DIN EN ISO/IEC 15408-2:2020-12 (D)

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

Inhalt

Seite

Europäisches Vorwort 18

Vorwort 19

Einleitung 21

1 Anwendungsbereich 22

2 Normative Verweisungen 22

3 Begriffe, Symbole und Abkürzungen 22

4 Übersicht 22
4.1 Aufbau dieses Teils von ISO/IEC 15408 22

5 Paradigma für Funktionsanforderungen 23

6 Sicherheitsfunktionskomponenten 26
6.1 Übersicht 26
6.1.1 Klassenstruktur 27
6.1.2 Familienstruktur 27
6.1.3 Komponentenstruktur 29
6.2 Komponentenkatalog 30
6.2.1 Hervorheben von Komponentenänderungen 31

7 Klasse FAU: Sicherheitsaudit 31
7.1 Automatische Antwort beim Sicherheitsaudit (FAU_ARP) 32
7.1.1 Familienverhalten 32
7.1.2 Komponentenebenen 32
7.1.3 Management von FAU_ARP.1 32
7.1.4 Audit von FAU_ARP.1 32
7.1.5 FAU_ARP.1 Sicherheitsalarme 33
7.2 Datengenerierung beim Sicherheitsaudit (FAU_GEN) 33
7.2.1 Familienverhalten 33
7.2.2 Komponentenebenen 33
7.2.3 Management von FAU_GEN.1, FAU_GEN.2 33
7.2.4 Audit von FAU_GEN.1, FAU_GEN.2 33
7.2.5 FAU_GEN.1 Auditdatengenerierung 33
7.2.6 FAU_GEN.2 Verknüpfung der Benutzeridentität 34
7.3 Sicherheitsauditanalyse (FAU_SAA) 34
7.3.1 Familienverhalten 34
7.3.2 Komponentenebenen 34
7.3.3 Management von FAU_SAA.1 35
7.3.4 Management von FAU_SAA.2 35
7.3.5 Management von FAU_SAA.3 35
7.3.6 Management von FAU_SAA.4 35
7.3.7 Audit von FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4 35
7.3.8 FAU_SAA.1 Analyse potentieller Verstöße 35
7.3.9 FAU_SAA.2 Profilbasierte Erkennung von Anomalien 36
7.3.10 FAU_SAA.3 Einfache Angriffsheuristiken 36
7.3.11 FAU_SAA.4 Komplexe Angriffsheuristiken 37

7.4 Sicherheitsauditüberprüfung (FAU_SAR) 37
7.4.1 Familienverhalten 37
7.4.2 Komponentenebenen 37
7.4.3 Management von FAU_SAR.1 37
7.4.4 Management von FAU_SAR.2, FAU_SAR.3 38
7.4.5 Audit von FAU_SAR.1 38
7.4.6 Audit von FAU_SAR.2 38
7.4.7 Audit von FAU_SAR.3 38
7.4.8 FAU_SAR.1 Auditüberprüfung 38
7.4.9 FAU_SAR.2 Beschränkte Auditüberprüfung 38
7.4.10 FAU_SAR.3 Auswählbare Auditüberprüfung 39
7.5 Sicherheitsaudit Ereignisauswahl (FAU_SEL) 39
7.5.1 Familienverhalten 39
7.5.2 Komponentenebenen 39
7.5.3 Management von FAU_SEL.1 39
7.5.4 Audit von FAU_SEL.1 39
7.5.5 FAU_SEL.1 Auswählbares Audit 39
7.6 Sicherheitsaudit Ereignisspeicherung (FAU_STG) 40
7.6.1 Familienverhalten 40
7.6.2 Komponentenebenen 40
7.6.3 Management von FAU_STG.1 40
7.6.4 Management von FAU_STG.2 40
7.6.5 Management von FAU_STG.3 40
7.6.6 Management von FAU_STG.4 40
7.6.7 Audit von FAU_STG.1, FAU_STG.2 40
7.6.8 Audit von FAU_STG.3 41
7.6.9 Audit von FAU_STG.4 41
7.6.10 FAU_STG.1 Geschützte Speicherung des Audit-Trails 41
7.6.11 FAU_STG.2 Garantien zur Auditdatenverfügbarkeit 41
7.6.12 FAU_STG.3 Aktionen bei möglichem Auditdatenverlust 41
7.6.13 FAU_STG.4 Verhinderung von Auditdatenverlust 42

