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

Erscheinungsdatum: 2024-03-22

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Evaluationskriterien für IT-Sicherheit - Teil 2: Sicherheitsfunktionskomponenten (ISO/IEC 15408-2:2022); Deutsche und Englische Fassung EN ISO/IEC 15408-2:2023

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components (ISO/IEC 15408-2:2022); German and English version EN ISO/IEC 15408-2:2023

Inhalt

Seite

Europäisches Vorwort ... **28**

Vorwort ... **29**

Einleitung ... **31**

1 Anwendungsbereich ... **32**

2 Normative Verweisungen ... **32**

3 Begriffe ... **32**

4 Abkürzungen ... **34**

5 Übersicht ... **35**
5.1 Allgemeines ... **35**
5.2 Aufbau dieses Dokuments ... **36**

6 Paradigma für Funktionsanforderungen ... **36**

7 Sicherheitsfunktionskomponenten ... **41**
7.1 Übersicht ... **41**
7.1.1 Allgemeines ... **41**
7.1.2 Klassenstruktur ... **41**
7.1.3 Familienstruktur ... **42**
7.1.4 Komponentenstruktur ... **44**
7.2 Komponentenkatalog ... **45**

8 Klasse FAU: Sicherheitsaudit ... **46**
8.1 Klassenbeschreibung ... **46**
8.2 Automatische Antwort beim Sicherheitsaudit (FAU_ARP) ... **47**
8.2.1 Familienverhalten ... **47**
8.2.2 Komponentenebenen und Beschreibung ... **47**
8.2.3 Management von FAU_ARP.1 ... **47**
8.2.4 Audit von FAU_ARP.1 ... **48**
8.2.5 FAU_ARP.1 Sicherheitsalarme ... **48**
8.3 Datengenerierung beim Sicherheitsaudit (FAU_GEN) ... **48**
8.3.1 Familienverhalten ... **48**
8.3.2 Komponentenebenen und Beschreibung ... **48**
8.3.3 Management von FAU_GEN.1, FAU_GEN.2 ... **48**
8.3.4 Audit von FAU_GEN.1, FAU_GEN.2 ... **49**
8.3.5 FAU_GEN.1 Generierung von Auditdaten ... **49**
8.3.6 FAU_GEN.2 Verknüpfung der Benutzeridentität ... **49**
8.4 Sicherheitsauditanalyse (FAU_SAA) ... **50**
8.4.1 Familienverhalten ... **50**
8.4.2 Komponentenebenen und Beschreibung ... **50**
8.4.3 Management von FAU_SAA.1 ... **50**

8.4.4 Management von FAU_SAA.2 ... 51
8.4.5 Management von FAU_SAA.3 ... 51
8.4.6 Management von FAU_SAA.4 ... 51
8.4.7 Audit von FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4 ... 51
8.4.8 „FAU_SAA.1 Potential violation analysis“ ... 51
8.4.9 FAU_SAA.2 Profilbasierte Erkennung von Anomalien ... 52
8.4.10 FAU_SAA.3 Einfache Angriffsheuristiken ... 52
8.4.11 FAU_SAA.4 Komplexe Angriffsheuristiken ... 53
8.5 Sicherheitsauditüberprüfung (FAU_SAR) ... 53
8.5.1 Familienverhalten ... 53
8.5.2 Komponentenebenen und Beschreibung ... 53
8.5.3 Management von FAU_SAR.1 ... 54
8.5.4 Management von FAU_SAR.2, FAU_SAR.3 ... 54
8.5.5 Audit von FAU_SAR.1 ... 54
8.5.6 Audit von FAU_SAR.2 ... 54
8.5.7 Audit von FAU_SAR.3 ... 54
8.5.8 FAU_SAR.1 Auditüberprüfung ... 54
8.5.9 FAU_SAR.2 Beschränkte Auditüberprüfung ... 55
8.5.10 FAU_SAR.3 Auswählbare Auditüberprüfung ... 55
8.6 Sicherheitsaudit Ereignisauswahl (FAU_SEL) ... 55
8.6.1 Familienverhalten ... 55
8.6.2 Komponentenebenen und Beschreibung ... 55
8.6.3 Management von FAU_SEL.1 ... 55
8.6.4 Audit von FAU_SEL.1 ... 56
8.6.5 FAU_SEL.1 Auswählbares Audit ... 56
8.7 Sicherheitsaudit Datenspeicherung (FAU_STG) ... 56
8.7.1 Familienverhalten ... 56
8.7.2 Komponentenebenen und Beschreibung ... 56
8.7.3 Management von FAU_STG.1 ... 57
8.7.4 Management von FAU_STG.2 ... 57
8.7.5 Management von FAU_STG.3 ... 57
8.7.6 Management von FAU_STG.4 ... 57
8.7.7 Management von FAU_STG.5 ... 57
8.7.8 Audit von FAU_STG.1 ... 57
8.7.9 Audit von FAU_STG.2, FAU_STG.3 ... 57
8.7.10 Audit von FAU_STG.4 ... 58
8.7.11 Audit von FAU_STG.5 ... 58
8.7.12 FAU_STG.1 Speicherort der Auditdaten ... 58
8.7.13 FAU_STG.2 Geschützte Speicherung der Auditdaten ... 58
8.7.14 FAU_STG.3 Garantien zur Auditdatenverfügbarkeit ... 58
8.7.15 FAU_STG.4 Aktion bei möglichem Auditdatenverlust ... 59
8.7.16 FAU_STG.5 Verhinderung von Auditdatenverlust ... 59

9 Klasse FCO: Kommunikation ... 59
9.1 Klassenbeschreibung ... 59
9.2 Nichtabstreitbarkeit des Ursprungs (FCO_NRO) ... 60
9.2.1 Familienverhalten ... 60
9.2.2 Komponentenebenen und Beschreibung ... 60
9.2.3 Management von FCO_NRO.1, FCO_NRO.2 ... 60
9.2.4 Audit von FCO_NRO.1 ... 61
9.2.5 Audit von FCO_NRO.2 ... 61
9.2.6 FCO_NRO.1 Auswählbarer Ursprungsnachweis ... 61
9.2.7 FCO_NRO.2 Erzwungener Ursprungsnachweis ... 62
9.3 Nichtabstreitbarkeit des Empfangs (FCO_NRR) ... 62
9.3.1 Familienverhalten ... 62
9.3.2 Komponentenebenen und Beschreibung ... 62
9.3.3 Management von FCO_NRR.1, FCO_NRR.2 ... 62
9.3.4 Audit von FCO_NRR.1 ... 63

9.3.5 Audit von FCO_NRR.2 ... 63
9.3.6 FCO_NRR.1 Auswählbarer Empfangsnachweis ... 63
9.3.7 FCO_NRR.2 Erzwungener Empfangsnachweis ... 64

10 Klasse FCS: Kryptographische Unterstützung ... 64
10.1 Klassenbeschreibung ... 64
10.2 Verwaltung kryptographischer Schlüssel (FCS_CKM) ... 65
10.2.1 Familienverhalten ... 65
10.2.2 Komponentenebenen und Beschreibung ... 65
10.2.3 Management von FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6 ... 66
10.2.4 Audit von FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6 ... 66
10.2.5 FCS_CKM.1 Generierung kryptographischer Schlüssel ... 66
10.2.6 FCS_CKM.2 Verteilung kryptographischer Schlüssel ... 67
10.2.7 FCS_CKM.3 Zugriff auf kryptographische Schlüssel ... 67
10.2.8 FCS_CKM.4 Zerstörung kryptographischer Schlüssel ... 68
10.2.9 FCS_CKM.5 Ableitung kryptographischer Schlüssel ... 68
10.2.10 FCS_CKM.6 Zeitablauf und Ereignis der Zerstörung kryptographischer Schlüssel ... 68
10.3 Kryptographische Operation (FCS_COP) ... 69
10.3.1 Familienverhalten ... 69
10.3.2 Komponentenebenen und Beschreibung ... 69
10.3.3 Management von FCS_COP.1 ... 69
10.3.4 Audit von FCS_COP.1 ... 69
10.3.5 FCS_COP.1 Kryptographische Operation ... 70
10.4 Generierung von Zufallsbits (FCS_RBG) ... 70
10.4.1 Familienverhalten ... 70
10.4.2 Komponentenebenen und Beschreibung ... 70
10.4.3 Management von FCS_RBG.1, FCS_RBG.2, FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6 ... 71
10.4.4 Audit von FCS_RBG.1, FCS_RBG.2 ... 71
10.4.5 Audit von FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6 ... 71
10.4.6 FCS_RBG.1 Generierung von Zufallsbits (RBG) ... 71
10.4.7 FCS_RBG.2 Generierung von Zufallsbits (externes Seeding) ... 72
10.4.8 FCS_RBG.3 Generierung von Zufallsbits (internal seeding – single source) ... 72
10.4.9 FCS_RBG.4 Generierung von Zufallsbits (internes Seeding – mehrere Quellen) ... 73
10.4.10 FCS_RBG.5 Generierung von Zufallsbits (Kombination von Rauschquellen) ... 73
10.4.11 FCS_RBG.6 Dienst zur Generierung von Zufallsbits ... 73
10.5 Generierung von Zufallszahlen (FCS_RNG) ... 74
10.5.1 Familienverhalten ... 74
10.5.2 Komponentenebenen und Beschreibung ... 74
10.5.3 Management von FCS_RNG.1 ... 74
10.5.4 Audit von FCS_RNG.1 ... 74
10.5.5 FCS_RNG.1 Generierung von Zufallszahlen ... 74

11 Klasse FDP: Schutz von Benutzerdaten ... 75
11.1 Klassenbeschreibung ... 75
11.2 Zugriffskontrollpolitik (FDP_ACC) ... 77
11.2.1 Familienverhalten ... 77
11.2.2 Komponentenebenen und Beschreibung ... 78
11.2.3 Management von FDP_ACC.1, FDP_ACC.2 ... 78
11.2.4 Audit von FDP_ACC.1, FDP_ACC.2 ... 78
11.2.5 FDP_ACC.1 Zugriffskontrolle auf Teilmengen ... 78
11.2.6 FDP_ACC.2 Vollständige Zugriffskontrolle ... 78
11.3 Funktionen zur Zugriffskontrolle (FDP_ACF) ... 79
11.3.1 Familienverhalten ... 79
11.3.2 Komponentenebenen und Beschreibung ... 79
11.3.3 Management von FDP_ACF.1 ... 79
11.3.4 Audit von FDP_ACF.1 ... 79
11.3.5 FDP_ACF.1 Zugriffskontrolle auf Grundlage von Sicherheitsattributen ... 80
11.4 Datenauthentifizierung (FDP_DAU) ... 80
11.4.1 Familienverhalten ... 80

