßen Betrieb des Konfigurationsmanagementsystems herzustellen

BEISPIEL *Konfigurationsmanagementausgabe* (3.8), vom Entwickler gelieferte Begründungen; Beobachtungen, Experimente oder Interviews, die während einer Standortbegehung vom Evaluator gemacht bzw. durchgeführt wurden.

3.8

Konfigurationsmanagementausgabe

Ergebnisse in Bezug auf das Konfigurationsmanagement, die vom Konfigurationsmanagementsystem erstellt oder durchgesetzt werden

Anmerkung 1 zum Begriff: Diese mit dem Konfigurationsmanagement in Zusammenhang stehenden Ergebnisse können die Form von Dokumenten haben (z. B. ausgefüllte Papierformulare, *Konfigurationsmanagementsystem-Datensätze* (3.11), Protokolldaten, Ausdrücke und elektronische Ausgabedaten) oder von Aktionen (z. B. manuelle Maßnahmen zur Erfüllung von Konfigurationsmanagementanweisungen). Beispiele für solche Konfigurationsmanagementausgaben sind *Konfigurationslisten* (3.4), *Konfigurationsmanagementpläne* (3.9) und/oder das Verhalten während des Produktlebenszyklus.

3.9

Konfigurationsmanagementplan

Beschreibung der Verwendung des Konfigurationsmanagementsystems für den Evaluierungsgegenstand (TOE)

Anmerkung 1 zum Begriff: Das Ziel bei der Erstellung eines Konfigurationsmanagementplans ist es, Mitarbeitern deutlich zu machen, was sie tun müssen. Aus Sicht des gesamten Konfigurationsmanagementsystems kann dieser als Ausgabedokument betrachtet werden (da er als Teil der Anwendung des Konfigurationsmanagementsystems erstellt werden kann). Aus Sicht des konkreten Projekts handelt es sich um ein Anwendungsdokument, da er von den Mitgliedern des Projektteams verwendet wird, um die Schritte zu verstehen, die sie während des Projekts durchführen müssen. Der Konfigurationsmanagementplan beschreibt die Verwendung des Systems für das spezifische Produkt; das gleiche System kann in einem anderen Umfang für andere Produkte verwendet werden. Der Konfigurationsmanagementplan definiert und beschreibt die Ausgaben des während der TOE-Entwicklung (3.15) eingesetzten Konfigurationsmanagementsystems eines Unternehmens.

BEISPIEL Die Struktur und der Inhalt eines Konfigurationsmanagementplans sind in ISO 10007:2017, Anhang A dargestellt.

3.10

Konfigurationsmanagementsystem

Satz von Verfahren und Werkzeugen (einschließlich deren Dokumentation), der von einem Entwickler zur Entwicklung und Wartung der Konfigurationen der Produkte während ihrer Lebenszyklen verwendet wird

Anmerkung 1 zum Begriff: Konfigurationsmanagementsysteme können über unterschiedliche Stringenz- und Funktionsgrade verfügen. Auf den höheren Stufen können Konfigurationsmanagementsysteme automatisiert sein und über Mechanismen für die Mängelbehebung, Änderungskontrolle und sonstige Nachverfolgungsmechanismen verfügen.

3.11

Konfigurationsmanagementsystem-Datensatz

Ausgaben, die während des Betriebs des Konfigurationsmanagementsystems erstellt werden und wichtige Konfigurationsmanagementaktivitäten dokumentieren

BEISPIEL Formulare zur Änderungskontrolle von Konfigurationsmanagementsystemelementen und Formulare zur Genehmigung des Zugriffs auf Konfigurationsmanagementsystemelemente.

3.12

Konfigurationsmanagementwerkzeug

manuell geführte oder automatisierte Werkzeuge, die ein Konfigurationsmanagementsystem realisieren oder unterstützen

BEISPIEL Werkzeuge für die Versionsverwaltung der Teile des Evaluierungsgegenstands (TOE).

3.13

Konfigurationsmanagement-Nutzungsdokumentation

Teil des Konfigurationsmanagementsystems, der beschreibt, wie das Konfigurationsmanagementsystem definiert und angewendet wird, z. B. mithilfe von Handbüchern, Vorschriften und/oder der Dokumentation von Werkzeugen und Verfahren

3.14

Auslieferung

Übergabe des fertiggestellten Evaluierungsgegenstands (TOE) von der Umgebung der *Herstellung* (3.24) in die Hände des Kunden

Anmerkung 1 zum Begriff: Diese Produktlebenszyklusphase kann die Verpackung und Lagerung am Standort der *Entwicklung* (3.15) beinhalten, aber umfasst nicht den Transport des nicht fertiggestellten TOE oder von dessen Teilen zwischen verschiedenen Entwicklern oder Entwicklungsstandorten.

3.15

Entwicklung

Produktlebenszyklusphase, welche die Erzeugung der Implementierungsrepräsentation des Evaluierungsgegenstands (TOE) betrifft

Anmerkung 1 zum Begriff: Im gesamten ALC: Anforderungen an die Lebenszyklusunterstützung, Entwicklung und verwandte Begriffe (Entwickler, entwickeln) sind im allgemeineren Sinn zu verstehen und umfassen die Entwicklung und die *Herstellung* (3.24).

3.16

aufgedeckte mögliche Anfälligkeit

potentielle Schwachstellen im Evaluierungsgegenstand (TOE), die vom Evaluator bei der Durchführung von Evaluierungsaufgaben festgestellt werden und die zur Verletzung der Sicherheitsfunktionsanforderungen (SFR) genutzt werden können

3.17

Evaluationsbeitrag

Ressource, die der Evaluator oder die Evaluierungsinstanz vom Antragsteller oder Entwickler zur Durchführung einer oder mehrerer Evaluierungs- oder Evaluierungsüberwachungsaufgaben benötigt

3.18

ausnutzbare Anfälligkeit

Schwachstelle im Evaluierungsgegenstand (TOE), die für Verletzungen von Sicherheitsfunktionsanforderungen (SFR) in der Betriebsumgebung des TOE genutzt werden kann

3.19

Installation

von einem menschlichen Benutzer durchgeführtes Verfahren zur Einbindung des Evaluierungsgegenstands (TOE) in seine Betriebsumgebung und zu dessen Inbetriebnahme

Anmerkung 1 zum Begriff: Diese Operation wird normalerweise nur einmal nach Erhalt und Abnahme des TOE durchgeführt. Es wird erwartet, dass der TOE soweit konfiguriert wird, dass die Konfiguration entsprechend der Sicherheitsvorgabe (ST) zulässig ist. Wenn ähnliche Prozesse durch den Entwickler durchgeführt werden müssen, dann werden sie im Rahmen der Klasse „ALC: Life-cycle support“ als „Generierung“ bezeichnet. Falls der TOE eine Erstinbetriebnahme erfordert, die nicht regelmäßig wiederholt werden muss, dann würde dieser Prozess als Installation eingestuft.

3.20

Lebenszyklusmodell

Rahmen, der die Prozesse, Aktivitäten und Aufgaben umfasst, die mit der *Entwicklung* (3.15), dem Betrieb und der Wartung eines Produkts verbunden sind, und der die Lebensdauer des Systems von der Definition seiner Anforderungen bis zur Beendigung seiner Nutzung umfasst

[QUELLE: ISO/IEC IEEE 24765:2017, 3.2219 2]

3.21

Betrieb

<TOE-Lebenszyklus>Nutzungszeitraum des Evaluierungsgegenstands (TOE) einschließlich üblicher Nutzung, Administration und Wartung des TOE nach *Auslieferung* (3.14) und *Bereitstellung* (3.23)

3.22

mögliche Anfälligkeit

vermutete, aber nicht bestätigte Schwachstelle

Anmerkung 1 zum Begriff: Der Verdacht ergibt sich aufgrund eines angenommenen Angriffspaths zur Verletzung der Sicherheitsfunktionsanforderungen (SFR).

3.23

Bereitstellung

Aktivität in der Lebenszyklusphase eines Produkts, die die Kundenabnahme des ausgelieferten Evaluierungsgegenstands (TOE) und dessen *Installation* (3.19) umfasst

Anmerkung 1 zum Begriff: Die Bereitstellung kann Aktivitäten wie das Hochfahren, die Initialisierung, die Erstinbetriebnahme und die Vorbereitung des TOE bis zu einem betriebsbereiten Zustand umfassen.

3.24

Herstellung

Lebenszyklusphase, die aus der Umsetzung der Implementierungsrepräsentation in die Implementierung des TOE besteht, d. h. in einen Zustand, der für die *Auslieferung* (3.14) an den Kunden geeignet ist

Anmerkung 1 zum Begriff: Diese Phase kann die Herstellung, Integration, Generierung, den internen Transport, die Lagerung und Kennzeichnung des TOE umfassen.

3.25

Restanfälligkeit

Schwachstelle, die nicht in der Betriebsumgebung des Evaluierungsgegenstands (TOE) ausgenutzt werden kann, die aber für Verletzungen der Sicherheitsfunktionsanforderungen (SFR) durch einen Angreifer genutzt werden kann, der ein höheres Angriffspotential hat, als es für die Betriebsumgebung des TOE angenommen wird

3.26

Unteraufgabe

Anwendung einer Vertrauenswürdigkeitskomponente aus ISO/IEC 15408-3

Anmerkung 1 zum Begriff: Vertrauenswürdigkeitsfamilien werden in der Normenreihe ISO/IEC 15408 nicht explizit behandelt, da Evaluierungen an einer einzelnen Vertrauenswürdigkeitskomponente aus einer Vertrauenswürdigkeitsfamilie durchgeführt werden.

