

DIN EN ISO/IEC 15408-3:2021-06 (D)

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

Inhalt	Seite
Europäisches Vorwort.....	9
Vorwort.....	10
Einleitung.....	12
1 Anwendungsbereich.....	13
2 Normative Verweisungen.....	13
3 Begriffe, Symbole und Abkürzungen.....	13
4 Übersicht.....	13
4.1 Aufbau dieses Teils von ISO/IEC 15408.....	13
5 Paradigma für Vertrauenswürdigkeit.....	14
5.1 Philosophie von ISO/IEC 15408.....	14
5.2 Ansatz für Vertrauenswürdigkeit.....	14
5.2.1 Bedeutung von Anfälligkeiten.....	14
5.2.2 Ursachen von Anfälligkeiten.....	15
5.2.3 ISO/IEC 15408 Vertrauenswürdigkeit.....	15
5.2.4 Vertrauenswürdigkeit durch Evaluierung.....	15
5.3 ISO/IEC 15408 Vertrauenswürdigkeitsskala.....	16
6 Vertrauenswürdigkeitskomponenten.....	16
6.1 Aufbau der Vertrauenswürdigkeitsklassen, -familien und -komponenten.....	16
6.1.1 Struktur der Vertrauenswürdigkeitsklassen.....	16
6.1.2 Struktur der Vertrauenswürdigkeitsfamilien.....	17
6.1.3 Struktur der Vertrauenswürdigkeitskomponenten.....	18
6.1.4 Vertrauenswürdigkeitselemente.....	20
6.1.5 Komponententaxonomie.....	20
6.2 Struktur der EAL-Stufen.....	21
6.2.1 Name der EAL-Stufe.....	21
6.2.2 Ziele.....	21
6.2.3 Anwendungshinweise.....	21
6.2.4 Vertrauenswürdigkeitskomponenten.....	22
6.2.5 Beziehung zwischen Vertrauenswürdigkeit und Vertrauenswürdigkeitsstufe.....	22
6.3 Struktur der CAPs.....	23
6.3.1 Name des CAPs.....	23
6.3.2 Ziele.....	23
6.3.3 Anwendungshinweise.....	23
6.3.4 Vertrauenswürdigkeitskomponenten.....	24
6.3.5 Beziehung zwischen Vertrauenswürdigkeit und Vertrauenswürdigkeitsstufe.....	24
7 Vertrauenswürdigkeitsstufen.....	25
7.1 Übersicht über die Vertrauenswürdigkeitsstufen (EAL-Stufen).....	25
7.2 Einzelheiten der Vertrauenswürdigkeitsstufen.....	27
7.3 Vertrauenswürdigkeitsstufe 1 (EAL1) – funktional geprüft.....	27
7.3.1 Ziele.....	27
7.3.2 Vertrauenswürdigkeitskomponenten.....	27
7.4 Vertrauenswürdigkeitsstufe 2 (EAL2) – strukturell geprüft.....	28