11.4.2 Komponentenebenen und Beschreibung ... 80
11.4.3 Management von FDP_DAU.1, FDP_DAU.2 ... 81
11.4.4 Audit von FDP_DAU.1 ... 81
11.4.5 Audit von FDP_DAU.2 ... 81
11.4.6 FDP_DAU.1 Einfache Datenauthentifizierung ... 81
11.4.7 FDP_DAU.2 Datenauthentifizierung mit Identität des Garantiegebers ... 82
11.5 Export aus dem TOE (FDP_ETC) ... 82
11.5.1 Familienverhalten ... 82
11.5.2 Komponentenebenen und Beschreibung ... 82
11.5.3 Management von FDP_ETC.1 ... 82
11.5.4 Management von FDP_ETC.2 ... 83
11.5.5 Audit von FDP_ETC.1, FDP_ETC.2 ... 83
11.5.6 FDP_ETC.1 Export von Benutzerdaten ohne Sicherheitsattribute ... 83
11.5.7 FDP_ETC.2 Export von Benutzerdaten mit Sicherheitsattributen ... 83
11.6 Informationsflusskontrollpolitik (FDP_IFC) ... 84
11.6.1 Familienverhalten ... 84
11.6.2 Komponentenebenen und Beschreibung ... 84
11.6.3 Management von FDP_IFC.1, FDP_IFC.2 ... 85
11.6.4 Audit von FDP_IFC.1, FDP_IFC.2 ... 85
11.6.5 FDP_IFC.1 Informationsflusskontrolle auf Teilmengen ... 85
11.6.6 FDP_IFC.2 Vollständige Informationsflusskontrolle ... 85
11.7 Funktionen zur Informationsflusskontrolle (FDP_IFF) ... 86
11.7.1 Familienverhalten ... 86
11.7.2 Komponentenebenen und Beschreibung ... 86
11.7.3 Management von FDP_IFF.1, FDP_IFF.2 ... 87
11.7.4 Management von FDP_IFF.3, FDP_IFF.4, FDP_IFF.5 ... 87
11.7.5 Management von FDP_IFF.6 ... 87
11.7.6 Audit von FDP_IFF.1, FDP_IFF.2, FDP_IFF.5 ... 87
11.7.7 Audit von FDP_IFF.3, FDP_IFF.4, FDP_IFF.6 ... 87
11.7.8 FDP_IFF.1 Einfache Sicherheitsattribute ... 88
11.7.9 FDP_IFF.2 Hierarchische Sicherheitsattribute ... 88
11.7.10 FDP_IFF.3 Eingeschränkte unerlaubte Informationsflüsse ... 89
11.7.11 FDP_IFF.4 Teilweise Verhinderung von unerlaubten Informationsflüssen ... 90
11.7.12 FDP_IFF.5 Keine unerlaubten Informationsflüsse ... 90
11.7.13 FDP_IFF.6 Überwachung unerlaubter Informationsflüsse ... 90
11.8 Kontrolle der Informationsspeicherung (FDP_IRC) ... 91
11.8.1 Familienverhalten ... 91
11.8.2 Komponentenebenen und Beschreibung ... 91
11.8.3 Management von FDP_IRC.1 ... 92
11.8.4 Audit von FDP_IRC.1 ... 92
11.8.5 FDP_IRC.1 Kontrolle der Informationsaufbewahrung ... 92
11.9 Import von außerhalb des TOEs (FDP_ITC) ... 92
11.9.1 Familienverhalten ... 92
11.9.2 Komponentenebenen und Beschreibung ... 92
11.9.3 Management von FDP_ITC.1, FDP_ITC.2 ... 93
11.9.4 Audit von FDP_ITC.1, FDP_ITC.2 ... 93
11.9.5 FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute ... 93
11.9.6 FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen ... 94
11.10 Interne TOE-Übertragung (FDP_ITT) ... 94
11.10.1 Familienverhalten ... 94
11.10.2 Komponentenebenen und Beschreibung ... 95
11.10.3 Management von FDP_ITT.1, FDP_ITT.2 ... 95
11.10.4 Management von FDP_ITT.3, FDP_ITT.4 ... 95
11.10.5 Audit von FDP_ITT.1, FDP_ITT.2 ... 95
11.10.6 Audit von FDP_ITT.3, FDP_ITT.4 ... 96
11.10.7 FDP_ITT.1 Einfacher interner Übertragungsschutz ... 96
11.10.8 FDP_ITT.2 Trennung der Übertragung durch Attribut ... 96
11.10.9 FDP_ITT.3 Integritätsüberwachung ... 97

11.10.10 FDP_ITT.4 Attributbasierte Integritätsüberwachung 97
11.11 Restinformationsschutz (FDP_RIP) 98
11.11.1 Familienverhalten 98
11.11.2 Komponentenebenen und Beschreibung 98
11.11.3 Management von FDP_RIP.1, FDP_RIP.2 98
11.11.4 Audit von FDP_RIP.1, FDP_RIP.2 98
11.11.5 FDP_RIP.1 Restinformationsschutz auf Teilmengen 98
11.11.6 FDP_RIP.2 Vollständiger Restinformationsschutz 99
11.12 Zurücksetzen (FDP_ROL) 99
11.12.1 Familienverhalten 99
11.12.2 Komponentenebenen und Beschreibung 99
11.12.3 Management von FDP_ROL.1, FDP_ROL.2 99
11.12.4 Audit von FDP_ROL.1, FDP_ROL.2 100
11.12.5 FDP_ROL.1 Einfaches Zurücksetzen 100
11.12.6 FDP_ROL.2 Erweitertes Zurücksetzen 100
11.13 Vertraulichkeit gespeicherter Daten (FDP_SDC) 101
11.13.1 Familienverhalten 101
11.13.2 Komponentenebenen und Beschreibung 101
11.13.3 Management von FDP_SDC.1, FDP_SDC.2 101
11.13.4 Audit von FDP_SDC.1, FDP_SDC.2 101
11.13.5 FDP_SDC.1 Vertraulichkeit gespeicherter Daten 101
11.13.6 FDP_SDC.2 Vertraulichkeit gespeicherter Daten mit zugehöriger Methode 102
11.14 Integrität gespeicherter Daten (FDP_SDI) 102
11.14.1 Familienverhalten 102
11.14.2 Komponentenebenen und Beschreibung 102
11.14.3 Management von FDP_SDI.1 102
11.14.4 Management von FDP_SDI.2 103
11.14.5 Audit von FDP_SDI.1 103
11.14.6 Audit von FDP_SDI.2 103
11.14.7 FDP_SDI.1 Überwachung der Integrität gespeicherter Daten 103
11.14.8 FDP_SDI.2 Überwachung der Integrität gespeicherter Daten und Aktionen 103
11.15 Inter-TSF-Schutz der Vertraulichkeit von Benutzerdaten bei Übertragung (FDP_UCT) 104
11.15.1 Familienverhalten 104
11.15.2 Komponentenebenen und Beschreibung 104
11.15.3 Management von FDP_UCT.1 104
11.15.4 Audit von FDP_UCT.1 104
11.15.5 FDP_UCT.1 Vertraulichkeit bei einfachem Datenaustausch 105
11.16 Inter-TSF-Schutz der Benutzerdatenintegrität bei Übertragung (FDP_UIT) 105
11.16.1 Familienverhalten 105
11.16.2 Komponentenebenen und Beschreibung 105
11.16.3 Management von FDP_UIT.1, FDP_UIT.2, FDP_UIT.3 106
11.16.4 Audit von FDP_UIT.1 106
11.16.5 Audit von FDP_UIT.2, FDP_UIT.3 106
11.16.6 FDP_UIT.1 Datenaustauschintegrität 106
11.16.7 FDP_UIT.2 Wiederherstellung bei Quelldatenaustausch 107
11.16.8 FDP_UIT.3 Wiederherstellung bei Zieldatenaustausch 107

12 Klasse FIA: Identifikation und Authentifizierung 108
12.1 Klassenbeschreibung 108
12.2 Authentifizierungsfehler (FIA_AFL) 109
12.2.1 Familienverhalten 109
12.2.2 Komponentenebenen und Beschreibung 109
12.2.3 Management von FIA_AFL.1 110
12.2.4 Audit von FIA_AFL.1 110
12.2.5 FIA_AFL.1 Handhabung von Authentifizierungsfehlern 110
12.3 Authentifizierungsnachweis der Identität (FIA_API) 110
12.3.1 Familienverhalten 110
12.3.2 Komponentenebenen und Beschreibung 110