3.27

Zeitspanne bis zur Aufdeckung

Zeitspanne, in der ein Element an einem IT-System beteiligt ist und angegriffen werden kann

3.28

Anfälligkeit

Schwachstelle im TOE, die für Verletzungen von Sicherheitsfunktionsanforderungen (SFR) in manchen Umgebungen ausgenutzt werden kann

3.29

Zugriff Gelegenheit

Zeitspanne, in der ein Angreifer Zugriff auf einen Evaluierungsgegenstand (TOE) hat

4 Übersicht

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

Abschnitt 6 beschreibt die Struktur der Darstellung der Vertrauenswürdigkeitsklassen, -familien und -komponenten, der Vertrauenswürdigkeitsstufen und ihrer Beziehungen sowie den Aufbau der zusammengesetzten Sicherheitspakete (CAP). Er charakterisiert außerdem die in Abschnitt 7 bis Abschnitt 15 dargestellten Klassen und Familien der Vertrauenswürdigkeit.

Abschnitt 7 bis Abschnitt 15 bieten die ausführlichen Definitionen der Vertrauenswürdigkeitsklassen nach diesem Dokument.

Anhang A bietet weitere Erklärungen und Beispiele der Konzepte hinter der Entwicklungsklasse.

Anhang B bietet eine Erklärung der Konzepte hinter Evaluierungen zusammengesetzter Evaluierungsgegenstände (TOE) und der Klasse „Zusammensetzung“.

Anhang C bietet eine Zusammenfassung der Abhängigkeiten zwischen den Vertrauenswürdigkeitskomponenten.

5 Paradigma für Vertrauenswürdigkeit

5.1 Allgemeines

Der Zweck dieses Abschnitts besteht darin, den zugrundeliegenden Ansatz der Normenreihe ISO/IEC 15408 zur Vertrauenswürdigkeit zu dokumentieren. Ein Verständnis dieses Abschnitts erlaubt dem Leser, den Grundgedanken hinter den Vertrauenswürdigkeitsanforderungen dieses Dokuments zu verstehen.

5.2 Ansatz der Normenreihe ISO/IEC 15408

Der Ansatz der Normenreihe ISO/IEC 15408 besagt, dass Bedrohungen der Sicherheit und Verpflichtungen organisatorischer Sicherheitspolitik deutlich formuliert sein sollten und dass die vorgeschlagenen Sicherheitskontrollen nachweisbar für den beabsichtigten Zweck ausreichen.

Außerdem sollten Maßnahmen getroffen werden, um die Wahrscheinlichkeit von Anfälligkeiten, die Möglichkeiten zum Verwenden (d. h. zum absichtlichen Ausnutzen oder unabsichtlichen Auslösen) einer Anfälligkeit und den Umfang des Schadens zu verringern, der durch das Verwenden einer Anfälligkeit eintreten kann. Zusätzlich sollten Maßnahmen getroffen werden, die eine anschließende Identifizierung der Anfälligkeiten und die Beseitigung, Umgehung und/oder Benachrichtigung ermöglichen, dass die Anfälligkeit ausgenutzt oder ausgelöst wurde.

5.3 Ansatz für Vertrauenswürdigkeit

5.3.1 Allgemeines

Der Ansatz der Normenreihe ISO/IEC 15408 ist die Bereitstellung von Vertrauenswürdigkeit auf Grundlage von Evaluierung eines IT-Produkts, das als vertrauenswürdig vorgesehen ist. Evaluierung ist das traditionelle Mittel zur Bereitstellung von Vertrauenswürdigkeit und bildet die Grundlage für vorgeordnete Dokumente zu Evaluierungskriterien. Die Normenreihe ISO/IEC 15408 übernimmt durch das Abstimmen bestehender Ansätze denselben Ansatz. Die Normenreihe ISO/IEC 15408 rät, die Gültigkeit der Dokumentation und des entsprechenden IT-Produkts von fachkundigen Evaluatoren messen zu lassen und dabei zunehmenden Wert auf Umfang, Tiefe und Strenge zu legen.

Die Normenreihe ISO/IEC 15408 schließt die relativen Vorzüge anderer Mittel zur Schaffung von Vertrauenswürdigkeit nicht aus und kommentiert diese auch nicht. Es erfolgt weiterhin Forschung in Hinblick auf alternative Möglichkeiten zur Schaffung von Vertrauenswürdigkeit. Wenn aus diesen Forschungsaktivitäten ausgereifte alternative Ansätze erwachsen, werden diese für die Aufnahme in die Normenreihe ISO/IEC 15408 berücksichtigt, die bereits für deren spätere Aufnahme entsprechend aufgebaut ist.

5.3.2 Bedeutung von Anfälligkeiten

Es wird angenommen, dass es Bedrohungsagenten gibt, die aktiv versuchen, Möglichkeiten zum Verletzen von Sicherheitspolitiken sowohl zur Erlangung unerlaubter Vorteile als auch für wohlgemeinte, aber dennoch unsichere Aktionen auszunutzen. Bedrohungsagenten können auch versehentlich Sicherheitsanfälligkeiten auslösen, die der Organisation Schaden zufügen. Durch das Bedürfnis zur Verarbeitung sensibler Informationen und den Mangel an Verfügbarkeit ausreichend vertrauenswürdiger Produkte entsteht ein erhebliches Risiko durch Ausfälle der IT. Daher ist es wahrscheinlich, dass IT-Sicherheitsverstöße zu erheblichen Verlusten führen können.

IT-Sicherheitsverstöße entstehen durch absichtliches Ausnutzen oder unabsichtliches Auslösen von Anfälligkeiten in IT-Anwendungen großer Unternehmen.

Es sollten Schritte zur Verhinderung von in IT-Produkten entstehenden Anfälligkeiten eingeleitet werden. Bis zu einem machbaren Umfang sollten Anfälligkeiten:

- a) beseitigt werden: es sollten aktiv Schritte unternommen werden, um alle ausführbaren Anfälligkeiten aufzudecken, zu entfernen oder aufzuheben;
- b) minimiert werden: es sollten aktiv Schritte unternommen werden, um die potentiellen Auswirkungen jeglicher Ausführung von Anfälligkeiten auf einen annehmbaren Restwert zu reduzieren;
- c) überwacht werden: es sollten aktiv Schritte unternommen werden, um jegliche Versuche zum Ausführen einer verbleibenden Anfälligkeit zu erkennen, damit Schritte zur Begrenzung des Schadens eingeleitet werden können.

5.3.3 Ursachen von Anfälligkeiten

Anfälligkeiten können auftreten durch Fehler:

- a) in den Anforderungen: ein IT-Produkt kann zwar alle von ihm geforderten Funktionen und Eigenschaften besitzen, aber immer noch Anfälligkeiten enthalten, die es in Hinblick auf Sicherheit ungeeignet oder unwirksam machen;

- b) im Design: ein IT-Produkt ist schlecht ausgelegt. Der Aufbau eines sicheren Produkts, Systems oder einer sicheren Anwendung erfordert nicht nur die Implementierung funktionaler Anforderungen, sondern auch eine Architektur, die die wirksame Durchsetzung spezifischer Sicherheitseigenschaften ermöglicht, die das Produkt, System oder die Anwendung durchsetzen soll. Die Fähigkeit, Angriffen standzuhalten, denen das Produkt, das System oder die Anwendung in der vorgesehenen Betriebsumgebung ausgesetzt sein kann, hängt in hohem Maße von einer Architektur ab, die diese Angriffe verhindert oder, falls sie nicht verhindert werden können, die Erkennung solcher Angriffe und/oder die Begrenzung des Schadens ermöglicht, den ein solcher Angriff verursachen kann;
- c) in der Entwicklung: ein IT-Produkt erfüllt nicht die Spezifikationen und/oder Anfälligkeiten wurden durch schlechte Entwicklungsrichtlinien oder fehlerhafte Designentscheidungen eingebracht;
- d) bei Auslieferung, Installation und Konfiguration: ein IT-Produkt weist Anfälligkeiten auf, die bei der Auslieferung, Installation und Konfiguration des Produkts eingeführt werden;
- e) im Betrieb: ein IT-Produkt wurde ordnungsgemäß nach einer korrekten Spezifikation erstellt, aber Anfälligkeiten wurden durch unzureichende Kontrollen im Betrieb eingebracht.
- f) bei der Wartung: ein IT-Produkt wird so gewartet, dass neue Anfälligkeiten eingeführt werden.

5.3.4 Vertrauenswürdigkeit der Normenreihe ISO/IEC 15408

Vertrauenswürdigkeit kann aus Verweisungen auf Quellen wie unbegründeten Behauptungen, relevante Vorerfahrung oder gezielte Erfahrung abgeleitet werden. Die Normenreihe ISO/IEC 15408 bietet allerdings Vertrauenswürdigkeit durch aktive Untersuchung oder einen spezifikationsbasierten Ansatz. Aktive Untersuchung ist eine Evaluierung des IT-Produkts zur Bestimmung seiner Sicherheitseigenschaften.

5.3.5 Vertrauenswürdigkeit durch Evaluierung

Evaluierung ist das traditionelle Mittel zur Schaffung von Vertrauenswürdigkeit und bildet die Grundlage für den Ansatz der Normenreihe ISO/IEC 15408. Evaluierungstechniken beinhalten, ohne darauf beschränkt zu sein:

- a) Analyse und Überprüfung von Prozess(en) und Verfahren;
- b) Überprüfung, dass Prozess(e) und Verfahren angewendet werden;
- c) Analyse der Übereinstimmung zwischen TOE-Design Darstellungen;
- d) Analyse der TOE-Design Darstellung gegen die Anforderungen;
- e) Verifizierung der Nachweise;
- f) Analyse der Leitliniendokumente;
- g) Analyse der entwickelten Funktionsprüfungen und der bereitgestellten Ergebnisse;
- h) unabhängige Funktionsprüfung;
- i) Analyse auf Anfälligkeiten (einschließlich Fehlerannahmen);
- j) Penetrationstest;
- k) Analyse des Auslieferungsverfahrens;
- l) Analyse des Wartungsverfahrens.