7.4.1	Ziele	28
7.4.2	Vertrauenswürdigkeitskomponenten.....	28
7.5	Vertrauenswürdigkeitsstufe 3 (EAL3) – methodisch geprüft und überprüft	29
7.5.1	Ziele	29
7.5.2	Vertrauenswürdigkeitskomponenten.....	29
7.6	Vertrauenswürdigkeitsstufe 4 (EAL4) – methodisch entwickelt, geprüft und überprüft	31
7.6.1	Ziele	31
7.6.2	Vertrauenswürdigkeitskomponenten.....	31
7.7	Vertrauenswürdigkeitsstufe 5 (EAL5) – semiformal entwickelt und geprüft.....	32
7.7.1	Ziele	32
7.7.2	Vertrauenswürdigkeitskomponenten.....	32
7.8	Vertrauenswürdigkeitsstufe 6 (EAL6) – semiformal verifiziertes Design und geprüft.....	33
7.8.1	Ziele	33
7.8.2	Vertrauenswürdigkeitskomponenten.....	34
7.9	Vertrauenswürdigkeitsstufe 7 (EAL7) – formal verifiziertes Design und geprüft.....	35
7.9.1	Ziele	35
7.9.2	Vertrauenswürdigkeitskomponenten.....	35
8	Zusammengesetzte Sicherheitspakete.....	36
8.1	Übersicht über die zusammengesetzten Sicherheitspakete (CAPs)	37
8.2	Einzelheiten zusammengesetzter Sicherheitspakete.....	38
8.3	Zusammengesetztes Sicherheitspaket A (CAP-A) – strukturell zusammengesetzt	38
8.3.1	Ziele	38
8.3.2	Vertrauenswürdigkeitskomponenten.....	39
8.4	Zusammengesetztes Sicherheitspaket B (CAP-B) – methodisch zusammengesetzt.....	39
8.4.1	Ziele	39
8.4.2	Vertrauenswürdigkeitskomponenten.....	40
8.5	Zusammengesetztes Sicherheitspaket C (CAP-C) – methodisch zusammengesetzt, geprüft und überprüft.....	41
8.5.1	Ziele	41
8.5.2	Vertrauenswürdigkeitskomponenten.....	41
9	Klasse APE: Evaluierung des Schutzprofils	42
9.1	PP-Einleitung (APE_INT)	43
9.1.1	Ziele	43
9.1.2	APE_INT.1 PP-Einleitung.....	43
9.2	Konformitätsansprüche (APE_CCL)	44
9.2.1	Ziele	44
9.2.2	APE_CCL.1 Konformitätsansprüche.....	44
9.3	Sicherheitsproblemdefinition (APE_SPD)	46
9.3.1	Ziele	46
9.3.2	APE_SPD.1 Sicherheitsproblemdefinition	46
9.4	Sicherheitszielsetzungen (APE_OBJ)	47
9.4.1	Ziele	47
9.4.2	Komponentenebenen	47
9.4.3	APE_OBJ.1 Sicherheitszielsetzungen für die Betriebsumgebung.....	47
9.4.4	APE_OBJ.2 Sicherheitszielsetzungen	47
9.5	Erweiterte Komponentendefinition (APE_ECD).....	48
9.5.1	Ziele	48
9.5.2	APE_ECD.1 Erweiterte Komponentendefinition.....	49
9.6	Sicherheitsanforderungen (APE_REQ)	50
9.6.1	Ziele	50
9.6.2	Komponentenebenen	50
9.6.3	APE_REQ.1 Festgelegte Sicherheitsanforderungen.....	50
9.6.4	APE_REQ.2 Abgeleitete Sicherheitsanforderungen.....	51
10	Klasse ASE: Evaluierung der Sicherheitsvorgabe	52
10.1	ST-Einleitung (ASE_INT)	53
10.1.1	Ziele	53

10.1.2	ASE_INT.1 ST-Einleitung.....	53
10.2	Konformitätsansprüche (ASE_CCL)	54
10.2.1	Ziele	54
10.2.2	ASE_CCL.1 Konformitätsansprüche	54
10.3	Sicherheitsproblemdefinition (ASE_SPD).....	56
10.3.1	Ziele	56
10.3.2	ASE_SPD.1 Sicherheitsproblemdefinition.....	56
10.4	Sicherheitszielsetzungen (ASE_OBJ)	57
10.4.1	Ziele	57
10.4.2	Komponentenebenen.....	57
10.4.3	ASE_OBJ.1 Sicherheitszielsetzungen für die Betriebsumgebung	57
10.4.4	ASE_OBJ.2 Sicherheitszielsetzungen	57
10.5	Erweiterte Komponentendefinition (ASE_ECD)	59
10.5.1	Ziele	59
10.5.2	ASE_ECD.1 Erweiterte Komponentendefinition	59
10.6	Sicherheitsanforderungen (ASE_REQ).....	60
10.6.1	Ziele	60
10.6.2	Komponentenebenen.....	60
10.6.3	ASE_REQ.1 Festgelegte Sicherheitsanforderungen.....	60
10.6.4	ASE_REQ.2 Abgeleitete Sicherheitsanforderungen	61
10.7	Zusammenfassende Spezifikation des TOEs (ASE_TSS)	62
10.7.1	Ziele	62
10.7.2	Komponentenebenen.....	62
10.7.3	ASE_TSS.1 Zusammenfassende Spezifikation des TOEs	63
10.7.4	ASE_TSS.2 Zusammenfassende Spezifikation des TOEs mit zusammenfassendem Architekturdesign	63
11	Klasse ADV: Entwicklung	64
11.1	Sicherheitsarchitektur (ADV_ARC)	69
11.1.1	Ziele	69
11.1.2	Komponentenebenen.....	69
11.1.3	Anwendungshinweise.....	70
11.1.4	ADV_ARC.1 Beschreibung der Sicherheitsarchitektur	70
11.2	Funktionsspezifikation (ADV_FSP)	71
11.2.1	Ziele	71
11.2.2	Komponentenebenen.....	72
11.2.3	Anwendungshinweise.....	72
11.2.4	ADV_FSP.1 Grundlegende Funktionsanforderungen	75
11.2.5	ADV_FSP.2 Sicherheit durchsetzende Funktionsspezifikation.....	75
11.2.6	ADV_FSP.3 Funktionsspezifikation mit vollständiger Zusammenfassung.....	76
11.2.7	ADV_FSP.4 Vollständige Funktionsspezifikation	78
11.2.8	ADV_FSP.5 Vollständige semiformale Funktionsspezifikation mit zusätzlichen Fehlerinformationen.....	79
11.2.9	ADV_FSP.6 Vollständige semiformale Funktionsspezifikation mit zusätzlicher formaler Spezifikation	80
11.3	Darstellung der Implementierung (ADV_IMP).....	81
11.3.1	Ziele	81
11.3.2	Komponentenebenen.....	82
11.3.3	Anwendungshinweise.....	82
11.3.4	ADV_IMP.1 Darstellung der Implementierung der TSF.....	83
11.3.5	ADV_IMP.2 Vollständige Zuordnung der Darstellung der Implementierung der TSF.....	84
11.4	TSF-Interna (ADV_INT)	84
11.4.1	Ziele	84
11.4.2	Komponentenebenen.....	85
11.4.3	Anwendungshinweise.....	85
11.4.4	ADV_INT.1 Wohlstrukturierte Teilmengen von TSF-Interna	85
11.4.5	ADV_INT.2 Wohlstrukturierte Interna	86
11.4.6	ADV_INT.3 Minimal komplexe Interna	87