12.3.3 Management von FIA_API.1 ... 111
12.3.4 Audit von FIA_API.1 ... 111
12.3.5 FIA_API.1 Authentifizierungsnachweis der Identität ... 111
12.4 Definition von Benutzerattributen (FIA_ATD) ... 111
12.4.1 Familienverhalten ... 111
12.4.2 Komponentenebenen und Beschreibung ... 111
12.4.3 Management von FIA_ATD.1 ... 111
12.4.4 Audit von FIA_ATD.1 ... 112
12.4.5 FIA_ATD.1 Definition von Benutzerattributen ... 112
12.5 Spezifikation von Sicherheitsinformationen (FIA_SOS) ... 112
12.5.1 Familienverhalten ... 112
12.5.2 Komponentenebenen und Beschreibung ... 112
12.5.3 Management von FIA_SOS.1 ... 112
12.5.4 Management von FIA_SOS.2 ... 112
12.5.5 Audit von FIA_SOS.1, FIA_SOS.2 ... 113
12.5.6 FIA_SOS.1 Verifizierung von Sicherheitsinformationen ... 113
12.5.7 FIA_SOS.2 Generierung von Sicherheitsinformationen durch die TSF ... 113
12.6 Benutzerauthentifizierung (FIA_UAU) ... 113
12.6.1 Familienverhalten ... 113
12.6.2 Komponentenebenen und Beschreibung ... 113
12.6.3 Management von FIA_UAU.1 ... 114
12.6.4 Management von FIA_UAU.2 ... 114
12.6.5 Management von FIA_UAU.3, FIA_UAU.4, FIA_UAU.7 ... 115
12.6.6 Management von FIA_UAU.5 ... 115
12.6.7 Management von FIA_UAU.6 ... 115
12.6.8 Management von FIA_UAU.7 ... 115
12.6.9 Audit von FIA_UAU.1 ... 115
12.6.10 Audit von FIA_UAU.2 ... 115
12.6.11 Audit von FIA_UAU.3 ... 115
12.6.12 Audit von FIA_UAU.4 ... 116
12.6.13 Audit von FIA_UAU.5 ... 116
12.6.14 Audit von FIA_UAU.6 ... 116
12.6.15 Audit von FIA_UAU.7 ... 116
12.6.16 FIA_UAU.1 Zeitpunkt der Authentifizierung ... 116
12.6.17 FIA_UAU.2 Benutzerauthentifizierung vor irgendeiner anderen Aktion ... 117
12.6.18 FIA_UAU.3 Fälschungssichere Authentifizierung ... 117
12.6.19 FIA_UAU.4 Einmaliger Authentifizierungsmechanismus ... 117
12.6.20 FIA_UAU.5 Mehrfachauthentifizierungsmechanismen ... 117
12.6.21 FIA_UAU.6 Erneute Authentifizierung ... 118
12.6.22 FIA_UAU.7 Geschützte Authentifizierungsrückmeldung ... 118
12.7 Benutzeridentifizierung (FIA_UID) ... 118
12.7.1 Familienverhalten ... 118
12.7.2 Komponentenebenen und Beschreibung ... 118
12.7.3 Management von FIA_UID.1 ... 119
12.7.4 Management von FIA_UID.2 ... 119
12.7.5 Audit von FIA_UID.1, FIA_UID.2 ... 119
12.7.6 FIA_UID.1 Zeitpunkt der Identifizierung ... 119
12.7.7 FIA_UID.2 Benutzeridentifizierung vor irgendeiner anderen Aktion ... 119
12.8 Benutzer-Subjekt-Bindung (FIA_USB) ... 120
12.8.1 Familienverhalten ... 120
12.8.2 Komponentenebenen und Beschreibung ... 120
12.8.3 Management von FIA_USB.1 ... 120
12.8.4 Audit von FIA_USB.1 ... 120
12.8.5 FIA_USB.1 Benutzer-Subjekt-Bindung ... 120

13 Klasse FMT: Sicherheitsmanagement ... 121
13.1 Klassenbeschreibung ... 121
13.2 Eingeschränkte Fähigkeiten und Verfügbarkeit (FMT_LIM) ... 122

13.2.1 Familienverhalten 122
13.2.2 Komponentenebenen und Beschreibung 122
13.2.3 Management von FMT_LIM.1, FMT_LIM.2 123
13.2.4 Audit von FMT_LIM.1 123
13.2.5 FMT_LIM.1 Eingeschränkte Fähigkeiten 123
13.2.6 FMT_LIM.2 Eingeschränkte Verfügbarkeit 123
13.3 Management von Funktionen in der TSF (FMT_MOF) 123
13.3.1 Familienverhalten 123
13.3.2 Komponentenebenen und Beschreibung 123
13.3.3 Management von FMT_MOF.1 124
13.3.4 Audit von FMT_MOF.1 124
13.3.5 FMT_MOF.1 Management des Verhaltens der Sicherheitsfunktionen 124
13.4 Management von Sicherheitsattributen (FMT_MSA) 124
13.4.1 Familienverhalten 124
13.4.2 Komponentenebenen und Beschreibung 124
13.4.3 Management von FMT_MSA.1 125
13.4.4 Management von FMT_MSA.2 125
13.4.5 Management von FMT_MSA.3 125
13.4.6 Management von FMT_MSA.4 125
13.4.7 Audit von FMT_MSA.1 126
13.4.8 Audit von FMT_MSA.2 126
13.4.9 Audit von FMT_MSA.3 126
13.4.10 Audit von FMT_MSA.4 126
13.4.11 FMT_MSA.1 Management von Sicherheitsattributen 126
13.4.12 FMT_MSA.2 Sichere Sicherheitsattribute 127
13.4.13 FMT_MSA.3 Statische Attributinitialisierung 127
13.4.14 FMT_MSA.4 Vererbung von Sicherheitsattributwerten 127
13.5 Management von TSF-Daten (FMT_MTD) 128
13.5.1 Familienverhalten 128
13.5.2 Komponentenebenen und Beschreibung 128
13.5.3 Management von FMT_MTD.1 128
13.5.4 Management von FMT_MTD.2 128
13.5.5 Management von FMT_MTD.3 128
13.5.6 Audit von FMT_MTD.1 129
13.5.7 Audit von FMT_MTD.2 129
13.5.8 Audit von FMT_MTD.3 129
13.5.9 FMT_MTD.1 Management von TSF-Daten 129
13.5.10 FMT_MTD.2 Management von Grenzen auf TSF-Daten 129
13.5.11 FMT_MTD.3 Sichere TSF-Daten 130
13.6 Widerruf (FMT_REV) 130
13.6.1 Familienverhalten 130
13.6.2 Komponentenebenen und Beschreibung 130
13.6.3 Management von FMT_REV.1 130
13.6.4 Audit von FMT_REV.1 131
13.6.5 FMT_REV.1 Widerruf 131
13.7 Ablauf von Sicherheitsattributen (FMT_SAE) 131
13.7.1 Familienverhalten 131
13.7.2 Komponentenebenen und Beschreibung 131
13.7.3 Management von FMT_SAE.1 131
13.7.4 Audit von FMT_SAE.1 132
13.7.5 FMT_SAE.1 Befristete Autorisierung 132
13.8 Spezifizierung von Managementfunktionen (FMT_SMF) 132
13.8.1 Familienverhalten 132
13.8.2 Komponentenebenen und Beschreibung 132
13.8.3 Management von FMT_SMF.1 133
13.8.4 Audit von FMT_SMF.1 133
13.8.5 FMT_SMF.1 Spezifizierung von Managementfunktionen 133
13.9 Sicherheitsmanagementrollen (FMT_SMR) 133

13.9.1 Familienverhalten 133
13.9.2 Komponentenebenen und Beschreibung 133
13.9.3 Management von FMT_SMR.1 134
13.9.4 Management von FMT_SMR.2 134
13.9.5 Management von FMT_SMR.3 134
13.9.6 Audit von FMT_SMR.1 134
13.9.7 Audit von FMT_SMR.2 134
13.9.8 Audit von FMT_SMR.3 134
13.9.9 FMT_SMR.1 Sicherheitsrollen 134
13.9.10 FMT_SMR.2 Einschränkungen zu Sicherheitsrollen 135
13.9.11 FMT_SMR.3 Übernahme von Rollen 135

14 Klasse FPR: Privatsphäre 135
14.1 Klassenbeschreibung 135
14.2 Anonymität (FPR_ANO) 136
14.2.1 Familienverhalten 136
14.2.2 Komponentenebenen und Beschreibung 136
14.2.3 Management von FPR_ANO.1, FPR_ANO.2 136
14.2.4 Audit von FPR_ANO.1, FPR_ANO.2 136
14.2.5 FPR_ANO.1 Anonymität 137
14.2.6 FPR_ANO.2 Anonymität ohne Anforderung von Informationen 137
14.3 Pseudonymität (FPR_PSE) 137
14.3.1 Familienverhalten 137
14.3.2 Komponentenebenen und Beschreibung 137
14.3.3 Management von FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 138
14.3.4 Audit von FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 138
14.3.5 FPR_PSE.1 Pseudonymität 138
14.3.6 FPR_PSE.2 Umkehrbare Pseudonymität 138
14.3.7 FPR_PSE.3 Alias-Pseudonymität 139
14.4 Unverknüpfbarkeit (FPR_UNL) 140
14.4.1 Familienverhalten 140
14.4.2 Komponentenebenen und Beschreibung 140
14.4.3 Management von FPR_UNL.1 140
14.4.4 Audit von FPR_UNL.1 140
14.4.5 FPR_UNL.1 Unverknüpfbarkeit von Operationen 140
14.5 Unbeobachtbarkeit (FPR_UNO) 141
14.5.1 Familienverhalten 141
14.5.2 Komponentenebenen und Beschreibung 141
14.5.3 Management von FPR_UNO.1, FPR_UNO.2 141
14.5.4 Management von FPR_UNO.3 141
14.5.5 Management von FPR_UNO.4 141
14.5.6 Audit von FPR_UNO.1, FPR_UNO.2 142
14.5.7 Audit von FPR_UNO.3 142
14.5.8 Audit von FPR_UNO.4 142
14.5.9 FPR_UNO.1 Unbeobachtbarkeit 142
14.5.10 FPR_UNO.2 Zuweisung von Informationen mit Einfluss auf Unbeobachtbarkeit 142
14.5.11 FPR_UNO.3 Unbeobachtbarkeit ohne Anforderung von Informationen 143
14.5.12 FPR_UNO.4 Autorisierte Benutzerbeobachtbarkeit 143

15 Klasse FPT: Schutz der TSF 143
15.1 Klassenbeschreibung 143
15.2 TOE-Emanation (FPT_EMS) 144
15.2.1 Familienverhalten 144
15.2.2 Komponentenebenen und Beschreibung 145
15.2.3 Management von FPT_EMS.1 145
15.2.4 Audit von FPT_EMS.1 145
15.2.5 FPT_EMS.1 Emanation der TSF und der Benutzerdaten 145
15.3 Sicherheit bei Ausfall (FPT_FLS) 146
15.3.1 Familienverhalten 146