8 Klasse FCO: Kommunikation 42
8.1 Nichtabstreitbarkeit des Ursprungs (FCO_NRO) 42
8.1.1 Familienverhalten 42
8.1.2 Komponentenebenen 42
8.1.3 Management von FCO_NRO.1, FCO_NRO.2 43
8.1.4 Audit von FCO_NRO.1 43
8.1.5 Audit von FCO_NRO.2 43
8.1.6 FCO_NRO.1 Auswählbarer Ursprungsnachweis 43
8.1.7 FCO_NRO.2 Erzwungener Ursprungsnachweis 44
8.2 Nichtabstreitbarkeit des Empfangs (FCO_NRR) 44
8.2.1 Familienverhalten 44
8.2.2 Komponentenebenen 44
8.2.3 Management von FCO_NRR.1, FCO_NRR.2 44
8.2.4 Audit von FCO_NRR.1 44
8.2.5 Audit von FCO_NRR.2 45
8.2.6 FCO_NRR.1 Auswählbarer Empfangssnachweis 45
8.2.7 FCO_NRR.2 Erzwungener Empfangsnachweis 45

9 Klasse FCS: Kryptographische Unterstützung 46
9.1 Verwaltung kryptographischer Schlüssel (FCS_CKM) 46
9.1.1 Familienverhalten 46
9.1.2 Komponentenebenen 46
9.1.3 Management von FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 47
9.1.4 Audit von FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 47
9.1.5 FCS_CKM.1 Generierung kryptographischer Schlüssel 47
9.1.6 FCS_CKM.2 Verteilung kryptographischer Schlüssel 47
9.1.7 FCS_CKM.3 Zugriff auf kryptographische Schlüssel 48

9.1.8 FCS_CKM.4 Zerstörung kryptographischer Schlüssel 48
9.2 Kryptographische Operation (FCS_COP) 48
9.2.1 Familienverhalten 48
9.2.2 Komponentenebenen 49
9.2.3 Management von FCS_COP.1 49
9.2.4 Audit von FCS_COP.1 49
9.2.5 FCS_COP.1 Kryptographische Operation 49
10 Klasse FDP: Schutz von Benutzerdaten 49
10.1 Zugriffskontrollpolitik (FDP_ACC) 51
10.1.1 Familienverhalten 51
10.1.2 Komponentenebenen 52
10.1.3 Management von FDP_ACC.1, FDP_ACC.2 52
10.1.4 Audit von FDP_ACC.1, FDP_ACC.2 52
10.1.5 FDP_ACC.1 Zugriffskontrolle auf Teilmengen 52
10.1.6 FDP_ACC.2 Vollständige Zugriffskontrolle 52
10.2 Funktionen zur Zugriffskontrolle (FDP_ACF) 53
10.2.1 Familienverhalten 53
10.2.2 Komponentenebenen 53
10.2.3 Management von FDP_ACF.1 53
10.2.4 Audit von FDP_ACF.1 53
10.2.5 FDP_ACF.1 Zugriffskontrolle auf Grundlage von Sicherheitsattributen 53
10.3 Datenauthentifizierung (FDP_DAU) 54
10.3.1 Familienverhalten 54
10.3.2 Komponentenebenen 54
10.3.3 Management von FDP_DAU.1, FDP_DAU.2 54
10.3.4 Audit von FDP_DAU.1 54
10.3.5 Audit von FDP_DAU.2 55
10.3.6 FDP_DAU.1 Einfache Datenauthentifizierung 55
10.3.7 FDP_DAU.2 Datenauthentifizierung mit Identität des Garantiegebers 55
10.4 Export aus dem TOE (FDP_ETC) 55
10.4.1 Familienverhalten 55
10.4.2 Komponentenebenen 56
10.4.3 Management von FDP_ETC.1 56
10.4.4 Management von FDP_ETC.2 56
10.4.5 Audit von FDP_ETC.1, FDP_ETC.2 56
10.4.6 FDP_ETC.1 Export von Benutzerdaten ohne Sicherheitsattribute 56
10.4.7 FDP_ETC.2 Export von Benutzerdaten mit Sicherheitsattributen 56
10.5 Informationsflusskontrollpolitik (FDP_IFC) 57
10.5.1 Familienverhalten 57
10.5.2 Komponentenebenen 57
10.5.3 Management von FDP_IFC.1, FDP_IFC.2 58
10.5.4 Audit von FDP_IFC.1, FDP_IFC.2 58
10.5.5 FDP_IFC.1 Informationsflusskontrolle auf Teilmengen 58
10.5.6 FDP_IFC.2 Vollständige Informationsflusskontrolle 58
10.6 Funktionen zur Informationsflusskontrolle (FDP_IFF) 58
10.6.1 Familienverhalten 58
10.6.2 Komponentenebenen 59
10.6.3 Management von FDP_IFF.1, FDP_IFF.2 59
10.6.4 Management von FDP_IFF.3, FDP_IFF.4, FDP_IFF.5 59
10.6.5 Management von FDP_IFF.6 59
10.6.6 Audit von FDP_IFF.1, FDP_IFF.2, FDP_IFF.5 59
10.6.7 Audit von FDP_IFF.3, FDP_IFF.4, FDP_IFF.6 60
10.6.8 FDP_IFF.1 Einfache Sicherheitsattribute 60
10.6.9 FDP_IFF.2 Hierarchische Sicherheitsattribute 61
10.6.10 FDP_IFF.3 Eingeschränkte unerlaubte Informationsflüsse 62
10.6.11 FDP_IFF.4 Teilweise Verhinderung von unerlaubten Informationsflüssen 62
10.6.12 FDP_IFF.5 Keine unerlaubten Informationsflüsse 62