11.5	Modellierung der Sicherheitspolitik (ADV_SPM)	88
11.5.1	Ziele	88
11.5.2	Komponentenebenen	89
11.5.3	Anwendungshinweise	89
11.5.4	ADV_SPM.1 Formales TOE-Sicherheitspolitikmodell	90
11.6	TOE-Design (ADV_TDS)	91
11.6.1	Ziele	91
11.6.2	Komponentenebenen	91
11.6.3	Anwendungshinweise	91
11.6.4	ADV_TDS.1 Grundsätzliches Design	92
11.6.5	ADV_TDS.2 Architekturdesign	94
11.6.6	ADV_TDS.3 Grundsätzliches modulares Design	95
11.6.7	ADV_TDS.4 Semiformales modulares Design	96
11.6.8	ADV_TDS.5 Vollständiges semiformales modulares Design	98
11.6.9	ADV_TDS.6 Vollständiges semiformales modulares Design mit formaler allgemeiner Designdarstellung	99
12	Klasse AGD: Leitliniendokumente	100
12.1	Operative Leitlinien für Benutzer (AGD_OPE)	101
12.1.1	Ziele	101
12.1.2	Komponentenebenen	101
12.1.3	Anwendungshinweise	101
12.1.4	AGD_OPE.1 Operative Leitlinien für Benutzer	102
12.2	Vorbereitende Verfahren (AGD_PRE)	103
12.2.1	Ziele	103
12.2.2	Komponentenebenen	103
12.2.3	Anwendungshinweise	103
12.2.4	AGD_PRE.1 Vorbereitende Verfahren	104
13	Klasse ALC: Unterstützung des Lebenszyklus	104
13.1	CM-Funktionen (ALC_CMC)	105
13.1.1	Ziele	105
13.1.2	Komponentenebenen	106
13.1.3	Anwendungshinweise	106
13.1.4	ALC_CMC.1 Kennzeichnung des TOEs	107
13.1.5	ALC_CMC.2 Verwendung eines CM-Systems	107
13.1.6	ALC_CMC.3 Autorisierungskontrollen	108
13.1.7	ALC_CMC.4 Herstellungsunterstützung, Abnahmeverfahren und Automatisierung	110
13.1.8	ALC_CMC.5 Erweiterte Unterstützung	112
13.2	CM-Umfang (ALC_CMS)	115
13.2.1	Ziele	115
13.2.2	Komponentenebenen	115
13.2.3	Anwendungshinweise	115
13.2.4	ALC_CMS.1 CM-Abdeckung des TOEs	115
13.2.5	ALC_CMS.2 CM-Abdeckung für Teile des TOEs	116
13.2.6	ALC_CMS.3 CM-Abdeckung für die Darstellung der Implementierung	117
13.2.7	ALC_CMS.4 CM-Abdeckung für die Problemverfolgung	118
13.2.8	ALC_CMS.5 CM-Abdeckung für Entwicklungswerkzeuge	118
13.3	Lieferung (ALC_DEL)	120
13.3.1	Ziele	120
13.3.2	Komponentenebenen	120
13.3.3	Anwendungshinweise	120
13.3.4	ALC_DEL.1 Lieferverfahren	120
13.4	Entwicklungssicherheit (ALC_DVS)	121
13.4.1	Ziele	121
13.4.2	Komponentenebenen	121
13.4.3	Anwendungshinweise	121
13.4.4	ALC_DVS.1 Identifikation von Sicherheitsmaßnahmen	122
13.4.5	ALC_DVS.2 Angemessenheit von Sicherheitsmaßnahmen	122