15.3.2 Komponentenebenen und Beschreibung 146
15.3.3 Management von FPT_FLS.1 146
15.3.4 Audit von FPT_FLS.1 146
15.3.5 FPT_FLS.1 Ausfall mit Beibehaltung des sicheren Zustands 146
15.4 TSF-Initialisierung (FPT_INI) 146
15.4.1 Familienverhalten 146
15.4.2 Komponentenebenen und Beschreibung 146
15.4.3 Management von FPT_INI.1 147
15.4.4 Audit von FPT_INI.1 147
15.4.5 FPT_INI.1 TSF-Initialisierung 147
15.5 Verfügbarkeit von exportierten TSF-Daten (FPT_ITA) 148
15.5.1 Familienverhalten 148
15.5.2 Komponentenebenen und Beschreibung 148
15.5.3 Management von FPT_ITA.1 148
15.5.4 Audit von FPT_ITA.1 148
15.5.5 FPT_ITA.1 Inter-TSF-Verfügbarkeit innerhalb einer definierten Verfügbarkeitsmetrik 148
15.6 Vertraulichkeit der exportierten TSF-Daten (FPT_ITC) 149
15.6.1 Familienverhalten 149
15.6.2 Komponentenebenen und Beschreibung 149
15.6.3 Management von FPT_ITC.1 149
15.6.4 Audit von FPT_ITC.1 149
15.6.5 FPT_ITC.1 Inter-TSF-Vertraulichkeit während der Übertragung 149
15.7 Integrität exportierter TSF-Daten (FPT_ITI) 149
15.7.1 Familienverhalten 149
15.7.2 Komponentenebenen und Beschreibung 149
15.7.3 Management von FPT_ITI.1 150
15.7.4 Management von FPT_ITI.2 150
15.7.5 Audit von FPT_ITI.1 150
15.7.6 Audit von FPT_ITI.2 150
15.7.7 FPT_ITI.1 Inter-TSF-Erkennung von Änderungen 150
15.7.8 FPT_ITI.2 Inter-TSF-Erkennung und Korrektur von Änderungen 151
15.8 Interne TOE-TSF-Datenübertragung (FPT_ITT) 151
15.8.1 Familienverhalten 151
15.8.2 Komponentenebenen und Beschreibung 151
15.8.3 Management von FPT_ITT.1 152
15.8.4 Management von FPT_ITT.2 152
15.8.5 Management von FPT_ITT.3 152
15.8.6 Audit von FPT_ITT.1, FPT_ITT.2 152
15.8.7 Audit von FPT_ITT.3 152
15.8.8 FPT_ITT.1 Einfacher Schutz der TSF-Daten bei interner Übertragung 153
15.8.9 FPT_ITT.2 Trennung des TSF-Datentransfers 153
15.8.10 FPT_ITT.3 Überwachung der Integrität von TSF-Daten 153
15.9 Physischer Schutz der TSF (FPT_PHP) 154
15.9.1 Familienverhalten 154
15.9.2 Komponentenebenen und Beschreibung 154
15.9.3 Management von FPT_PHP.1 154
15.9.4 Management von FPT_PHP.2 154
15.9.5 Management von FPT_PHP.3 155
15.9.6 Audit von FPT_PHP.1 155
15.9.7 Audit von FPT_PHP.2 155
15.9.8 Audit von FPT_PHP.3 155
15.9.9 FPT_PHP.1 Passive Erkennung von physischen Angriffen 155
15.9.10 FPT_PHP.2 Mitteilung von physischen Angriffen 155
15.9.11 FPT_PHP.3 Widerstand gegen physische Angriffe 156
15.10 Vertrauenswürdige Wiederherstellung (FPT_RCV) 156
15.10.1 Familienverhalten 156
15.10.2 Komponentenebenen und Beschreibung 156
15.10.3 Management von FPT_RCV.1 157

15.10.4Management von FPT_RCV.2, FPT_RCV.3 157
15.10.5Management von FPT_RCV.4 157
15.10.6Audit von FPT_RCV.1, FPT_RCV.2, FPT_RCV.3 157
15.10.7Audit von FPT_RCV.4 157
15.10.8FPT_RCV.1 Manuelle Wiederherstellung 157
15.10.9FPT_RCV.2 Automatische Wiederherstellung 158
15.10.10FPT_RCV.3 Automatische Wiederherstellung ohne übermäßigen Verlust 158
15.10.11FPT_RCV.4 Funktionswiederherstellung 159
15.11 Erkennung von Wiederverwendung (FPT_RPL) 159
15.11.1Familienverhalten 159
15.11.2Komponentenebenen und Beschreibung 159
15.11.3Management von FPT_RPL.1 159
15.11.4Audit von FPT_RPL.1 159
15.11.5FPT_RPL.1 Erkennung von Wiederverwendung 160
15.12 Zustandssynchronitätsprotokoll (FPT_SSP) 160
15.12.1Familienverhalten 160
15.12.2Komponentenebenen und Beschreibung 160
15.12.3Management von FPT_SSP.1, FPT_SSP.2 160
15.12.4Audit von FPT_SSP.1, FPT_SSP.2 161
15.12.5FPT_SSP.1 Einfache vertrauenswürdige Bestätigung 161
15.12.6FPT_SSP.2 Gegenseitige vertrauenswürdige Bestätigung 161
15.13 Zeitstempel (FPT_STM) 161
15.13.1Familienverhalten 161
15.13.2Komponentenebenen und Beschreibung 161
15.13.3Management von FPT_STM.1 162
15.13.4Management von FPT_STM.2 162
15.13.5Audit von FPT_STM.1 162
15.13.6Audit von FPT_STM.2 162
15.13.7FPT_STM.1 Verlässliche Zeitstempel 162
15.13.8FPT_STM.2 Zeitquelle 162
15.14 Inter-TSF-TSF-Datenkonsistenz (FPT_TDC) 163
15.14.1Familienverhalten 163
15.14.2Komponentenebenen und Beschreibung 163
15.14.3Management von FPT_TDC.1 163
15.14.4Audit von FPT_TDC.1 163
15.14.5FPT_TDC.1 Einfache Inter-TSF-TSF-Datenkonsistenz 163
15.15 Prüfen von externen Entitäten (FPT_TEE) 164
15.15.1Familienverhalten 164
15.15.2Komponentenebenen und Beschreibung 164
15.15.3Management von FPT_TEE.1 164
15.15.4Audit von FPT_TEE.1 164
15.15.5FPT_TEE.1 Prüfen von externen Entitäten 164
15.16 Interne TOE-TSF-Datenreplizierungskonsistenz (FPT_TRC) 165
15.16.1Familienverhalten 165
15.16.2Komponentenebenen und Beschreibung 165
15.16.3Management von FPT_TRC.1 165
15.16.4Audit von FPT_TRC.1 165
15.16.5FPT_TRC.1 Interne TSF-Konsistenz 165
15.17 TSF-Selbstprüfung (FPT_TST) 166
15.17.1Familienverhalten 166
15.17.2Komponentenebenen und Beschreibung 166
15.17.3Management von FPT_TST.1 166
15.17.4Audit von FPT_TST.1 167
15.17.5FPT_TST.1 TSF-Selbstprüfung 167

16 Klasse FRU: Verwendung von Ressourcen 167
16.1 Klassenbeschreibung 167
16.2 Fehlertoleranz (FRU_FLT) 168

16.2.1 Familienverhalten ... 168
16.2.2 Komponentenebenen und Beschreibung ... 168
16.2.3 Management von FRU_FLT.1, FRU_FLT.2 ... 168
16.2.4 Audit von FRU_FLT.1 ... 168
16.2.5 Audit von FRU_FLT.2 ... 169
16.2.6 FRU_FLT.1 Verminderte Fehlertoleranz ... 169
16.2.7 FRU_FLT.2 Begrenzte Fehlertoleranz ... 169
16.3 Priorität von Diensten (FRU_PRS) ... 169
16.3.1 Familienverhalten ... 169
16.3.2 Komponentenebenen und Beschreibung ... 169
16.3.3 Management von FRU_PRS.1, FRU_PRS.2 ... 170
16.3.4 Audit von FRU_PRS.1, FRU_PRS.2 ... 170
16.3.5 FRU_PRS.1 Begrenzte Priorität von Diensten ... 170
16.3.6 FRU_PRS.2 Vollständige Priorität von Diensten ... 170
16.4 Ressourcenzuweisung (FRU_RSA) ... 170
16.4.1 Familienverhalten ... 170
16.4.2 Komponentenebenen und Beschreibung ... 171
16.4.3 Management von FRU_RSA.1 ... 171
16.4.4 Management von FRU_RSA.2 ... 171
16.4.5 Audit von FRU_RSA.1, FRU_RSA.2 ... 171
16.4.6 FRU_RSA.1 Höchstquoten ... 171
16.4.7 FRU_RSA.2 Mindestquoten und Höchstquoten ... 172

17 Klasse FTA: TOE-Zugriff ... 172
17.1 Klassenbeschreibung ... 172
17.2 Einschränkung des Umfangs auswählbarer Attribute (FTA_LSA) ... 173
17.2.1 Familienverhalten ... 173
17.2.2 Komponentenebenen und Beschreibung ... 173
17.2.3 Management von FTA_LSA.1 ... 173
17.2.4 Audit von FTA_LSA.1 ... 173
17.2.5 FTA_LSA.1 Einschränkung des Umfangs auswählbarer Attribute ... 173
17.3 Einschränkung von mehreren gleichzeitigen Sitzungen (FTA_MCS) ... 174
17.3.1 Familienverhalten ... 174
17.3.2 Komponentenebenen und Beschreibung ... 174
17.3.3 Management von FTA_MCS.1 ... 174
17.3.4 Management von FTA_MCS.2 ... 174
17.3.5 Audit von FTA_MCS.1, FTA_MCS.2 ... 174
17.3.6 FTA_MCS.1 Einfache Einschränkung von mehreren gleichzeitigen Sitzungen ... 174
17.3.7 FTA_MCS.2 Einschränkung von mehreren gleichzeitigen Sitzungen je Benutzerattribut ... 175
17.4 Sperren und Beenden von Sitzungen (FTA_SSL) ... 175
17.4.1 Familienverhalten ... 175
17.4.2 Komponentenebenen und Beschreibung ... 175
17.4.3 Management von FTA_SSL.1 ... 176
17.4.4 Management von FTA_SSL.2 ... 176
17.4.5 Management von FTA_SSL.3 ... 176
17.4.6 Management von FTA_SSL.4 ... 176
17.4.7 Audit von FTA_SSL.1, FTA_SSL.2 ... 176
17.4.8 Audit von FTA_SSL.3 ... 176
17.4.9 Audit von FTA_SSL.4 ... 177
17.4.10 FTA_SSL.1 Durch die TSF ausgelöstes Sperren der Sitzung ... 177
17.4.11 FTA_SSL.2 Durch den Benutzer ausgelöstes Sperren ... 177
17.4.12 FTA_SSL.3 Durch die TSF ausgelöstes Beenden ... 178
17.4.13 FTA_SSL.4 Durch den Benutzer ausgelöstes Beenden ... 178
17.5 TOE-Zugriffsbanner (FTA_TAB) ... 178
17.5.1 Familienverhalten ... 178
17.5.2 Komponentenebenen und Beschreibung ... 178
17.5.3 Management von FTA_TAB.1 ... 178
17.5.4 Audit von FTA_TAB.1 ... 178