10.6.13 FDP_IFF.6 Überwachung unerlaubter Informationsflüsse 62
10.7 Import von außerhalb des TOEs (FDP_ITC) 63
10.7.1 Familienverhalten 63
10.7.2 Komponentenebenen 63
10.7.3 Management von FDP_ITC.1, FDP_ITC.2 63
10.7.4 Audit von FDP_ITC.1, FDP_ITC.2 63
10.7.5 FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute 63
10.7.6 FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen 64
10.8 Interne TOE-Übertragung (FDP_ITT) 64
10.8.1 Familienverhalten 64
10.8.2 Komponentenebenen 65
10.8.3 Management von FDP_ITT.1, FDP_ITT.2 65
10.8.4 Management von FDP_ITT.3, FDP_ITT.4 65
10.8.5 Audit von FDP_ITT.1, FDP_ITT.2 65
10.8.6 Audit von FDP_ITT.3, FDP_ITT.4 65
10.8.7 FDP_ITT.1 Einfacher interner Übertragungsschutz 66
10.8.8 FDP_ITT.2 Trennung der Übertragung durch Attribut 66
10.8.9 FDP_ITT.3 Integritätsüberwachung 66
10.8.10 FDP_ITT.4 Attributbasierte Integritätsüberwachung 67
10.9 Restinformationsschutz (FDP_RIP) 67
10.9.1 Familienverhalten 67
10.9.2 Komponentenebenen 67
10.9.3 Management von FDP_RIP.1, FDP_RIP.2 67
10.9.4 Audit von FDP_RIP.1, FDP_RIP.2 67
10.9.5 FDP_RIP.1 Restinformationsschutz auf Teilmengen 67
10.9.6 FDP_RIP.2 Vollständiger Restinformationsschutz 68
10.10 Zurücksetzen (FDP_ROL) 68
10.10.1 Familienverhalten 68
10.10.2 Komponentenebenen 68
10.10.3 Management von FDP_ROL.1, FDP_ROL.2 68
10.10.4 Audit von FDP_ROL.1, FDP_ROL.2 68
10.10.5 FDP_ROL.1 Einfaches Zurücksetzen 69
10.10.6 FDP_ROL.2 Erweitertes Zurücksetzen 69
10.11 Integrität gespeicherter Daten (FDP_SDI) 69
10.11.1 Familienverhalten 69
10.11.2 Komponentenebenen 69
10.11.3 Management von FDP_SDI.1 70
10.11.4 Management von FDP_SDI.2 70
10.11.5 Audit von FDP_SDI.1 70
10.11.6 Audit von FDP_SDI.2 70
10.11.7 FDP_SDI.1 Überwachung der Integrität gespeicherter Daten 70
10.11.8 FDP_SDI.2 Überwachung der Integrität gespeicherter Daten und Aktionen 70
10.12 Inter-TSF-Schutz der Vertraulichkeit von Benutzerdaten bei Übertragung (FDP_UCT) 71
10.12.1 Familienverhalten 71
10.12.2 Komponentenebenen 71
10.12.3 Management von FDP_UCT.1 71
10.12.4 Audit von FDP_UCT.1 71
10.12.5 FDP_UCT.1 Vertraulichkeit bei einfachem Datenaustausch 71
10.13 Inter-TSF-Schutz der Benutzerdatenintegrität bei Übertragung (FDP_UIT) 72
10.13.1 Familienverhalten 72
10.13.2 Komponentenebenen 72
10.13.3 Management von FDP_UIT.1, FDP_UIT.2, FDP_UIT.3 72
10.13.4 Audit von FDP_UIT.1 72
10.13.5 Audit von FDP_UIT.2, FDP_UIT.3 73
10.13.6 FDP_UIT.1 Datenaustauschintegrität 73
10.13.7 FDP_UIT.2 Wiederherstellung bei Quelldatenaustausch 73
10.13.8 FDP_UIT.3 Wiederherstellung bei Zieldatenaustausch 74