13.5	Mängelbeseitigung (ALC_FLR)	123
13.5.1	Ziele	123
13.5.2	Komponentenebenen	123
13.5.3	Anwendungshinweise	123
13.5.4	ALC_FLR.1 Grundlegende Mängelbeseitigung	124
13.5.5	ALC_FLR.2 Verfahren zu Mängelberichten	124
13.5.6	ALC_FLR.3 Systematische Mängelbeseitigung	126
13.6	Definition des Lebenszyklus (ALC_LCD)	128
13.6.1	Ziele	128
13.6.2	Komponentenebenen	128
13.6.3	Anwendungshinweise	128
13.6.4	ALC_LCD.1 Vom Entwickler definiertes Lebenszyklusmodell	129
13.6.5	ALC_LCD.2 Messbares Lebenszyklusmodell	129
13.7	Werkzeuge und Techniken (ALC_TAT)	130
13.7.1	Ziele	130
13.7.2	Komponentenebenen	130
13.7.3	Anwendungshinweise	130
13.7.4	ALC_TAT.1 Genau festgelegte Entwicklungswerkzeuge	131
13.7.5	ALC_TAT.2 Konformität mit Implementierungsstandards	131
13.7.6	ALC_TAT.3 Konformität mit Implementierungsstandards - alle Teile	132
14	Klasse ATE: Prüfungen	133
14.1	Abdeckung (ATE_COV)	134
14.1.1	Ziele	134
14.1.2	Komponentenebenen	134
14.1.3	Anwendungshinweise	134
14.1.4	ATE_COV.1 Nachweis der Abdeckung	134
14.1.5	ATE_COV.2 Analyse der Abdeckung	135
14.1.6	ATE_COV.3 Strenge Analyse der Abdeckung	136
14.2	Tiefe (ATE_DPT)	136
14.2.1	Ziele	136
14.2.2	Komponentenebenen	137
14.2.3	Anwendungshinweise	137
14.2.4	ATE_DPT.1 Prüfung: grundlegendes Design	137
14.2.5	ATE_DPT.2 Prüfung: sicherheit-durchsetzende Module	138
14.2.6	ATE_DPT.3 Prüfung: modulares Design	139
14.2.7	ATE_DPT.4 Prüfung: Darstellung der Implementierung	139
14.3	Funktionsprüfungen (ATE_FUN)	140
14.3.1	Ziele	140
14.3.2	Komponentenebenen	141
14.3.3	Anwendungshinweise	141
14.3.4	ATE_FUN.1 Funktionsprüfung	141
14.3.5	ATE_FUN.2 Geordnete Funktionsprüfungen	142
14.4	Unabhängiges Prüfen (ATE_IND)	143
14.4.1	Ziele	143
14.4.2	Komponentenebenen	143
14.4.3	Anwendungshinweise	143
14.4.4	ATE_IND.1 Unabhängige Prüfungen - Konformität	144
14.4.5	ATE_IND.2 Unabhängige Prüfungen - Stichprobe	145
14.4.6	ATE_IND.3 Unabhängige Prüfungen - vollständig	146
15	Klasse AVA: Anfälligkeitsbewertung	147
15.1	Anwendungshinweise	147
15.2	Anfälligkeitsanalyse (AVA_VAN)	148
15.2.1	Ziele	148
15.2.2	Komponentenebenen	148
15.2.3	AVA_VAN.1 Anfälligkeitsuntersuchung	148
15.2.4	AVA_VAN.2 Anfälligkeitsanalyse	149
15.2.5	AVA_VAN.3 Konzentrierte Anfälligkeitsanalyse	150