17.5.5 FTA_TAB.1 Standard-TOE-Zugriffsbanner 179
17.6 TOE-Zugriffsverlauf (FTA_TAH) 179
17.6.1 Familienverhalten 179
17.6.2 Komponentenebenen und Beschreibung 179
17.6.3 Management von FTA_TAH.1 179
17.6.4 Audit von FTA_TAH.1 179
17.6.5 FTA_TAH.1 TOE-Zugriffsverlauf 179
17.7 TOE-Sitzungsaufbau (FTA_TSE) 180
17.7.1 Familienverhalten 180
17.7.2 Komponentenebenen und Beschreibung 180
17.7.3 Management von FTA_TSE.1 180
17.7.4 Audit von FTA_TSE.1 180
17.7.5 FTA_TSE.1 TOE-Sitzungsaufbau 181

18 Klasse FTP: Vertrauenswürdiger Pfad/vertrauenswürdige Kanäle 181
18.1 Klassenbeschreibung 181
18.2 Vertrauenswürdiger Kanal Inter-TSF (FTP_ITC) 182
18.2.1 Familienverhalten 182
18.2.2 Komponentenebenen und Beschreibung 182
18.2.3 Management von FTP_ITC.1 182
18.2.4 Audit von FTP_ITC.1 182
18.2.5 FTP_ITC.1 Vertrauenswürdiger Kanal Inter-TSF 183
18.3 Vertrauenswürdiges Kanalprotokoll (FTP_PRO) 183
18.3.1 Familienverhalten 183
18.3.2 Komponentenebenen und Beschreibung 183
18.3.3 Management von FTP_PRO.1 184
18.3.4 Management von FTP_PRO.2 184
18.3.5 Management von FTP_PRO.3 184
18.3.6 Audit von FTP_PRO.1 184
18.3.7 Audit von FTP_PRO.2 184
18.3.8 Audit von FTP_PRO.3 185
18.3.9 FTP_PRO.1 Protokoll des vertrauenswürdigen Kanals 185
18.3.10 FTP_PRO.2 Einrichtung des vertrauenswürdigen Kanals 186
18.3.11 FTP_PRO.3 Datenschutz für den vertrauenswürdigen Kanal 186
18.4 Vertrauenswürdiger Pfad (FTP_TRP) 187
18.4.1 Familienverhalten 187
18.4.2 Komponentenebenen und Beschreibung 187
18.4.3 Management von FTP_TRP.1 187
18.4.4 Audit von FTP_TRP.1 187
18.4.5 FTP_TRP.1 Vertrauenswürdiger Pfad 187

Anhang A (informativ) Struktur der Sicherheitsfunktionsanforderungen (SFR) in den Anwendungshinweisen 189
A.1 Allgemeines 189
A.2 Aufbau der Hinweise 189
A.2.1 Allgemeines 189
A.2.2 Klassenstruktur 189
A.2.3 Familienstruktur 190
A.2.4 Komponentenstruktur 191

Anhang B (informativ) Abhängigkeitstabellen für Sicherheitsfunktionskomponenten 192
B.1 Abhängigkeitstabellen 192

Anhang C (normativ) Klasse FAU: Sicherheitsaudit — Anwendungshinweise 202
C.1 Allgemeines 202
C.1.1 Allgemeine Informationen zu Auditanforderungen 202
C.1.2 Auditanforderungen in einer verteilten Umgebung 202
C.2 Automatische Antwort beim Sicherheitsaudit (FAU_ARP) 203
C.2.1 Anwendungshinweise für Benutzer 203
C.2.2 FAU_ARP.1 Sicherheitsalarme 203

C.3 Datengenerierung beim Sicherheitsaudit (FAU_GEN) 203
C.3.1 Allgemeines 203
C.3.2 FAU_GEN.1 Generierung von Auditdaten 205
C.3.3 FAU_GEN.2 Verknüpfung der Benutzeridentität 206
C.4 Sicherheitsauditanalyse (FAU_SAA) 206
C.4.1 Anwendungshinweise für Benutzer 206
C.4.2 „FAU_SAA.1 Potential violation analysis“ 207
C.4.3 FAU_SAA.2 Profilbasierte Erkennung von Anomalien 207
C.4.4 FAU_SAA.3 Einfache Angriffsheuristiken 208
C.4.5 FAU_SAA.4 Komplexe Angriffsheuristiken 209
C.5 Sicherheitsauditüberprüfung (FAU_SAR) 211
C.5.1 Anwendungshinweise für Benutzer 211
C.5.2 FAU_SAR.1 Auditüberprüfung 211
C.5.3 FAU_SAR.2 Beschränkte Auditüberprüfung 212
C.5.4 FAU_SAR.3 Auswählbare Auditüberprüfung 212
C.6 Sicherheitsaudit Ereignisauswahl (FAU_SEL) 212
C.6.1 Anwendungshinweise für Benutzer 212
C.6.2 FAU_SEL.1 Auswählbares Audit 213
C.7 Sicherheitsaudit Datenspeicherung (FAU_STG) 213
C.7.1 Anwendungshinweise für Benutzer 213
C.7.2 FAU_STG.1 Speicherort der Auditdaten 213
C.7.3 FAU_STG.2 Geschützte Speicherung der Auditdaten 214
C.7.4 FAU_STG.3 Garantien zur Auditdatenverfügbarkeit 214
C.7.5 FAU_STG.4 Verhinderung von Auditdatenverlust 215
C.7.6 FAU_STG.5 Aktionen bei möglichem Auditdatenverlust 215

Anhang D (normativ) Klasse FCO: Kommunikation — Anwendungshinweise 217
D.1 Allgemeines 217
D.2 Nichtabstreitbarkeit des Ursprungs (FCO_NRO) 217
D.2.1 Anwendungshinweise für Benutzer 217
D.2.2 FCO_NRO.1 Auswählbarer Ursprungsnachweis 218
D.2.3 FCO_NRO.2 Erzwungener Ursprungsnachweis 219
D.3 Nichtabstreitbarkeit des Empfangs (FCO_NRR) 219
D.3.1 Anwendungshinweise für Benutzer 219
D.3.2 FCO_NRR.1 Auswählbarer Empfangsnachweis 220
D.3.3 FCO_NRR.2 Erzwungener Empfangsnachweis 221

Anhang E (normativ) Klasse FCS: Kryptographische Unterstützung — Anwendungshinweise 223
E.1 Allgemeines 223
E.2 Verwaltung kryptographischer Schlüssel (FCS_CKM) 224
E.2.1 Anwendungshinweise für Benutzer 224
E.2.2 Hinweise für Evaluatoren 225
E.2.3 FCS_CKM.1 Generierung kryptographischer Schlüssel 226
E.2.4 FCS_CKM.2 Verteilung kryptographischer Schlüssel 226
E.2.5 FCS_CKM.3 Zugriff auf kryptographische Schlüssel 227
E.2.6 FCS_CKM.5 Ableitung kryptographischer Schlüssel 227
E.2.7 FCS_CKM.6 Zeitablauf und Ereignis der Zerstörung kryptographischer Schlüssel 227
E.3 Kryptographische Operation (FCS_COP) 228
E.3.1 Anwendungshinweise für Benutzer 228
E.3.2 FCS_COP.1 Kryptographische Operation 229
E.4 Generierung von Zufallsbits (FCS_RBG) 230
E.4.1 Anwendungshinweise für Benutzer 230
E.4.2 FCS_RBG.1 Generierung von Zufallsbits (RBG) 230
E.4.3 FCS_RBG.2 Generierung von Zufallsbits (externes Seeding) 231
E.4.4 FCS_RBG.3 Generierung von Zufallsbits (internal seeding — single source) 231
E.4.5 FCS_RBG.4 Generierung von Zufallsbits (internes Seeding — mehrere Quellen) 231
E.4.6 FCS_RBG.6 Dienst zur Generierung von Zufallsbits 232
E.5 Generierung von Zufallszahlen (FCS_RNG) 232
E.5.1 Anwendungshinweise für Benutzer 232