5.4 Vertrauenswürdigkeitsskala der Normenreihe ISO/IEC 15408

Der Ansatz der Normenreihe ISO/IEC 15408 versichert, dass höherer Evaluierungsaufwand zu höherer Vertrauenswürdigkeit führt, und dass das Ziel darin besteht, den geringstmöglichen Aufwand zu betreiben, der erforderlich ist, um die geforderte Vertrauenswürdigkeit zu erreichen. Der zunehmende Grad an Aufwand basiert auf:

- a) dem Umfang: der Aufwand ist größer, weil ein größerer Teil des IT-Produkts eingebunden wird;
- b) der Tiefe: der Aufwand ist größer, weil er sich auf einen feineren Designgrad und Einzelheiten der Implementierung bezieht;
- c) der Strenge: der Aufwand ist größer, weil er in einer strukturierten und formaleren Art und Weise eingebracht wird.

6 Vertrauenswürdigkeitskomponenten

6.1 Allgemeines

6.2 bis 6.6 beschreiben die verwendeten Konstrukte zur Darstellung von Vertrauenswürdigkeitsklassen, -familien und -komponenten.

Bild 1 zeigt die in diesem Dokument definierten Vertrauenswürdigkeitsanforderungen (SAR). Es ist zu beachten, dass auf die abstrakteste Sammlung an SARs als eine Klasse verwiesen wird. Jede Klasse enthält Vertrauenswürdigkeitsfamilien, die Vertrauenswürdigkeitskomponenten enthalten, die wiederum Vertrauenswürdigkeitselemente enthalten. Klassen und Familien werden zur Bereitstellung einer Taxonomie für die Klassifizierung von SARs verwendet, während Komponenten zur Spezifizierung von SARs in einem PP/einer ST verwendet werden.

6.2 Struktur der Vertrauenswürdigkeitsklassen

6.2.1 Allgemeines

Bild 1 stellt die Struktur der Vertrauenswürdigkeitsklassen dar.

6.2.2 Klassenname

Jeder Vertrauenswürdigkeitsklasse ist ein eindeutiger Name zugewiesen. Der Name deutet auf die von der Vertrauenswürdigkeitsklasse behandelten Themen hin.

Außerdem wird eine eindeutige Kurzform für den Namen der Vertrauenswürdigkeitsklasse bereitgestellt. Dies ist das vorrangige Mittel zur Verweisung auf die Vertrauenswürdigkeitsklasse. Die festgelegte Konvention ist ein „A“ gefolgt von zwei Buchstaben mit Bezug zum Klassennamen.

6.2.3 Klasseneinleitung

Jede Vertrauenswürdigkeitsklasse hat einen einleitenden Unterabschnitt, der die Zusammensetzung der Klasse beschreibt, und erläuternden Text zum Zweck der Klasse enthält.

6.2.4 Vertrauenswürdigkeitsfamilien

Jede Vertrauenswürdigkeitsklasse enthält mindestens eine Vertrauenswürdigkeitsfamilie. Die Struktur der Vertrauenswürdigkeitsfamilien ist in folgendem Unterabschnitt beschrieben.

Bild 1 stellt die Struktur der Vertrauenswürdigkeitsfamilien dar.

Vertrauenswürdigkeitsanforderungen der Common Criteria

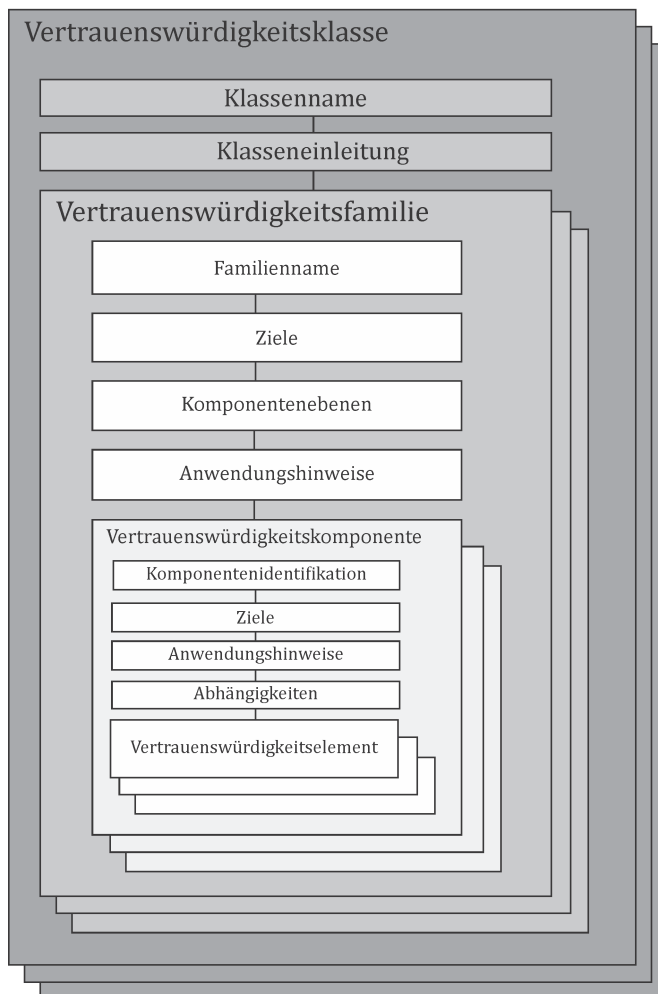


Bild 1 — Hierarchie von Vertrauenswürdigkeitsklasse/-familie/-komponente/-element

6.3 Struktur der Vertrauenswürdigkeitsfamilien

6.3.1 Familiennamen

Jeder Vertrauenswürdigkeitsfamilie ist ein eindeutiger Name zugewiesen. Der Name enthält beschreibende Informationen zu den behandelten Themen der Vertrauenswürdigkeitsfamilie. Jede Vertrauenswürdigkeitsfamilie ist in eine Vertrauenswürdigkeitsklasse eingeordnet, die weitere Familien mit gleichem Zweck enthält.

Außerdem wird eine eindeutige Kurzform für den Namen der Vertrauenswürdigkeitsfamilie bereitgestellt. Diese ist das vorrangige Mittel zur Verweisung auf die Vertrauenswürdigkeitsfamilie. Die festgelegte Konvention ist, dass die Kurzform des Klassennamens verwendet wird, gefolgt von einem Unterstrich und anschließend drei Buchstaben mit Bezug zum Familiennamen.

6.3.2 Ziele

Der Unterabschnitt „Ziele“ der Vertrauenswürdigkeitsfamilie stellt den Zweck der Vertrauenswürdigkeitsfamilie dar.

Dieser Unterabschnitt beschreibt die Ziele, insbesondere die Ziele in Bezug auf das Vertrauenswürdigkeitsparadigma der Normenreihe ISO/IEC 15408, das von der Familie behandelt wird. Die Beschreibung der Vertrauens-

würdigkeitsfamilie ist allgemein gehalten. Alle erforderlichen Einzelheiten für die Ziele sind in der jeweiligen Vertrauenswürdigkeitskomponente enthalten.

6.3.3 Komponentenebenen

Jede Vertrauenswürdigkeitsfamilie enthält eine oder mehrere Vertrauenswürdigkeitskomponenten. Dieser Unterabschnitt der Vertrauenswürdigkeitsfamilie beschreibt die verfügbaren Komponenten und erklärt zwischen ihnen bestehende Unterschiede. Der wesentliche Zweck des Unterabschnitts ist die Differenzierung zwischen den Vertrauenswürdigkeitskomponenten, nachdem festgestellt wurde, dass die Vertrauenswürdigkeitsfamilie ein erforderlicher oder sinnvoller Teil der SARs für ein PP/eine ST ist.

Vertrauenswürdigkeitsfamilien mit mehr als einer Komponente werden eingestuft und für die Art der Einstufung wird eine Begründung bereitgestellt. Diese Begründung bezieht sich auf den Umfang, die Tiefe und/oder die Strenge.

6.3.4 Anwendungshinweise

Falls vorhanden, enthält der Unterabschnitt „Anwendungshinweise“ der Vertrauenswürdigkeitsfamilie zusätzliche Informationen zur Vertrauenswürdigkeitsfamilie. Diese Informationen sollten von besonderem Interesse für Anwender der Vertrauenswürdigkeitsfamilie (z. B. PP-/ST-Autoren, Designer von TOEs, Evaluatoren) sein. Die Darstellung ist informativ und enthält beispielsweise Warnungen zu Anwendungsgrenzen und Bereiche, für die besondere Beachtung erforderlich sein kann.

6.3.5 Vertrauenswürdigkeitskomponenten

Jede Vertrauenswürdigkeitsfamilie enthält mindestens eine Vertrauenswürdigkeitskomponente. Die Struktur der Vertrauenswürdigkeitskomponenten ist in folgendem Unterabschnitt beschrieben.

6.4 Struktur der Vertrauenswürdigkeitskomponenten

6.4.1 Allgemeines

Bild 2 stellt die Struktur der Vertrauenswürdigkeitskomponenten dar.

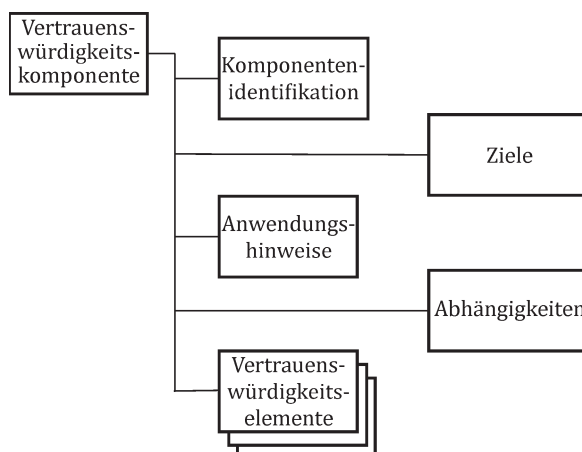


Bild 2 — Struktur der Vertrauenswürdigkeitskomponenten

Die Beziehung zwischen den Komponenten einer Familie wird durch Fettmarkierung hervorgehoben. Teile der Anforderungen, die neu oder erweitert sind oder die über die Anforderungen der vorherigen Komponente innerhalb einer Hierarchie hinaus geändert wurden, sind fett hervorgehoben.