15.2.6	AVA_VAN.4 Methodische Anfälligkeitsanalyse	151
15.2.7	AVA_VAN.5 Erweiterte methodische Anfälligkeitsanalyse	152
16	Klasse ACO: Zusammensetzung	153
16.1	Begründung der Zusammensetzung (ACO_COR).....	156
16.1.1	Ziele	156
16.1.2	Komponentenebenen	156
16.1.3	ACO_COR.1 Begründung der Zusammensetzung.....	156
16.2	Entwicklungsnachweis (ACO_DEV).....	157
16.2.1	Ziele	157
16.2.2	Komponentenebenen	157
16.2.3	Anwendungshinweise.....	157
16.2.4	ACO_DEV.1 Funktionsbeschreibung.....	158
16.2.5	ACO_DEV.2 Einfacher Nachweis des Designs	158
16.2.6	ACO_DEV.3 Detaillierter Nachweis des Designs	159
16.3	Verlässlichkeit der abhängigen Komponente (ACO_REL)	160
16.3.1	Ziele	160
16.3.2	Komponentenebenen	161
16.3.3	Anwendungshinweise.....	161
16.3.4	ACO_REL.1 Einfache Verlässlichkeitsinformation	161
16.3.5	ACO_REL.2 Verlässlichkeitsinformation	162
16.4	Prüfen des zusammengesetzten TOEs (ACO_CTT).....	163
16.4.1	Ziele	163
16.4.2	Komponentenebenen	163
16.4.3	Anwendungshinweise.....	163
16.4.4	ACO_CTT.1 Schnittstellenprüfung.....	163
16.4.5	ACO_CTT.2 Strenge Schnittstellenprüfung.....	165
16.5	Anfälligkeitsanalyse der Zusammensetzung (ACO_VUL)	166
16.5.1	Ziele	166
16.5.2	Komponentenebenen	166
16.5.3	Anwendungshinweise.....	166
16.5.4	ACO_VUL.1 Anfälligkeitsüberprüfung der Zusammensetzung	167
16.5.5	ACO_VUL.2 Anfälligkeitsanalyse der Zusammensetzung	167
16.5.6	ACO_VUL.3 Erweitert-einfache Anfälligkeitsanalyse der Zusammensetzung.....	168
	Anhang A (informativ) Entwicklung (ADV)	170
A.1	Ergänzende Informationen zu ADV_ARC: Sicherheitsarchitekturen	170
A.1.1	Sicherheitsarchitektureigenschaften	170
A.1.2	Sicherheitsarchitekturbeschreibungen.....	171
A.2	ADV_FSP: Ergänzende Informationen zu TSFIs	173
A.2.1	Bestimmen der TSFI	174
A.2.2	Beispiel: Ein komplexes DBMS.....	176
A.2.3	Beispiel-Funktionsspezifikation	178
A.3	ADV_INT: Ergänzende Informationen zu TSF-Interna.....	179
A.3.1	Struktur von prozeduraler Software	180
A.3.2	Komplexität von prozeduraler Software.....	182
A.4	ADV_TDS: Teilsysteme und Module.....	182
A.4.1	Teilsysteme	182
A.4.2	Module	183
A.4.3	Ansatz zur Einstufung.....	186
A.5	Ergänzende Informationen zu formalen Methoden.....	188
	Anhang B (informativ) Zusammensetzung (ACO)	190
B.1	Notwendigkeit für Evaluierungen zusammengesetzter TOEs	190
B.2	Durchführung der Evaluierung von Sicherheitsvorgaben für einen zusammengesetzten TOE.....	192
B.3	Interaktionen zwischen zusammengesetzten IT-Entitäten.....	192
	Anhang C (informativ) Querverweisung von Abhängigkeiten der Vertrauenswürdigkeitskomponenten.....	198

Anhang D (informativ) Querverweisung von PPs und Vertrauenswürdigkeitskomponenten.....	203
Anhang E (informativ) Querverweisung von EAL-Stufen und Vertrauenswürdigkeitskomponenten.....	204
Anhang F (informativ) Querverweisung von CAPs und Vertrauenswürdigkeitskomponenten.....	205