E.5.2 FCS_RNG.1 Generierung von Zufallszahlen 232

Anhang F (normativ) Klasse FDP: Schutz von Benutzerdaten — Anwendungshinweise 235
F.1 Allgemeines 235
F.2 Zugriffskontrollpolitik (FDP_ACC) 237
F.2.1 Anwendungshinweise für Benutzer 237
F.2.2 FDP_ACC.1 Zugriffskontrolle auf Teilmengen 238
F.2.3 FDP_ACC.2 Vollständige Zugriffskontrolle 238
F.3 Funktionen zur Zugriffskontrolle (FDP_ACF) 239
F.3.1 Anwendungshinweise für Benutzer 239
F.3.2 FDP_ACF.1 Zugriffskontrolle auf Grundlage von Sicherheitsattributen 240
F.4 Datenauthentifizierung (FDP_DAU) 241
F.4.1 Anwendungshinweise für Benutzer 241
F.4.2 FDP_DAU.1 Einfache Datenauthentifizierung 241
F.4.3 FDP_DAU.2 Datenauthentifizierung mit Identität des Garantiegebers 242
F.5 Export aus dem TOE (FDP_ETC) 242
F.5.1 Anwendungshinweise für Benutzer 242
F.5.2 FDP_ETC.1 Export von Benutzerdaten ohne Sicherheitsattribute 243
F.5.3 FDP_ETC.2 Export von Benutzerdaten mit Sicherheitsattributen 243
F.6 Informationsflusskontrollpolitik (FDP_IFC) 243
F.6.1 Anwendungshinweise für Benutzer 243
F.6.2 FDP_IFC.1 Informationsflusskontrolle auf Teilmengen 245
F.6.3 FDP_IFC.2 Vollständige Informationsflusskontrolle 245
F.7 Funktionen zur Informationsflusskontrolle (FDP_IFF) 246
F.7.1 Anwendungshinweise für Benutzer 246
F.7.2 FDP_IFF.1 Einfache Sicherheitsattribute 246
F.7.3 FDP_IFF.2 Hierarchische Sicherheitsattribute 247
F.7.4 FDP_IFF.3 Eingeschränkte unerlaubte Informationsflüsse 249
F.7.5 FDP_IFF.4 Teilweise Verhinderung von unerlaubten Informationsflüssen 249
F.7.6 FDP_IFF.5 Keine unerlaubten Informationsflüsse 250
F.7.7 FDP_IFF.6 Überwachung unerlaubter Informationsflüsse 250
F.8 Kontrolle der Informationsaufbewahrung (FDP_IRC) 251
F.8.1 Anwendungshinweise für Benutzer 251
F.8.2 FDP_IRC.1 Kontrolle der Informationsaufbewahrung 251
F.9 Import von außerhalb des TOEs (FDP_ITC) 252
F.9.1 Anwendungshinweise für Benutzer 252
F.9.2 FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute 253
F.9.3 FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen 253
F.10 Interne TOE-Übertragung (FDP_ITT) 254
F.10.1 Anwendungshinweise für Benutzer 254
F.10.2 FDP_ITT.1 Einfacher interner Übertragungsschutz 254
F.10.3 FDP_ITT.2 Trennung der Übertragung durch Attribut 254
F.10.4 FDP_ITT.3 Integritätsüberwachung 255
F.10.5 FDP_ITT.4 Attributbasierte Integritätsüberwachung 256
F.11 Restinformationsschutz (FDP_RIP) 257
F.11.1 Anwendungshinweise für Benutzer 257
F.11.2 FDP_RIP.1 Restinformationsschutz auf Teilmengen 258
F.11.3 FDP_RIP.2 Vollständiger Restinformationsschutz 258
F.12 Zurücksetzen (FDP_ROL) 258
F.12.1 Anwendungshinweise für Benutzer 258
F.12.2 FDP_ROL.1 Einfaches Zurücksetzen 259
F.12.3 FDP_ROL.2 Erweitertes Zurücksetzen 259
F.13 Vertraulichkeit gespeicherter Daten (FDP_SDC) 260
F.13.1 Anwendungshinweise für Benutzer 260
F.13.2 Hinweise für Evaluatoren 260
F.13.3 FDP_SDC.1 Vertraulichkeit gespeicherter Daten 260
F.13.4 FDP_SDC.2 Vertraulichkeit gespeicherter Daten mit zugehöriger Methode 261
F.14 Integrität gespeicherter Daten (FDP_SDI) 261

F.14.1 Anwendungshinweise für Benutzer 261
F.14.2 FDP_SDI.1 Überwachung der Integrität gespeicherter Daten 261
F.14.3 FDP_SDI.2 Überwachung der Integrität gespeicherter Daten und Aktionen 262
F.15 Inter-TSF-Schutz der Vertraulichkeit von Benutzerdaten bei Übertragung (FDP_UCT) 262
F.15.1 Anwendungshinweise für Benutzer 262
F.15.2 FDP_UCT.1 Vertraulichkeit bei einfachem Datenaustausch 262
F.16 Inter-TSF-Schutz der Benutzerdatenintegrität bei Übertragung (FDP_UIT) 263
F.16.1 Anwendungshinweise für Benutzer 263
F.16.2 FDP_UIT.1 Datenaustauschintegrität 263
F.16.3 FDP_UIT.2 Wiederherstellung bei Quelldatenaustausch 263
F.16.4 FDP_UIT.3 Wiederherstellung bei Zieldatenaustausch 264

Anhang G (normativ) Klasse FIA: Identifikation und Authentifizierung — Anwendungshinweise 265
G.1 Allgemeines 265
G.2 Authentifizierungsfehler (FIA_AFL) 265
G.2.1 Anwendungshinweise für Benutzer 265
G.2.2 FIA_AFL.1 Handhabung von Authentifizierungsfehlern 266
G.3 Authentifizierungsnachweis der Identität (FIA_API) 267
G.3.1 Anwendungshinweise für Benutzer 267
G.3.2 FIA_API.1 Authentifizierungsnachweis der Identität 267
G.4 Definition von Benutzerattributen (FIA_ATD) 268
G.4.1 Anwendungshinweise für Benutzer 268
G.4.2 FIA_ATD.1 Definition von Benutzerattributen 268
G.5 Spezifikation von Sicherheitsinformationen (FIA_SOS) 268
G.5.1 Anwendungshinweise für Benutzer 268
G.5.2 FIA_SOS.1 Verifizierung von Sicherheitsinformationen 269
G.5.3 FIA_SOS.2 Generierung von Sicherheitsinformationen durch die TSF 269
G.6 Benutzerauthentifizierung (FIA_UAU) 270
G.6.1 Anwendungshinweise für Benutzer 270
G.6.2 FIA_UAU.1 Zeitpunkt der Authentifizierung 270
G.6.3 FIA_UAU.2 Benutzerauthentifizierung vor irgendeiner anderen Aktion 270
G.6.4 FIA_UAU.3 Fälschungssichere Authentifizierung 271
G.6.5 FIA_UAU.4 Einmaliger Authentifizierungsmechanismus 271
G.6.6 FIA_UAU.5 Mehrfachauthentifizierungsmechanismen 271
G.6.7 FIA_UAU.6 Erneute Authentifizierung 272
G.6.8 FIA_UAU.7 Geschützte Authentifizierungsrückmeldung 273
G.7 Benutzeridentifizierung (FIA_UID) 273
G.7.1 Anwendungshinweise für Benutzer 273
G.7.2 FIA_UID.1 Zeitpunkt der Identifizierung 273
G.7.3 FIA_UID.2 Benutzeridentifizierung vor irgendeiner anderen Aktion 274
G.8 Benutzer-Subjekt-Bindung (FIA_USB) 274
G.8.1 Anwendungshinweise für Benutzer 274
G.8.2 FIA_USB.1 Benutzer-Subjekt-Bindung 274

Anhang H (normativ) Klasse FMT: Sicherheitsmanagement — Anwendungshinweise 275
H.1 Allgemeines 275
H.2 Eingeschränkte Fähigkeiten und Verfügbarkeit (FMT_LIM) 275
H.2.1 Anwendungshinweise für Benutzer 275
H.2.2 FMT_LIM.1 Eingeschränkte Fähigkeiten 276
H.2.3 FMT_LIM.2 Eingeschränkte Verfügbarkeit 276
H.3 Management von Funktionen in der TSF (FMT_MOF) 276
H.3.1 Anwendungshinweise für Benutzer 276
H.3.2 FMT_MOF.1 Management des Verhaltens der Sicherheitsfunktionen 277
H.4 Management von Sicherheitsattributen (FMT_MSA) 277
H.4.1 Anwendungshinweise für Benutzer 277
H.4.2 FMT_MSA.1 Management von Sicherheitsattributen 278
H.4.3 FMT_MSA.2 Sichere Sicherheitsattribute 278
H.4.4 FMT_MSA.3 Statische Attributinitialisierung 279
H.4.5 FMT_MSA.4 Vererbung von Sicherheitsattributwerten 279

H.5 Management von TSF-Daten (FMT_MTD) ... 280
H.5.1 Anwendungshinweise für Benutzer ... 280
H.5.2 FMT_MTD.1 Management von TSF-Daten ... 280
H.5.3 FMT_MTD.2 Management von Grenzen auf TSF-Daten ... 280
H.5.4 FMT_MTD.3 Sichere TSF-Daten ... 281
H.6 Widerruf (FMT_REV) ... 281
H.6.1 Anwendungshinweise für Benutzer ... 281
H.6.2 FMT_REV.1 Widerruf ... 281
H.7 Ablauf von Sicherheitsattributen (FMT_SAE) ... 282
H.7.1 Anwendungshinweise für Benutzer ... 282
H.7.2 FMT_SAE.1 Befristete Autorisierung ... 282
H.8 Spezifizierung von Managementfunktionen (FMT_SMF) ... 283
H.8.1 Anwendungshinweise für Benutzer ... 283
H.8.2 FMT_SMF.1 Spezifizierung von Managementfunktionen ... 283
H.9 Sicherheitsmanagementrollen (FMT_SMR) ... 283
H.9.1 Anwendungshinweise für Benutzer ... 283
H.9.2 FMT_SMR.1 Sicherheitsrollen ... 284
H.9.3 FMT_SMR.2 Einschränkungen zu Sicherheitsrollen ... 284
H.9.4 FMT_SMR.3 Übernahme von Rollen ... 284

Anhang I (normativ) Klasse FPR: Privatsphäre — Anwendungshinweise ... 285
I.1 Allgemeines ... 285
I.2 Anonymität (FPR_ANO) ... 286
I.2.1 Anwendungshinweise für Benutzer ... 286
I.2.2 FPR_ANO.1 Anonymität ... 287
I.2.3 FPR_ANO.2 Anonymität ohne Anforderung von Informationen ... 287
I.3 Pseudonymität (FPR_PSE) ... 288
I.3.1 Anwendungshinweise für Benutzer ... 288
I.3.2 FPR_PSE.1 Pseudonymität ... 289
I.3.3 FPR_PSE.2 Umkehrbare Pseudonymität ... 290
I.3.4 FPR_PSE.3 Alias-Pseudonymität ... 291
I.4 Unverknüpfbarkeit (FPR_UNL) ... 292
I.4.1 Anwendungshinweise für Benutzer ... 292
I.4.2 FPR_UNL.1 Unverknüpfbarkeit ... 293
I.5 Unbeobachtbarkeit (FPR_UNO) ... 294
I.5.1 Anwendungshinweise für Benutzer ... 294
I.5.2 FPR_UNO.1 Unbeobachtbarkeit ... 294
I.5.3 FPR_UNO.2 Zuweisung von Informationen mit Einfluss auf Unbeobachtbarkeit ... 295
I.5.4 FPR_UNO.3 Unbeobachtbarkeit ohne Anforderung von Informationen ... 296
I.5.5 FPR_UNO.4 Autorisierte Benutzerbeobachtbarkeit ... 297