6.4.2 Komponentenidentifikation

Der Unterabschnitt „Komponentenidentifikation“ bietet beschreibende Informationen, die zur Identifizierung, Kategorisierung, Registrierung und Verweisung einer Komponente erforderlich sind.

Jeder Vertrauenswürdigkeitskomponente ist ein eindeutiger Name zugewiesen. Der Name enthält beschreibende Informationen zu den behandelten Themen der Vertrauenswürdigkeitskomponente. Jede Vertrauenswürdigkeitskomponente ist in eine Vertrauenswürdigkeitsfamilie eingeordnet, die ihre Sicherheitszielsetzung teilt.

Außerdem wird eine eindeutige Kurzform für den Namen der Vertrauenswürdigkeitskomponente bereitgestellt. Diese ist das vorrangige Mittel zur Verweisung auf die Vertrauenswürdigkeitskomponente. Die festgelegte Konvention ist, dass die Kurzform des Familiennamens verwendet wird, gefolgt von einem Punkt und einem numerischen Zeichen. Die numerischen Zeichen für Komponenten innerhalb einer Familie werden fortlaufend zugewiesen, beginnend bei 1.

6.4.3 Ziele

Falls vorhanden, enthält der Unterabschnitt „Ziele“ der Vertrauenswürdigkeitskomponente bestimmte Ziele für die jeweilige Vertrauenswürdigkeitskomponente. Bei Vertrauenswürdigkeitskomponenten, die diesen Unterabschnitt aufweisen, werden hier der besondere Zweck der Komponente und eine ausführlichere Erklärung der Ziele dargestellt.

6.4.4 Anwendungshinweise

Falls vorhanden, enthält der Unterabschnitt „Anwendungshinweise“ der Vertrauenswürdigkeitskomponente zusätzliche Informationen, um die Verwendung der Komponente zu erleichtern.

6.4.5 Abhängigkeiten

Wenn eine Komponente für sich genommen nicht ausreichend und auf das Vorhandensein einer anderen Komponente angewiesen ist, entstehen Abhängigkeiten unter Vertrauenswürdigkeitskomponenten.

Jede Vertrauenswürdigkeitskomponente bietet eine vollständige Liste an Abhängigkeiten zu anderen Vertrauenswürdigkeitskomponenten. Manche Komponenten können auch „keine Abhängigkeiten“ aufführen, um anzuzeigen, dass keine Abhängigkeiten identifiziert wurden. Die abhängigen Komponenten können Abhängigkeiten zu weiteren Komponenten haben.

Die Abhängigkeitsliste identifiziert die minimale Reihe an Vertrauenswürdigkeitskomponenten, auf die sich verlassen wird. Komponenten, die zu einer Komponente in der Abhängigkeitsliste hierarchisch sind, dürfen auch zur Erfüllung der Abhängigkeit verwendet werden.

In bestimmten Situationen ist es möglich, dass die angegebenen Abhängigkeiten nicht anwendbar sind. Durch die Angabe einer Begründung, warum eine bestimmte Abhängigkeit nicht anwendbar ist, darf der Autor eines PP, PP-Moduls, einer PP-Konfiguration oder einer ST auch auswählen, dass die Abhängigkeit nicht erfüllt wird.

6.4.6 Vertrauenswürdigkeitselemente

Für jede Vertrauenswürdigkeitskomponente wird eine Reihe an Vertrauenswürdigkeitselementen bereitgestellt. Ein Vertrauenswürdigkeitselement ist eine Sicherheitsanforderung, die bei weiterer Aufteilung zu keinem sinnvollen Evaluierungsergebnis führen würde. Es ist die kleinste Einheit der in der Normenreihe ISO/IEC 15408 angegebenen Sicherheitsanforderungen.

Jedes Vertrauenswürdigkeitselement wird als zu einer der drei Sätze an Vertrauenswürdigkeitselementen zugehörig identifiziert:

- a) Elemente der Entwickleraktionen: die Aktivitäten, die vom Entwickler ausgeführt werden müssen. Dieser Satz an Aktionen wird über das in den folgenden Elementsätzen verwiesene Nachweismaterial weiter

qualifiziert. Anforderungen für Entwickleraktionen werden über Anhängen des Buchstabens „D“ (en: developer) an die Elementnummer identifiziert.

- b) Elemente von Inhalt und Darstellung des Nachweises: der erforderliche Nachweis, was der Nachweis darlegen muss und welche Informationen der Nachweis vermitteln muss. Anforderungen für Inhalt und Darstellung des Nachweises werden über Anhängen des Buchstabens „C“ (en: content) an die Elementnummer identifiziert.
- c) Elemente der Evaluatoraktionen: die Aktivitäten, die vom Evaluator ausgeführt werden müssen. Dieser Satz an Aktionen enthält explizit die Bestätigung, dass die vorgeschriebenen Anforderungen in den Elementen zu Inhalt und Darstellung des Nachweises erfüllt wurden. Er enthält außerdem explizite Aktionen und Analyse, die zusätzlich zu den bereits vom Entwickler ausgeführten Aktionen durchgeführt werden müssen. Implizite Evaluatoraktionen müssen ebenfalls als Ergebnis von Elementen zu Entwickleraktionen durchgeführt werden, die nicht von Anforderungen zu Inhalt und Darstellung des Nachweises abgedeckt sind. Anforderungen für Evaluatoraktionen werden über Anhängen des Buchstabens „E“ (en: evaluator) an die Elementnummer identifiziert.

Die Entwickleraktionen und Inhalt und Darstellung des Nachweises definieren die Vertrauenswürdigkeitsanforderungen, die zur Abbildung der Verantwortung des Entwicklers zum Nachweis der Vertrauenswürdigkeit des TOE zur Erfüllung der SFRs eines PP, PP-Moduls, einer PP-Konfiguration oder einer ST verwendet wird.

Die Evaluatoraktionen definieren die Verantwortung des Evaluators bei zwei Aspekten der Evaluierung. Der erste Aspekt ist die Validierung des PP, PP-Moduls, der PP-Konfiguration oder der ST in Übereinstimmung mit den Klassen ACE, APE und ASE in den Abschnitten „ACE: „ACE: Protection Profile Configuration evaluation“, „APE: Protection Profile evaluation“ und „ASE: Security Target evaluation“. Der zweite Aspekt ist die Verifizierung der Konformität des TOE mit seinen SFRs und SARs. Durch den Nachweis, dass das PP, PP-Modul, die PP-Konfiguration oder die ST gültig ist und dass die Anforderungen vom TOE erfüllt werden, kann der Evaluator eine Grundlage für das Vertrauen schaffen, dass der TOE das definierte Sicherheitsproblem in seiner Betriebsumgebung löst.

Die Elemente der Entwickleraktionen, Elemente von Inhalt und Darstellung des Nachweises und die expliziten Elemente der Evaluatoraktionen identifizieren den Aufwand des Evaluators, der zum Verifizieren der in der ST des TOE gemachten Sicherheitsansprüche aufgebracht werden muss.

6.5 Vertrauenswürdigkeitselemente

Jedes Element stellt eine zu erfüllende Anforderung dar. Diese Aussagen zu Anforderungen sind auf Klarheit, Knappheit und Eindeutigkeit ausgelegt. Daher gibt es keine zusammengesetzten Sätze: jede trennbare Anforderung ist als einzelnes Element angegeben.

6.6 Komponententaxonomie

Dieses Dokument enthält Klassen von Familien und Komponenten, die auf Grundlage zusammengehöriger Vertrauenswürdigkeit gruppiert sind. Zu Beginn jeder Klasse gibt es ein Diagramm, das die Familien in der Klasse und die Komponenten in jeder Familie anzeigt.

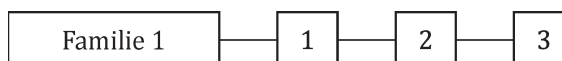


Bild 3 — Muster eines Klassenaufbaudiagramms

Bild 3 zeigt eine Klasse, die eine einzige Familie enthält. Die Familie enthält drei Komponenten, die linear hierarchisch sind (d. h. Komponente 2 erfordert mehr als Komponente 1 bezüglich bestimmter Aktionen, bestimmter Nachweise oder Strenge der Aktionen oder der Nachweise). Die Vertrauenswürdigkeitsfamilien in diesem Dokument sind alle linear hierarchisch, wobei Linearität kein verpflichtendes Kriterium für Vertrauenswürdigkeitsfamilien ist, die möglicherweise zukünftig hinzugefügt werden.

7 Klasse APE: Evaluierung des Schutzprofils (PP)

7.1 Allgemeines

Evaluierung eines PP ist erforderlich zum Nachweis, dass ein PP sachgerecht und in sich konsistent ist und, wenn das PP auf einem oder mehreren anderen PPs oder Paketen basiert, dass das PP eine korrekte Instanziierung dieser PPs und Pakete darstellt. Diese Eigenschaften sind erforderlich, damit das PP für die Verwendung als Grundlage zum Schreiben einer ST oder anderer PPs geeignet ist.

Abschnitt 7 sollte in Verbindung mit ISO/IEC 15408-1:2022, Anhang B und Anhang D, verwendet werden, da diese Anhänge die hier dargestellten Konzepte verdeutlichen und eine Vielzahl an Beispielen zeigen.

Bild 4 zeigt die Familien in dieser Klasse sowie die Hierarchie der Komponenten innerhalb der Familien.