11 Klasse FIA: Identifikation und Authentifizierung 74
11.1 Authentifizierungsfehler (FIA_AFL) 75
11.1.1 Familienverhalten 75
11.1.2 Komponentenebenen 75
11.1.3 Management von FIA_AFL.1 76
11.1.4 Audit von FIA_AFL.1 76
11.1.5 FIA_AFL.1 Handhabung von Authentifizierungsfehlern 76
11.2 Definition von Benutzerattributen (FIA_ATD) 76
11.2.1 Familienverhalten 76
11.2.2 Komponentenebenen 76
11.2.3 Management von FIA_ATD.1 77
11.2.4 Audit von FIA_ATD.1 77
11.2.5 FIA_ATD.1 Definition von Benutzerattributen 77
11.3 Spezifikation von Sicherheitsinformationen (FIA_SOS) 77
11.3.1 Familienverhalten 77
11.3.2 Komponentenebenen 77
11.3.3 Management von FIA_SOS.1 77
11.3.4 Management von FIA_SOS.2 77
11.3.5 Audit von FIA_SOS.1, FIA_SOS.2 78
11.3.6 FIA_SOS.1 Verifizierung von Sicherheitsinformationen 78
11.3.7 FIA_SOS.2 Generierung von Sicherheitsinformationen durch die TSF 78
11.4 Benutzerauthentifizierung (FIA_UAU) 78
11.4.1 Familienverhalten 78
11.4.2 Komponentenebenen 78
11.4.3 Management von FIA_UAU.1 79
11.4.4 Management von FIA_UAU.2 79
11.4.5 Management von FIA_UAU.3, FIA_UAU.4, FIA_UAU.7 79
11.4.6 Management von FIA_UAU.5 79
11.4.7 Management von FIA_UAU.6 79
11.4.8 Audit von FIA_UAU.1 80
11.4.9 Audit von FIA_UAU.2 80
11.4.10 Audit von FIA_UAU.3 80
11.4.11 Audit von FIA_UAU.4 80
11.4.12 Audit von FIA_UAU.5 80
11.4.13 Audit von FIA_UAU.6 80
11.4.14 Audit von FIA_UAU.7 81
11.4.15 FIA_UAU.1 Zeitpunkt der Authentifizierung 81
11.4.16 FIA_UAU.2 Benutzerauthentifizierung vor irgendeiner anderen Aktion 81
11.4.17 FIA_UAU.3 Fälschungssichere Authentifizierung 81
11.4.18 FIA_UAU.4 Einmaliger Authentifizierungsmechanismus 81
11.4.19 FIA_UAU.5 Mehrfachauthentifizierungsmechanismen 82
11.4.20 FIA_UAU.6 Erneute Authentifizierung 82
11.4.21 FIA_UAU.7 Geschützte Authentifizierungsrückmeldung 82
11.5 Benutzeridentifizierung (FIA_UID) 82
11.5.1 Familienverhalten 82
11.5.2 Komponentenebenen 82
11.5.3 Management von FIA_UID.1 83
11.5.4 Management von FIA_UID.2 83
11.5.5 Audit von FIA_UID.1, FIA_UID.2 83
11.5.6 FIA_UID.1 Zeitpunkt der Identifizierung 83
11.5.7 FIA_UID.2 Benutzeridentifizierung vor irgendeiner anderen Aktion 83
11.6 Benutzer-Subjekt-Bindung (FIA_USB) 84
11.6.1 Familienverhalten 84
11.6.2 Komponentenebenen 84
11.6.3 Management von FIA_USB.1 84
11.6.4 Audit von FIA_USB.1 84
11.6.5 FIA_USB.1 Benutzer-Subjekt-Bindung 84