Anhang J (normativ) Klasse FPT: Schutz der TSF — Anwendungshinweise ... 298
J.1 Allgemeines ... 298
J.2 FPT_EMS TOE-Emanation ... 299
J.2.1 Anwendungshinweise für Benutzer ... 299
J.2.2 FPT_EMS.1 TOE-Emanation ... 299
J.3 Sicherheit bei Ausfall (FPT_FLS) ... 299
J.3.1 Anwendungshinweise für Benutzer ... 299
J.3.2 FPT_FLS.1 Ausfall mit Beibehaltung des sicheren Zustands ... 300
J.4 TSF-Initialisierung (FPT_INI) ... 300
J.4.1 Anwendungshinweise für Benutzer ... 300
J.4.2 FPT_INI.1 TSF-Initialisierung ... 300
J.5 Verfügbarkeit von exportierten TSF-Daten (FPT_ITA) ... 301
J.5.1 Anwendungshinweise für Benutzer ... 301
J.5.2 FPT_ITA.1 Inter-TSF-Verfügbarkeit innerhalb einer definierten Verfügbarkeitsmetrik ... 301
J.6 Vertraulichkeit der exportierten TSF-Daten (FPT_ITC) ... 301
J.6.1 Anwendungshinweise für Benutzer ... 301
J.6.2 Hinweise für Evaluatoren ... 301
J.6.3 FPT_ITC.1 Inter-TSF-Vertraulichkeit während der Übertragung ... 302

J.7 Integrität exportierter TSF-Daten (FPT_ITI) 302
J.7.1 Anwendungshinweise für Benutzer 302
J.7.2 FPT_ITI.1 Inter-TSF-Erkennung von Änderungen 302
J.7.3 FPT_ITI.2 Inter-TSF-Erkennung und Korrektur von Änderungen 303
J.8 Interne TOE-TSF-Datenübertragung (FPT_ITT) 303
J.8.1 Anwendungshinweise für Benutzer 303
J.8.2 Hinweise für Evaluatoren 304
J.8.3 FPT_ITT.1 Einfacher Schutz der TSF-Daten bei interner Übertragung 304
J.8.4 FPT_ITT.2 Trennung des TSF-Datentransfers 304
J.8.5 FPT_ITT.3 Überwachung der Integrität von TSF-Daten 304
J.9 Physischer Schutz der TSF (FPT_PHP) 305
J.9.1 Anwendungshinweise für Benutzer 305
J.9.2 FPT_PHP.1 Passive Erkennung von physischen Angriffen 305
J.9.3 FPT_PHP.2 Mitteilung von physischen Angriffen 306
J.9.4 FPT_PHP.3 Widerstand gegen physische Angriffe 306
J.10 Vertrauenswürdige Wiederherstellung (FPT_RCV) 307
J.10.1 Anwendungshinweise für Benutzer 307
J.10.2 FPT_RCV.1 Manuelle Wiederherstellung 309
J.10.3 FPT_RCV.2 Automatische Wiederherstellung 309
J.10.4 FPT_RCV.3 Automatische Wiederherstellung ohne übermäßigen Verlust 309
J.10.5 FPT_RCV.4 Funktionswiederherstellung 310
J.11 Erkennung von Wiederverwendung (FPT_RPL) 310
J.11.1 Anwendungshinweise für Benutzer 310
J.11.2 FPT_RPL.1 Erkennung von Wiederverwendung 310
J.12 Zustandssynchronitätsprotokoll (FPT_SSP) 311
J.12.1 Anwendungshinweise für Benutzer 311
J.12.2 FPT_SSP.1 Einfache vertrauenswürdige Bestätigung 311
J.12.3 FPT_SSP.2 Gegenseitige vertrauenswürdige Bestätigung 312
J.13 Zeitstempel (FPT_STM) 312
J.13.1 Anwendungshinweise für Benutzer 312
J.13.2 FPT_STM.1 Verlässliche Zeitstempel 312
J.14 Inter-TSF-TSF-Datenkonsistenz (FPT_TDC) 312
J.14.1 Anwendungshinweise für Benutzer 312
J.14.2 FPT_TDC.1 Einfache Inter-TSF-TSF-Datenkonsistenz 313
J.15 Prüfen von externen Entitäten (FPT_TEE) 313
J.15.1 Anwendungshinweise für Benutzer 313
J.15.2 Hinweise für Evaluatoren 314
J.15.3 FPT_TEE.1 Prüfen von externen Entitäten 314
J.16 Interne TOE-TSF-Datenreplizierungskonsistenz (FPT_TRC) 315
J.16.1 Anwendungshinweise für Benutzer 315
J.16.2 FPT_TRC.1 Interne TSF-Konsistenz 315
J.17 TSF-Selbstprüfung (FPT_TST) 315
J.17.1 Anwendungshinweise für Benutzer 315
J.17.2 Hinweise für Evaluatoren 316
J.17.3 FPT_TST.1 TSF-Prüfung 316

Anhang K (normativ) Klasse FRU: Verwendung von Ressourcen — Anwendungshinweise 318
K.1 Allgemeines 318
K.2 Fehlertoleranz (FRU_FLT) 318
K.2.1 Anwendungshinweise für Benutzer 318
K.2.2 FRU_FLT.1 Verminderte Fehlertoleranz 318
K.2.3 FRU_FLT.2 Begrenzte Fehlertoleranz 319
K.3 Priorität von Diensten (FRU_PRS) 319
K.3.1 Anwendungshinweise für Benutzer 319
K.3.2 FRU_PRS.1 Begrenzte Priorität von Diensten 320
K.3.3 FRU_PRS.2 Vollständige Priorität von Diensten 320
K.4 Ressourcenzuweisung (FRU_RSA) 320
K.4.1 Anwendungshinweise für Benutzer 320

K.4.2 FRU_RSA.1 Höchstquoten ... 321
K.4.3 FRU_RSA.2 Mindestquoten und Höchstquoten ... 321

Anhang L (normativ) Klasse FTA: TOE-Zugriff — Anwendungshinweise ... 323
L.1 Allgemeines ... 323
L.2 Einschränkung des Umfangs auswählbarer Attribute (FTA_LSA) ... 323
L.2.1 Anwendungshinweise für Benutzer ... 323
L.2.2 FTA_LSA.1 Einschränkung des Umfangs auswählbarer Attribute ... 324
L.3 Einschränkung von mehreren gleichzeitigen Sitzungen (FTA_MCS) ... 324
L.3.1 Anwendungshinweise für Benutzer ... 324
L.3.2 FTA_MCS.1 Einfache Einschränkung von mehreren gleichzeitigen Sitzungen ... 324
L.3.3 FTA_MCS.2 Einschränkung von mehreren gleichzeitigen Sitzungen je Benutzerattribut ... 324
L.4 Sperren und Beenden von Sitzungen (FTA_SSL) ... 325
L.4.1 Anwendungshinweise für Benutzer ... 325
L.4.2 FTA_SSL.1 Durch die TSF ausgelöstes Sperren der Sitzung ... 325
L.4.3 FTA_SSL.2 Durch den Benutzer ausgelöstes Sperren ... 326
L.4.4 FTA_SSL.3 Durch die TSF ausgelöstes Beenden ... 326
L.4.5 FTA_SSL.4 Durch den Benutzer ausgelöstes Beenden ... 327
L.5 TOE-Zugriffsbanner (FTA_TAB) ... 327
L.5.1 Anwendungshinweise für Benutzer ... 327
L.5.2 FTA_TAB.1 Standard-TOE-Zugriffsbanner ... 327
L.6 TOE-Zugriffsverlauf (FTA_TAH) ... 327
L.6.1 Anwendungshinweise für Benutzer ... 327
L.6.2 FTA_TAH.1 TOE-Zugriffsverlauf ... 328
L.7 TOE-Sitzungsaufbau (FTA_TSE) ... 328
L.7.1 Anwendungshinweise für Benutzer ... 328
L.7.2 FTA_TSE.1 TOE-Sitzungsaufbau ... 329

Anhang M (normativ) Klasse FTP: Vertrauenswürdiger Pfad/vertrauenswürdige Kanäle — Anwendungshinweise ... 330
M.1 Allgemeines ... 330
M.2 Vertrauenswürdiger Kanal Inter-TSF (FTP_ITC) ... 330
M.2.1 Anwendungshinweise für Benutzer ... 330
M.2.2 FTP_ITC.1 Vertrauenswürdiger Kanal Inter-TSF ... 330
M.3 Vertrauenswürdiges Kanalprotokoll (FTP_PRO) ... 331
M.3.1 Anwendungshinweise für Benutzer ... 331
M.3.2 FTP_PRO.1 Protokoll des vertrauenswürdigen Kanals ... 331
M.3.3 FTP_PRO.2 Einrichtung des vertrauenswürdigen Kanals ... 332
M.3.4 FTP_PRO.3 Datenschutz für den vertrauenswürdigen Kanal ... 333
M.4 Vertrauenswürdiger Pfad (FTP_TRP) ... 333
M.4.1 Anwendungshinweise für Benutzer ... 333
M.4.2 FTP_TRP.1 Vertrauenswürdiger Pfad ... 333

Literaturhinweise ... 335

Bilder

Nationaler Anhang NA **Bild 1 — Beziehung zwischen Benutzerdaten und TSF-Daten ... 40**

Nationaler Anhang NB **Bild 2 — Beziehung zwischen „Authentisierungsdaten“ und „Sicherheitsinformationen“ ... 41**