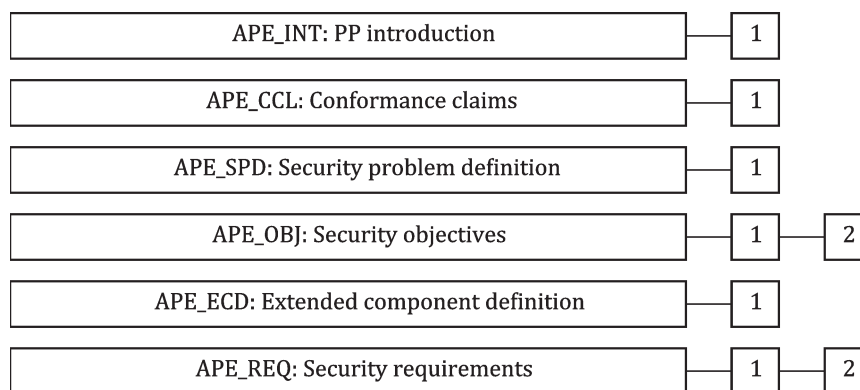


Bild 4 — APE: Evaluierung des Schutzprofils (PP), Klassenaufbau

7.2 PP-Einleitung (APE_INT)

7.2.1 Ziele

Das Ziel dieser Familie ist die ausformulierte Beschreibung des TOE.

Evaluierung der PP-Einleitung ist erforderlich, um nachzuweisen, dass das PP korrekt identifiziert wurde und dass die PP-Verweisung und der TOE-Überblick konsistent miteinander sind.

7.2.2 APE_INT.1 PP-Einleitung

Abhängigkeiten: keine Abhängigkeiten.

Entwickleraktionselemente

APE_INT.1.1D

Der Entwickler muss eine PP-Einleitung bereitstellen.

Elemente von Inhalt und Darstellung

APE_INT.1.1C

Die PP-Einleitung muss eine PP-Verweisung und einen TOE-Überblick enthalten.

APE_INT.1.2C

Die PP-Verweisung muss das PP eindeutig identifizieren.

APE_INT.1.3C

Der TOE-Überblick muss die Verwendung und wesentliche Sicherheitsmerkmale des TOE zusammenfassen.

APE_INT.1.4C

Der TOE-Überblick muss den TOE-Typ identifizieren.

APE_INT.1.5C

Der TOE-Überblick muss jede nicht im TOE enthaltene, aber für den TOE verfügbare Hardware/Software/Firmware identifizieren.

Evaluatorenaktionselemente

APE_INT.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

7.3 Konformitätsansprüche (APE_CCL)

7.3.1 Ziele

Das Ziel dieser Familie ist die Bestimmung der Gültigkeit des Konformitätsanspruchs. Zusätzlich spezifiziert diese Familie, wie STs und andere PPs Konformität mit dem PP beanspruchen müssen.

7.3.2 APE_CCL.1 Konformitätsansprüche

Abhängigkeiten: „APE_INT.1 PP introduction“

— „APE_ECD.1 Extended components definition“

— „APE_REQ.1 Direct rationale PP-Module security requirements“

Entwickleraktionselemente

APE_CCL.1.1D

Der Entwickler muss einen Konformitätsanspruch bereitstellen.

APE_CCL.1.2D

Der Entwickler muss eine Begründung zum Konformitätsanspruch bereitstellen.

APE_CCL.1.3D

Der Entwickler muss eine Konformitätserklärung bereitstellen.

Elemente von Inhalt und Darstellung

APE_CCL.1.1C

Der Konformitätsanspruch muss die Ausgabe der ISO/IEC 15408 identifizieren, mit der das PP Konformität beansprucht.

APE_CCL.1.2C

Der Konformitätsanspruch muss die Konformität des PP mit ISO/IEC 15408-2 entweder als ISO/IEC 15408-2-konform oder ISO/IEC 15408-2-erweitert beschreiben.

APE_CCL.1.3C

Der Konformitätsanspruch muss die Konformität des PP entweder als „ISO/IEC 15408-3-konform“ oder als „ISO/IEC 15408-3-erweitert“ beschreiben.

APE_CCL.1.4C

Der Konformitätsanspruch muss mit der erweiterten Komponentendefinition konsistent sein.

APE_CCL.1.5C

Der Konformitätsanspruch muss alle PPs und Pakete identifizieren, mit denen das PP Konformität beansprucht.

APE_CCL.1.6C

Der Konformitätsanspruch muss jede Konformität des PP mit einem Funktionspaket als eine der folgenden beschreiben: Paket-konform, Paket-ergänzt oder Paket-angepasst.

APE_CCL.1.7C

Der Konformitätsanspruch muss jede Konformität des PP mit einem Vertrauenswürdigkeitspaket entweder als Paket-konform oder als Paket-ergänzt beschreiben.

APE_CCL.1.8C

Der Konformitätsanspruch muss jede Konformität des PP mit einem anderen PP als PP-konform beschreiben.

APE_CCL.1.9C

Die Begründung für den Konformitätsanspruch muss nachweisen, dass der TOE-Typ mit dem TOE-Typ in den PP konsistent ist, für die Konformität beansprucht wird.

APE_CCL.1.10C

Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zur Sicherheitsproblemdefinition mit der Aussage zur Sicherheitsproblemdefinition in den PP und allen Funktionspaketen konsistent ist, für die Konformität beansprucht wird.

APE_CCL.1.11C

Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zu den Sicherheitszielsetzungen mit der Aussage zu den Sicherheitszielsetzungen in den PPs und allen Funktionspaketen konsistent ist, für die Konformität beansprucht wird.

APE_CCL.1.12C

Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zu den Sicherheitsanforderungen mit der Aussage zu den Sicherheitsanforderungen in den PPs und allen Funktionspaketen konsistent ist, für die Konformität beansprucht wird.

APE_CCL.1.13C

Die Konformitätserklärung muss die geforderte Konformität aller PPs/STs mit dem PP als genaue PP-Konformität, strikte PP-Konformität oder nachweisliche PP-Konformität beschreiben.

APE_CCL.1.14C

Für eine genaue Konformitäts-PP muss die Konformitätserklärung eine Zulässigkeitsaussage enthalten, die die Menge des PP (falls vorhanden) identifiziert, für den in Kombination mit dem zu evaluierenden PP eine genaue Konformität beansprucht werden kann.

APE_CCL.1.15C

Für ein genaues Konformitäts-PP muss die Konformitätserklärung eine Zulässigkeitsaussage enthalten, in der die Reihe von PP-Modulen (falls vorhanden) angegeben ist, die mit dem zu evaluierenden PP in einer PP-Konfiguration verwendet werden dürfen.

APE_CCL.1.16C

Die Konformitätserklärung muss den Satz von abgeleiteten Evaluierungsverfahren und Evaluierungsaufgaben (falls vorhanden) angeben, die mit dem zu evaluierenden PP verwendet werden müssen. Diese Liste muss Folgendes enthalten:

- alle Evaluierungsverfahren und Evaluierungsaufgaben, die für das zu evaluierende PP festgelegt sind;
- alle Evaluierungsverfahren und Evaluierungsaufgaben, die in Konformitätserklärungen der PP festgelegt sind, mit denen Konformität des zu evaluierenden PP beansprucht wird;
- alle Evaluierungsverfahren und Evaluierungsaufgaben, die in den Abschnitten über die Sicherheitsanforderungen der Pakete festgelegt sind, mit denen Konformität des zu evaluierenden PP beansprucht wird.

Evaluatorenaktionselemente

APE_CCL.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

7.4 Sicherheitsproblemdefinition (APE_SPD)

7.4.1 Ziele

Dieser Teil des PPs definiert das vom TOE zu behandelnde Sicherheitsproblem und die Betriebsumgebung des TOE.

Evaluierung der Sicherheitsproblemdefinition ist erforderlich, um nachzuweisen, dass das vom TOE zu behandelnde Sicherheitsproblem und seine Betriebsumgebung klar definiert sind.

7.4.2 APE_SPD.1 Sicherheitsproblemdefinition

Abhängigkeiten: keine Abhängigkeiten.

Entwickleraktionselemente

APE_SPD.1.1D

Der Entwickler muss eine Sicherheitsproblemdefinition bereitstellen.

Elemente von Inhalt und Darstellung

APE_SPD.1.1C

Die Sicherheitsproblemdefinition muss die Bedrohungen beschreiben.

APE_SPD.1.2C

Alle Bedrohungen müssen in Bezug auf einen Bedrohungsagenten, einen Vermögenswert und eine unerwünschte Aktion beschrieben werden.

APE_SPD.1.3C

Die Sicherheitsproblemdefinition muss die organisatorischen Sicherheitsrichtlinien (OSP) beschreiben.

APE_SPD.1.4C

Die Sicherheitsproblemdefinition muss die Annahmen über die Betriebsumgebung des TOE beschreiben.

Evaluatorenaktionselemente

APE_SPD.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

7.5 Sicherheitszielsetzungen (APE_OBJ)

7.5.1 Ziele

Die Sicherheitszielsetzungen sind eine präzise Aussage zur angestrebten Antwort auf das Sicherheitsproblem, das durch die Familie „Security problem definition“ (APE_SPD) definiert ist.

Evaluierung der Sicherheitszielsetzungen ist erforderlich, um nachzuweisen, dass die Sicherheitszielsetzungen die Sicherheitsproblemdefinition angemessen und vollständig behandeln und dass die Aufteilung dieses Problems zwischen dem TOE seiner Betriebsumgebung klar definiert ist.

7.5.2 Komponentenebenen

Die Komponenten in dieser Familie sind danach eingestuft, ob sie nur Sicherheitszielsetzungen für die Betriebsumgebung oder auch Sicherheitszielsetzungen für den TOE vorschreiben.

7.5.3 APE_OBJ.1 Sicherheitszielsetzungen für die Betriebsumgebung

Abhängigkeiten: keine Abhängigkeiten.

Entwickleraktionselemente

APE_OBJ.1.1D

Der Entwickler muss eine Aussage zu Sicherheitszielsetzungen für die Betriebsumgebung bereitstellen.

APE_OBJ.1.2D

Der Entwickler muss eine Begründung für die Sicherheitszielsetzungen in der Betriebsumgebung bereitstellen.