Nationaler Anhang NC **Bild 3 — Struktur der Funktionsklassen ... 41**

Nationaler Anhang ND **Bild 4 — Struktur der Funktionsfamilien ... 42**

Nationaler Anhang NE **Bild 5 — Struktur der Funktionskomponenten ... 44**

Nationaler Anhang NF**Bild 6 — Muster eines Klassenaufbaudiagramms** ... 46
Nationaler Anhang NG**Bild 7 — FAU: Klassenaufbau Sicherheitsaudit** ... 47
Nationaler Anhang NH**Bild 8 — FAU_ARP: Komponentenebenen** ... 47
Nationaler Anhang NI**Bild 9 — FAU_GEN: Komponentenebenen** ... 48
Nationaler Anhang NJ**Bild 10 — FAU_SAA: Komponentenebenen** ... 50
Nationaler Anhang NK**Bild 11 — FAU_SAR: Komponentenebenen** ... 53
Nationaler Anhang NL**Bild 12 — FAU_SEL: Komponentenebenen** ... 55
Nationaler Anhang NM**Bild 13 — FAU_STG: Komponentenebenen** ... 56
Nationaler Anhang NN**Bild 14 — FCO: Klassenaufbau Kommunikation** ... 60
Nationaler Anhang NO**Bild 15 — FCO_NRO: Komponentenebenen** ... 60
Nationaler Anhang NP**Bild 16 — FCO_NRR: Komponentenebenen** ... 62
Nationaler Anhang NQ**Bild 17 — FCS: Klassenaufbau Kryptographische Unterstützung** ... 65
Nationaler Anhang NR**Bild 18 — FCS_CKM: Komponentenebenen** ... 66
Nationaler Anhang NS**Bild 19 — FCS_COP: Komponentenebenen** ... 69
Nationaler Anhang NT**Bild 20 — FCS_RBG: Komponentenebenen** ... 70
Nationaler Anhang NU**Bild 21 — FCS_RNG: Komponentenebenen** ... 74
Nationaler Anhang NV**Bild 22 — FDP: Klassenaufbau Schutz von Benutzerdaten** ... 77
Nationaler Anhang NW**Bild 23 — FDP_ACC: Komponentenebenen** ... 78
Nationaler Anhang NX**Bild 24 — FDP_ACF: Komponentenebenen** ... 79
Nationaler Anhang NY**Bild 25 — FDP_DAU: Komponentenebenen** ... 80
Nationaler Anhang NZ**Bild 26 — FDP_ETC: Komponentenebenen** ... 82
Nationaler Anhang NAA**Bild 27 — FDP_IFC: Komponentenebenen** ... 85
Nationaler Anhang NBB**Bild 28 — FDP_IFF: Komponentenebenen** ... 86
Nationaler Anhang NCC**Bild 29 — FDP_IRC: Komponentenebenen** ... 92
Nationaler Anhang NDD**Bild 30 — FDP_ITC: Komponentenebenen** ... 93
Nationaler Anhang NEE**Bild 31 — FDP_ITT: Komponentenebenen** ... 95
Nationaler Anhang NFF**Bild 32 — FDP_RIP: Komponentenebenen** ... 98
Nationaler Anhang NGG**Bild 33 — FDP_ROL: Komponentenebenen** ... 99
Nationaler Anhang NHH**Bild 34 — FDP_SDC: Komponentenebenen** ... 101

Nationaler Anhang NII**Bild 35 — FDP_SDI: Komponentenebenen** **102**

Nationaler Anhang NJJ**Bild 36 — FDP_UCT: Komponentenebenen** **104**

Nationaler Anhang NKK**Bild 37 — FDP_UIT: Komponentenebenen** **105**

Nationaler Anhang NLL**Bild 38 — FIA: Klassenaufbau Identifikation und Authentifizierung** **109**

Nationaler Anhang NMM**Bild 39 — FIA_AFL: Komponentenebenen** **109**

Nationaler Anhang NNN**Bild 40 — FIA_API: Komponentenebenen** **110**

Nationaler Anhang NOO**Bild 41 — FIA_ATD: Komponentenebenen** **111**

Nationaler Anhang NPP**Bild 42 — FIA_SOS: Komponentenebenen** **112**

Nationaler Anhang NQQ**Bild 43 — FIA_UAU: Komponentenebenen** **114**

Nationaler Anhang NRR**Bild 44 — FIA_UID: Komponentenebenen** **118**

Nationaler Anhang NSS**Bild 45 — FIA_USB: Komponentenebenen** **120**

Nationaler Anhang NTT**Bild 46 — FMT: Klassenaufbau Sicherheitsmanagement** **122**

Nationaler Anhang NUU**Bild 47 — FMT_LIM: Komponentenebenen** **122**

Nationaler Anhang NVV**Bild 48 — FMT_MOF: Komponentenebenen** **124**

Nationaler Anhang NWW**Bild 49 — FMT_MSA: Komponentenebenen** **125**

Nationaler Anhang NXX**Bild 50 — FMT_MTD: Komponentenebenen** **128**

Nationaler Anhang NYY**Bild 51 — FMT_REV: Komponentenebenen** **130**

Nationaler Anhang NZZ**Bild 52 — FMT_SAE: Komponentenebenen** **131**

Nationaler Anhang NAAA**Bild 53 — FMT_SMF: Komponentenebenen** **132**

Nationaler Anhang NBBB**Bild 54 — FMT_SMR: Komponentenebenen** **133**

Nationaler Anhang NCCC**Bild 55 — FPR: Klassenaufbau Privatsphäre** **136**

Nationaler Anhang NDDD**Bild 56 — FPR_ANO: Komponentenebenen** **136**

Nationaler Anhang NEEE**Bild 57 — FPR_PSE: Komponentenebenen** **137**

Nationaler Anhang NFFF**Bild 58 — FPR_UNL: Komponentenebenen** **140**

Nationaler Anhang NGGG**Bild 59 — FPR_UNO: Komponentenebenen** **141**

Nationaler Anhang NHHH**Bild 60 — FPT: Klassenaufbau Schutz der TSF** **144**

Nationaler Anhang NIII**Bild 61 — FPT_EMS: Komponentenebenen** **145**

Nationaler Anhang NJJJ**Bild 62 — FPT_FLS: Komponentenebenen** **146**

Nationaler Anhang NKKK**Bild 63 — FPT_INI: Komponentenebenen** **147**

Nationaler Anhang NLLL**Bild 64 — FPT_ITA: Komponentenebenen** **148**

Nationaler Anhang NMMM**Bild 65 — FPT_ITC: Komponentenebenen** **149**

Nationaler Anhang NNNN**Bild 66 — FPT_ITI: Komponentenebenen** **150**

Nationaler Anhang NOOO**Bild 67 — FPT_ITT: Komponentenebenen** **151**

Nationaler Anhang NPPP**Bild 68 — FPT_PHP: Komponentenebenen** **154**

Nationaler Anhang NQQQ**Bild 69 — FPT_RCV: Komponentenebenen** **156**

Nationaler Anhang NRRR**Bild 70 — FPT_RPL: Komponentenebenen** **159**

Nationaler Anhang NSSS**Bild 71 — FPT_SSP: Komponentenebenen** **160**

Nationaler Anhang NTTT**Bild 72 — FPR_STM: Komponentenebenen** **161**

Nationaler Anhang NUUU**Bild 73 — FPT_TDC: Komponentenebenen** **163**

Nationaler Anhang NVVV**Bild 74 — FPT_TEE: Komponentenebenen** **164**

Nationaler Anhang NWWW**Bild 75 — FPT_TRC: Komponentenebenen** **165**

Nationaler Anhang NXXX**Bild 76 — FPT_TST: Komponentenebenen** **166**

Nationaler Anhang NYYY**Bild 77 — FRU: Klassenaufbau Verwendung von Ressourcen** **168**

Nationaler Anhang NZZZ**Bild 78 — FRU_FLT: Komponentenebenen** **168**

Nationaler Anhang NAAAA**Bild 79 — FRU_PRS: Komponentenebenen** **169**

Nationaler Anhang NBBBB**Bild 80 — FRU_RSA: Komponentenebenen** **171**

Nationaler Anhang NCCCC**Bild 81 — FTA: Klassenaufbau TOE-Zugriff** **173**

Nationaler Anhang NDDDD**Bild 82 — FTA_LSA: Komponentenebenen** **173**

Nationaler Anhang NEEEE**Bild 83 — FTA_MCS: Komponentenebenen** **174**

Nationaler Anhang NFFFF**Bild 84 — FTA_SSL: Komponentenebenen** **175**

Nationaler Anhang NGGGG**Bild 85 — FTA_TAB: Komponentenebenen** **178**

Nationaler Anhang NHHHH**Bild 86 — FTA_TAH: Komponentenebenen** **179**

Nationaler Anhang NIIII**Bild 87 — FTA_TSE: Komponentenebenen** **180**

Nationaler Anhang NJJJJ**Bild 88 — FTP: Klassenaufbau Vertrauenswürdiger Pfad/vertrauenswürdige Kanäle** **182**

Nationaler Anhang NKKKK**Bild 89 — FTP_ITC: Komponentenebenen** **182**

Nationaler Anhang NLLLL**Bild 90 — FTP_PRO: Komponentenebenen** **183**

Nationaler Anhang NMMMM**Bild 91 — FTP_TRP: Komponentenebenen** **187**

Nationaler Anhang NNNNN**Bild A.1 — Struktur der Funktionsklassen** **189**

Nationaler Anhang NOOOO**Bild A.2 — Struktur der Funktionsfamilien für Anwendungshinweise** **190**

Nationaler Anhang NPPPP**Bild A.3 — Struktur der Funktionskomponenten** **191**

Tabellen

Nationaler Anhang NQQQQ**Tabelle 1 — FPT_EMS.1.1 Tabelle** **145**

Nationaler Anhang NRRRR**Tabelle 2 — FPT_INI.1.2 Tabelle** **147**

Nationaler Anhang NSSSS**Tabelle B.1 — Abhängigkeitstabelle für Klasse FAU: Sicherheitsaudit** **192**

Nationaler Anhang NTTTT**Tabelle B.2 — Abhängigkeitstabelle für Klasse FCO: Kommunikation** **193**

Nationaler Anhang NUUUU**Tabelle B.3 — Abhängigkeitstabelle für Klasse FCS: Kryptographische Unterstützung** **194**

Nationaler Anhang NVVVV**Tabelle B.4 — Abhängigkeitstabelle für Klasse FDP: Schutz von Benutzerdaten** **194**

Nationaler Anhang NWWWW**Tabelle B.5 — Abhängigkeitstabelle für Klasse FIA: Identifikation und Authentifizierung** **197**

Nationaler Anhang NXXXX**Tabelle B.6 — Abhängigkeitstabelle für Klasse FMT: Sicherheitsmanagement** **197**

Nationaler Anhang NYYYY**Tabelle B.7 — Abhängigkeitstabelle für Klasse FPR: Privatsphäre** **198**

Nationaler Anhang NZZZZ**Tabelle B.8 — Abhängigkeitstabelle für Klasse FPT: Schutz der TSF** **198**

Nationaler Anhang NAAAAA**Tabelle B.9 — Abhängigkeitstabelle für Klasse FRU: Verwendung von Ressourcen** **200**

Nationaler Anhang NBBBBB**Tabelle B.10 — Abhängigkeitstabelle für Klasse FTA: TOE-Zugriff** **200**

Nationaler Anhang NCCCCC**Tabelle B.11 — Abhängigkeitstabelle für Klasse FTP: Vertrauenswürdiger Pfad/vertrauenswürdige Kanäle** **201**