Elemente von Inhalt und Darstellung

APE_OBJ.1.1C

Die Aussage zu den Sicherheitszielsetzungen muss die Sicherheitszielsetzungen für die Betriebsumgebung beschreiben.

APE_OBJ.1.2C

Die Begründung für die Sicherheitszielsetzungen muss jede Sicherheitszielsetzung für die Betriebsumgebung zu den Bedrohungen zurückführen, die durch diese Sicherheitszielsetzung abgewehrt werden, zu den OSPs, die durch diese Sicherheitszielsetzung durchgesetzt werden, und zu den Annahmen, die durch diese Sicherheitszielsetzung eingehalten werden.

APE_OBJ.1.3C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen für die Betriebsumgebung alle Annahmen einhalten.

Evaluatorenaktionselemente

APE_OBJ.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

7.5.4 APE_OBJ.2 Sicherheitszielsetzungen

Abhängigkeiten: „APE_SPD.1 Security problem definition“.

Entwickleraktionselemente

APE_OBJ.2.1D

Der Entwickler muss eine Aussage zu Sicherheitszielsetzungen bereitstellen.

APE_OBJ.2.2D

Der Entwickler muss eine Begründung für die Sicherheitszielsetzungen bereitstellen.

Elemente von Inhalt und Darstellung

APE_OBJ.2.1C

Die Aussage zu Sicherheitszielsetzungen muss die Sicherheitszielsetzungen für den **TOE und die Sicherheitszielsetzungen** für die Betriebsumgebung beschreiben.

APE_OBJ.2.2C

Die Begründung für die Sicherheitszielsetzungen muss jede Sicherheitszielsetzung für den TOE zurückführen zu den Bedrohungen, die durch diese Sicherheitszielsetzung abgewehrt werden und zu den OSPs, die durch diese Sicherheitszielsetzung durchgesetzt werden.

APE_OBJ.2.3C

Die Begründung für die Sicherheitszielsetzungen muss jede Sicherheitszielsetzung für die Betriebsumgebung zu den Bedrohungen zurückführen, die durch diese Sicherheitszielsetzung abgewehrt werden, zu den OSPs, die durch diese Sicherheitszielsetzung durchgesetzt werden, und zu den Annahmen, die durch diese Sicherheitszielsetzung eingehalten werden.

APE_OBJ.2.4C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen alle Bedrohungen abwehren.

APE_OBJ.2.5C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen alle OSPs durchsetzen.

APE_OBJ.2.6C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen für die Betriebsumgebung alle Annahmen einhalten.

Evaluatorenaktionselemente

APE_OBJ.2.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

7.6 Erweiterte Komponentendefinition (APE_ECD)

7.6.1 Ziele

Erweiterte Sicherheitsanforderungen sind Anforderungen, die nicht auf Komponenten aus ISO/IEC 15408-2 oder diesem Dokument basieren, sondern auf vom PP-Autor definierten erweiterten Komponenten.

Evaluierung der Definition von erweiterten Komponenten ist erforderlich zur Bestimmung, dass sie klar und eindeutig sind und dass sie erforderlich sind, d. h. sie können unter Verwendung bestehender Komponenten von ISO/IEC 15408-2 oder Komponenten dieses Dokuments nicht klar formuliert werden.

7.6.2 APE_ECD.1 Erweiterte Komponentendefinition

Abhängigkeiten: keine Abhängigkeiten.

Entwickleraktionselemente

APE_ECD.1.1D

Der Entwickler muss eine Aussage zu Sicherheitsanforderungen bereitstellen.

APE_ECD.1.2D

Der Entwickler muss eine erweiterte Komponentendefinition bereitstellen.

Elemente von Inhalt und Darstellung

APE_ECD.1.1C

Die Aussage zu den Sicherheitsanforderungen muss alle erweiterten Sicherheitsanforderungen identifizieren.

APE_ECD.1.2C

Die erweiterte Komponentendefinition muss für jede erweiterte Sicherheitsanforderung eine erweiterte Komponente definieren.

APE_ECD.1.3C

Die erweiterte Komponentendefinition muss beschreiben, wie jede erweiterte Komponente mit den bestehenden Komponenten, Familien und Klassen der Normenreihe ISO/IEC 15408 in Beziehung steht.

APE_ECD.1.4C

Die erweiterte Komponentendefinition muss die bestehenden Komponenten, Familien, Klassen und die Methodik der Normenreihe ISO/IEC 15408 als ein Modell der Darstellung verwenden.

APE_ECD.1.5C

Die erweiterten Komponenten müssen aus messbaren und objektiven Elementen bestehen, sodass Konformität oder Nichtkonformität mit diesen Elementen nachgewiesen werden kann.

Evaluatorenaktionselemente

APE_ECD.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

APE_ECD.1.2E

Der Evaluator *muss bestätigen*, dass keine erweiterte Komponente unter Verwendung bestehender Komponenten klar formuliert werden kann.

7.7 Sicherheitsanforderungen (APE_REQ)

7.7.1 Ziele

Die SFRs bilden eine deutliche, eindeutige und klar definierte Beschreibung des erwarteten Sicherheitsverhaltens des TOE. Die SARs bilden eine deutliche, eindeutige und klar definierte Beschreibung der erwarteten Aktivitäten, die zur Gewinnung der Vertrauenswürdigkeit im TOE unternommen werden.

Evaluierung der Sicherheitsanforderungen ist erforderlich, um sicherzustellen, dass sie deutlich, eindeutig und klar definiert sind.

7.7.2 Komponentenebenen

Die Komponenten in dieser Familie sind danach eingestuft, ob die SFRs aus der SDP abgeleitet werden oder ob die SFRs aus Sicherheitszielsetzungen für den TOE abgeleitet werden.

7.7.3 APE_REQ.1 Sicherheitsanforderungen des PP-Moduls mit direkter Begründung

Abhängigkeiten: „APE_ECD.1 Extended components definition“

— „APE_OBJ.1 Security objectives for the operational environment“

Entwickleraktionselemente

APE_REQ.1.1D

Der Entwickler muss eine Aussage zu Sicherheitsanforderungen bereitstellen.

APE_REQ.1.2D

Der Entwickler muss eine Begründung für die Sicherheitsanforderungen bereitstellen.

Elemente von Inhalt und Darstellung

APE_REQ.1.1C

Die Aussage zu den Sicherheitsanforderungen muss die SFRs und die SARs beschreiben.

APE_REQ.1.2C

Alle Subjekte, Objekte, Operationen, Sicherheitsattribute, externen Entitäten und andere in den SFRs und SARs verwendeten Begriffe müssen definiert sein.

APE_REQ.1.3C

Die Aussage zu den Sicherheitsanforderungen muss alle Operationen im Zusammenhang mit den Sicherheitsanforderungen identifizieren.

APE_REQ.1.4C

Alle Operationen müssen korrekt durchgeführt werden.

APE_REQ.1.5C

Jede Abhängigkeit der Sicherheitsanforderungen muss entweder erfüllt sein, oder die Begründung für die Sicherheitsanforderungen muss rechtfertigen, dass die Abhängigkeit nicht erfüllt wird.

APE_REQ.1.6C

Die Begründung für die Sicherheitsanforderungen muss jede SFR auf die Bedrohungen zurückführen, die durch diese SFR und die durch diese SFR durchgesetzten OSP abgewehrt werden.

APE_REQ.1.7C

Die Begründung der Sicherheitsanforderungen muss nachweisen, dass die SFRs (in Verbindung mit den Sicherheitszielsetzungen für die Systemumgebung) alle Bedrohungen für den TOE abwehren.

APE_REQ.1.8C

Die Begründung der Sicherheitsanforderungen muss nachweisen, dass die SFRs (in Verbindung mit den Sicherheitszielsetzungen für die Systemumgebung) alle OSP für den TOE durchsetzen.

APE_REQ.1.9C

Die Begründung für die Sicherheitsanforderungen muss erklären, warum die SARs ausgewählt wurden.

APE_REQ.1.10C

Die Aussage zu den Sicherheitsanforderungen muss in sich konsistent sein.

Evaluatorenaktionselemente

APE_REQ.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

7.7.4 APE_REQ.2 Abgeleitete Sicherheitsanforderungen

Abhängigkeiten: „APE_OBJ.2 Security objectives“

— „APE_ECD.1 Extended components definition“

Entwickleraktionselemente

APE_REQ.2.1D

Der Entwickler muss eine Aussage zu Sicherheitsanforderungen bereitstellen.

APE_REQ.2.2D

Der Entwickler muss eine Begründung für die Sicherheitsanforderungen bereitstellen.

Elemente von Inhalt und Darstellung

APE_REQ.2.1C

Die Aussage zu den Sicherheitsanforderungen muss die SFRs und die SARs beschreiben.

APE_REQ.2.2C

Alle Subjekte, Objekte, Operationen, Sicherheitsattribute, externen Entitäten und andere in den SFRs und SARs verwendeten Begriffe müssen definiert sein.

APE_REQ.2.3C

Die Aussage zu den Sicherheitsanforderungen muss alle Operationen im Zusammenhang mit den Sicherheitsanforderungen identifizieren.

APE_REQ.2.4C

Alle Operationen müssen korrekt durchgeführt werden.

APE_REQ.2.5C

Jede Abhängigkeit der Sicherheitsanforderungen muss entweder erfüllt sein, oder die Begründung für die Sicherheitsanforderungen muss rechtfertigen, dass die Abhängigkeit nicht erfüllt wird.

APE_REQ.2.6C

Die Begründung für die Sicherheitsanforderungen muss jede SFR zu den Sicherheitszielsetzungen für den TOE zurückverfolgen, die durch diese SFR durchgesetzt werden.

APE_REQ.2.7C

Die Begründung für die Sicherheitsanforderungen muss nachweisen, dass die SFRs alle Sicherheitszielsetzungen für den TOE erfüllen.

APE_REQ.2.8C

Die Begründung für die Sicherheitsanforderungen muss erklären, warum die SARs ausgewählt wurden.

APE_REQ.2.9C

Die Aussage zu den Sicherheitsanforderungen muss in sich konsistent sein.

Evaluatorenaktionselemente

APE_REQ.2.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

8 Klasse ACE: Evaluierung der Schutzprofilkonfiguration

8.1 Allgemeines

Die Evaluierung einer PP-Konfiguration ist erforderlich, um nachzuweisen, dass die PP-Konfiguration sachgemäß und konsistent ist. Diese Eigenschaften sind erforderlich, damit die PP-Konfiguration für die Verwendung als Grundlage zum Schreiben einer ST geeignet ist.

Die Klasse ACE ist für die Evaluierung einer PP-Konfiguration definiert, die aus mindestens einem PP und einer weiteren Komponente (PP und/oder PP-Modulen) besteht. Die Evaluierung der PP wird in Klasse APE behandelt. Die Klasse ACE definiert die Anforderungen für:

- Evaluierung der PP-Module im Rahmen ihrer PP-Modulbasis/-basen (Komponenten ACE_INT.1, ACE_CCL.1, ACE_SPD.1, ACE_OBJ.1 oder ACE_OBJ.2, ACE_REQ.1 oder ACE_REQ.2, und ACE_MCO.1).
- Evaluierung der Konsistenz der Kombination aller PP und PP-Module, die zur PP-Konfiguration gehören (siehe ACE_CCO.1).

Abschnitt 8 sollte in Verbindung mit ISO/IEC 15408-1:2022, Anhang C, verwendet werden.

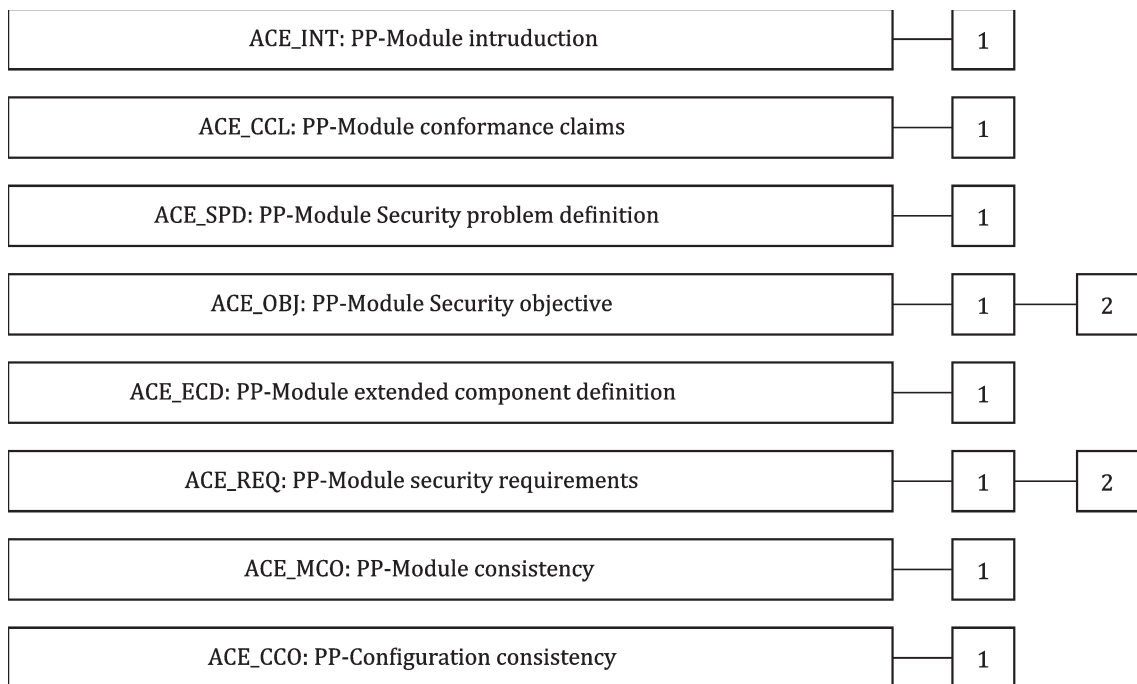


Bild 5 — ACE: Evaluierung der Schutzprofilkonfiguration, Klassenaufbau

8.2 Einleitung für PP-Module (ACE_INT)

8.2.1 Ziele

Das Ziel dieser Familie ist die ausformulierte Beschreibung des TOE.

Die Evaluierung der Einleitung für PP-Module ist erforderlich, um nachzuweisen, dass das PP-Modul korrekt identifiziert wurde und dass die PP-Modulverweisung und der TOE-Überblick konsistent miteinander sind.

8.2.2 ACE_INT.1 Einleitung für PP-Module

Abhängigkeiten: keine Abhängigkeiten.

Entwickleraktionselemente

ACE_INT.1.1D

Der Entwickler muss eine Einleitung für PP-Module bereitstellen.

Elemente von Inhalt und Darstellung

ACE_INT.1.1C

Die Einleitung für PP-Module muss eine PP-Modulverweisung, die Identifizierung der PP-Modulbasis/-basen und einen TOE-Überblick enthalten.

ACE_INT.1.2C

Die PP-Modulverweisung muss das PP-Modul eindeutig identifizieren.

ACE_INT.1.3C

Die Identifizierung der PP-Modulbasis muss aus einer Liste mit mindestens einem PP und möglicherweise anderen PP und PP-Modulen bestehen, von denen das PP-Modul abhängt.

ACE_INT.1.4C

Die Identifizierung der PP-Modulbasis/-basen muss die Abhängigkeitsstruktur der PP-Modulbasis/-basen beschreiben.

ACE_INT.1.5C

Die Einleitung für PP-Module muss so viele TOE-Überblicke enthalten wie alternative PP-Modulbasen.

ACE_INT.1.6C

Der TOE-Überblick muss die Verwendung und wesentliche Sicherheitsmerkmale des TOE zusammenfassen.

ACE_INT.1.7C

Der TOE-Überblick muss den TOE-Typ identifizieren.

ACE_INT.1.8C

Der TOE-Überblick muss jede nicht im TOE enthaltene, aber für den TOE verfügbare Hardware/Software/Firmware identifizieren.

ACE_INT.1.9C

Der TOE-Überblick muss die Unterschiede des TOE im Hinblick auf die in der/den PP-Modulbasis/-basen definierten TOE beschreiben.

Evaluatorenaktionselemente

ACE_INT.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

8.3 Konformitätsansprüche des PP-Moduls (ACE_CCL)

8.3.1 Ziele

Das Ziel dieser Familie ist die Bestimmung der Gültigkeit des Konformitätsanspruchs und der Konformitätserklärung. Ein PP-Modul kann keinen Anspruch auf Konformität mit einem PP, einer PP-Konfiguration oder einem anderen PP-Modul erheben.

8.3.2 ACE_CCL.1 Konformitätsansprüche des PP-Moduls

Abhängigkeiten: „ACE_INT.1 PP-Module introduction“

— „ACE_ECD.1 PP-Module extended components definition“

— „ACE_REQ.1 PP-Module stated security requirements“ oder „ACE_REQ.2 PP-Module derived security requirements“

Entwickleraktionselemente

ACE_CCL.1.1D

Der Entwickler muss einen Konformitätsanspruch bereitstellen.

ACE_CCL.1.2D

Der Entwickler muss eine Konformitätserklärung bereitstellen.

Elemente von Inhalt und Darstellung

ACE_CCL.1.1C

Der Konformitätsanspruch muss die Ausgabe der ISO/IEC 15408 identifizieren, mit der das PP-Modul Konformität beansprucht.

ACE_CCL.1.2C

Der Konformitätsanspruch muss die Konformität des PP-Moduls mit ISO/IEC 15408-2 entweder als ISO/IEC 15408-2-konform oder ISO/IEC 15408-2-erweitert beschreiben.

ACE_CCL.1.3C

Die Konformitätserklärung muss den Typ der Konformität beschreiben, der von jeder ST zum PP-Modul (als Teil einer PP-Konfiguration) verlangt wird, und zwar als genau, strikt oder nachweislich.

ACE_CCL.1.4C

Der Konformitätsanspruch muss die Konformität des PP-Moduls mit diesem Dokument entweder als „ISO/IEC 15408-3-konform“ oder als „ISO/IEC 15408-3-erweitert“ beschreiben.

ACE_CCL.1.5C

Der Konformitätsanspruch muss mit der erweiterten Komponentendefinition konsistent sein.

ACE_CCL.1.6C

Der Konformitätsanspruch muss alle Funktionspakete identifizieren, mit denen das PP-Modul Konformität beansprucht.

ACE_CCL.1.7C

Der Konformitätsanspruch muss jede Konformität des PP-Moduls mit einem Funktionspaket als entweder Paket-konform, Paket-ergänzt oder Paket-angepasst beschreiben.

ACE_CCL.1.8C

Der Konformitätsanspruch muss alle Sicherheitspakete identifizieren, mit denen das PP-Modul Konformität beansprucht.

ACE_CCL.1.9C

Der Konformitätsanspruch muss jede Konformität des PP-Moduls mit einem Vertrauenswürdigkeitspaket entweder als Paket-konform oder als Paket-ergänzt beschreiben.

ACE_CCL.1.10C

Für eine genaue Konformität muss die Konformitätserklärung des PP-Moduls eine Zulässigkeitsaussage enthalten, die die Menge der PP und PP-Module (mit Ausnahme der PP und PP-Module, die in der PP-Modulbasis enthalten sind) identifiziert, für die in Kombination mit dem zu evaluierenden PP-Modul eine genaue Konformität beansprucht werden kann.

ACE_CCL.1.11C

Die Konformitätserklärung kann die von ISO/IEC 18045 abgeleiteten Evaluierungsverfahren und Evaluierungsaufgaben angeben, die mit dem zu evaluierenden PP-Modul verwendet werden müssen. Diese Liste muss alle Evaluierungsverfahren und Evaluierungsaufgaben enthalten, die im PP-Modul festgelegt sind, aber auch alle Evaluierungsverfahren und Evaluierungsaufgaben, die in der/den PP-Modulbasis/-basen und/oder in den Paketen (falls vorhanden) festgelegt sind, für die das zu evaluierende PP-Modul Konformität beansprucht.

Evaluatorenaktionselemente

ACE_CCL.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

8.4 Sicherheitsproblemdefinition des PP-Moduls (ACE_SPD)

8.4.1 Ziele

Dieser Teil des PP-Moduls definiert das vom TOE zu behandelnde Sicherheitsproblem und die Betriebsumgebung des TOE.

Evaluierung der Sicherheitsproblemdefinition ist erforderlich, um nachzuweisen, dass das vom TOE zu behandelnde Sicherheitsproblem und seine Betriebsumgebung klar definiert sind.

8.4.2 ACE_SPD.1 Sicherheitsproblemdefinition des PP-Moduls

Abhängigkeiten: keine Abhängigkeiten.

Entwickleraktionselemente

ACE_SPD.1.1D

Der Entwickler muss eine Sicherheitsproblemdefinition bereitstellen.

Elemente von Inhalt und Darstellung

ACE_SPD.1.1C

Die Sicherheitsproblemdefinition muss die Bedrohungen beschreiben.

ACE_SPD.1.2C

Alle Bedrohungen müssen in Bezug auf einen Bedrohungsagenten, einen Vermögenswert und eine unerwünschte Aktion beschrieben werden.

ACE_SPD.1.3C

Die Sicherheitsproblemdefinition muss die OSPs beschreiben.

ACE_SPD.1.4C

Die Sicherheitsproblemdefinition muss die Annahmen über die Betriebsumgebung des TOE beschreiben.

Evaluatorenaktionselemente

ACE_SPD.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

8.5 Sicherheitszielsetzungen des PP-Moduls (ACE_OBJ)

8.5.1 Ziele

Die Sicherheitszielsetzungen sind eine präzise Aussage zur angestrebten Antwort auf das Sicherheitsproblem, das durch die Familie „Security problem definition“ (APE_SPD) definiert ist.

Evaluierung der Sicherheitszielsetzungen ist erforderlich, um nachzuweisen, dass die Sicherheitszielsetzungen die Sicherheitsproblemdefinition angemessen und vollständig behandeln und dass die Aufteilung dieses Problems zwischen dem TOE seiner Betriebsumgebung klar definiert ist.

8.5.2 Komponentenebenen

Die Komponenten in dieser Familie sind danach eingestuft, ob sie nur Sicherheitszielsetzungen für die Betriebsumgebung (siehe ACE_OBJ.1) oder auch Sicherheitszielsetzungen für den TOE (siehe ACE_OBJ.2) vorschreiben.

8.5.3 ACE_OBJ.1 Sicherheitszielsetzungen des PP-Moduls für die Betriebsumgebung

Abhängigkeiten: keine Abhängigkeiten.

Entwickleraktionselemente

ACE_OBJ.1.1D

Der Entwickler muss eine Aussage zu Sicherheitszielsetzungen für die Betriebsumgebung des PP-Moduls bereitstellen.

ACE_OBJ.1.2D

Der Entwickler muss eine Begründung für die Sicherheitszielsetzungen in der Betriebsumgebung des PP-Moduls bereitstellen.

Elemente von Inhalt und Darstellung

ACE_OBJ.1.1C

Die Aussage zu den Sicherheitszielsetzungen muss die Sicherheitszielsetzungen für die Betriebsumgebung beschreiben.

ACE_OBJ.1.2C

Die Begründung für die Sicherheitszielsetzungen muss jede Sicherheitszielsetzung für die Betriebsumgebung zu den Bedrohungen zurückführen, die durch diese Sicherheitszielsetzung abgewehrt werden, zu den OSPs, die durch diese Sicherheitszielsetzung durchgesetzt werden, und zu den Annahmen, die durch diese Sicherheitszielsetzung eingehalten werden.

ACE_OBJ.1.3C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen für die Betriebsumgebung alle Annahmen einhalten.

Evaluatorenaktionselemente

ACE_OBJ.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

8.5.4 ACE_OBJ.2 Sicherheitszielsetzungen des PP-Moduls

Abhängigkeiten: „ACE_SPD.1 PP-Module security problem definition“.

Entwickleraktionselemente

ACE_OBJ.2.1D

Der Entwickler muss eine Aussage zu Sicherheitszielsetzungen für das PP-Modul bereitstellen.

ACE_OBJ.2.2D

Der Entwickler muss eine Begründung für die Sicherheitszielsetzungen des PP-Moduls bereitstellen.

Elemente von Inhalt und Darstellung

ACE_OBJ.2.1C

Die Aussage zu den Sicherheitszielsetzungen muss die Sicherheitszielsetzungen für den TOE und die Sicherheitszielsetzungen für die Betriebsumgebung beschreiben.

ACE_OBJ.2.2C

Die Begründung für die Sicherheitszielsetzungen muss jede Sicherheitszielsetzung für den TOE zurückführen zu den Bedrohungen, die durch diese Sicherheitszielsetzung abgewehrt werden und zu den OSPs, die durch diese Sicherheitszielsetzung durchgesetzt werden.

ACE_OBJ.2.3C

Die Begründung für die Sicherheitszielsetzungen muss jede Sicherheitszielsetzung für die Betriebsumgebung zu den Bedrohungen zurückführen, die durch diese Sicherheitszielsetzung abgewehrt werden, zu den OSPs, die durch diese Sicherheitszielsetzung durchgesetzt werden, und zu den Annahmen, die durch diese Sicherheitszielsetzung eingehalten werden.

ACE_OBJ.2.4C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen alle Bedrohungen abwehren.

ACE_OBJ.2.5C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen alle OSPs durchsetzen.

ACE_OBJ.2.6C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen für die Betriebsumgebung alle Annahmen einhalten.

Evaluatorenaktionselemente

ACE_OBJ.2.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

8.6 Erweiterte Komponentendefinition des PP-Moduls (ACE_ECD)

8.6.1 Ziele

Erweiterte SFR sind Anforderungen, die nicht auf Komponenten aus ISO/IEC 15408-2 oder diesem Dokument basieren, sondern auf vom Autor eines PP-Moduls definierten erweiterten Komponenten.

Evaluierung der Definition von erweiterten Funktionskomponenten ist erforderlich zur Bestimmung, dass sie klar und eindeutig sind und dass sie erforderlich sind, d. h. sie können unter Verwendung bestehender Komponenten von ISO/IEC 15408-2 oder Komponenten dieses Dokuments nicht klar formuliert werden.

8.6.2 ACE_ECD.1 Erweiterte Komponentendefinition des PP-Moduls

Abhängigkeiten: keine Abhängigkeiten.

Entwickleraktionselemente

ACE_ECD.1.1D

Der Entwickler muss eine Aussage zu Sicherheitsanforderungen für das PP-Modul bereitstellen.

ACE_ECD.1.2D

Der Entwickler muss eine erweiterte Komponentendefinition für das PP-Modul bereitstellen.

Elemente von Inhalt und Darstellung

ACE_ECD.1.1C

Die Aussage zu den Sicherheitsanforderungen muss alle erweiterten Sicherheitsanforderungen identifizieren.

ACE_ECD.1.2C

Die erweiterte Komponentendefinition muss für jede erweiterte Sicherheitsanforderung eine erweiterte Komponente definieren.

ACE_ECD.1.3C

Die erweiterte Komponentendefinition muss beschreiben, wie jede erweiterte Komponente mit den bestehenden Komponenten, Familien und Klassen der Normenreihe ISO/IEC 15408 in Beziehung steht.

ACE_ECD.1.4C

Die erweiterte Komponentendefinition muss die bestehenden Komponenten, Familien, Klassen und die Methodik der Normenreihe ISO/IEC 15408 als ein Modell der Darstellung verwenden.

ACE_ECD.1.5C

Die erweiterten Komponenten müssen aus messbaren und objektiven Elementen bestehen, sodass Konformität oder Nichtkonformität mit diesen Elementen nachgewiesen werden kann.

Evaluatorenaktionselemente

ACE_ECD.1.1E

Der Evaluator *muss bestätigen*, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

ACE_ECD.1.2E

Der Evaluator *muss bestätigen*, dass keine erweiterte Komponente unter Verwendung bestehender Komponenten klar formuliert werden kann.

8.7 Sicherheitsanforderungen des PP-Moduls (ACE_REQ)

8.7.1 Ziele

Die SFRs bilden eine deutliche, eindeutige und klar definierte Beschreibung des erwarteten Sicherheitsverhaltens des TOE. Die SARs bilden eine deutliche, eindeutige und klar definierte Beschreibung der erwarteten Aktivitäten, die zur Gewinnung der Vertrauenswürdigkeit im TOE unternommen werden.

Evaluierung der Sicherheitsanforderungen ist erforderlich, um sicherzustellen, dass sie deutlich, eindeutig und klar definiert sind.

8.7.2 Komponentenebenen

Die Komponenten in dieser Familie sind danach eingestuft, ob die SFR aus der SDP abgeleitet werden (siehe ACE_REQ.1) oder ob die SFRs aus den Sicherheitszielsetzungen für den TOE abgeleitet werden (siehe ACE_REQ.2.).

8.7.3 ACE_REQ.1 Festgelegte Sicherheitsanforderungen des PP-Moduls

Abhängigkeiten: „APE_ECD.1 Extended components definition“

— „ACE_SPD.1 PP-Module security problem definition“

Entwickleraktionselemente

ACE_REQ.1.1D

Der Entwickler muss eine Aussage zu Sicherheitsanforderungen für das PP-Modul bereitstellen.

ACE_REQ.1.2D

Der Entwickler muss eine Begründung für die Sicherheitsanforderungen des PP-Moduls bereitstellen.