12 Klasse FMT: Sicherheitsmanagement 85
12.1 Management von Funktionen in der TSF (FMT_MOF) 86
12.1.1 Familienverhalten 86
12.1.2 Komponentenebenen 86
12.1.3 Management von FMT_MOF.1 86
12.1.4 Audit von FMT_MOF.1 86
12.1.5 FMT_MOF.1 Management des Verhaltens der Sicherheitsfunktionen 86
12.2 Management von Sicherheitsattributen (FMT_MSA) 86
12.2.1 Familienverhalten 86
12.2.2 Komponentenebenen 86
12.2.3 Management von FMT_MSA.1 87
12.2.4 Management von FMT_MSA.2 87
12.2.5 Management von FMT_MSA.3 87
12.2.6 Management von FMT_MSA.4 87
12.2.7 Audit von FMT_MSA.1 87
12.2.8 Audit von FMT_MSA.2 87
12.2.9 Audit von FMT_MSA.3 88
12.2.10 Audit von FMT_MSA.4 88
12.2.11 FMT_MSA.1 Management von Sicherheitsattributen 88
12.2.12 FMT_MSA.2 Sichere Sicherheitsattribute 88
12.2.13 FMT_MSA.3 Statische Attributinitialisierung 89
12.2.14 FMT_MSA.4 Vererbung von Sicherheitsattributwerten 89
12.3 Management von TSF-Daten (FMT_MTD) 89
12.3.1 Familienverhalten 89
12.3.2 Komponentenebenen 89
12.3.3 Management von FMT_MTD.1 90
12.3.4 Management von FMT_MTD.2 90
12.3.5 Management von FMT_MTD.3 90
12.3.6 Audit von FMT_MTD.1 90
12.3.7 Audit von FMT_MTD.2 90
12.3.8 Audit von FMT_MTD.3 90
12.3.9 FMT_MTD.1 Management von TSF-Daten 90
12.3.10 FMT_MTD.2 Management von Grenzen auf TSF-Daten 91
12.3.11 FMT_MTD.3 Sichere TSF-Daten 91
12.4 Widerruf (FMT_REV) 91
12.4.1 Familienverhalten 91
12.4.2 Komponentenebenen 91
12.4.3 Management von FMT_REV.1 91
12.4.4 Audit von FMT_REV.1 92
12.4.5 FMT_REV.1 Widerruf 92
12.5 Ablauf von Sicherheitsattributen (FMT_SAE) 92
12.5.1 Familienverhalten 92
12.5.2 Komponentenebenen 92
12.5.3 Management von FMT_SAE.1 92
12.5.4 Audit von FMT_SAE.1 92
12.5.5 FMT_SAE.1 Befristete Autorisierung 93
12.6 Spezifizierung von Managementfunktionen (FMT_SMF) 93
12.6.1 Familienverhalten 93
12.6.2 Komponentenebenen 93
12.6.3 Management von FMT_SMF.1 93
12.6.4 Audit von FMT_SMF.1 93
12.6.5 FMT_SMF.1 Spezifizierung von Managementfunktionen 93
12.7 Sicherheitsmanagementrollen (FMT_SMR) 94
12.7.1 Familienverhalten 94
12.7.2 Komponentenebenen 94
12.7.3 Management von FMT_SMR.1 94
12.7.4 Management von FMT_SMR.2 94
12.7.5 Management von FMT_SMR.3 94

12.7.6 Audit von FMT_SMR.1 94
12.7.7 Audit von FMT_SMR.2 95
12.7.8 Audit von FMT_SMR.3 95
12.7.9 FMT_SMR.1 Sicherheitsrollen 95
12.7.10 FMT_SMR.2 Einschränkungen zu Sicherheitsrollen 95
12.7.11 FMT_SMR.3 Übernahme von Rollen 95

13 Klasse FPR: Privatsphäre 96
13.1 Anonymität (FPR_ANO) 96
13.1.1 Familienverhalten 96
13.1.2 Komponentenebenen 96
13.1.3 Management von FPR_ANO.1, FPR_ANO.2 96
13.1.4 Audit von FPR_ANO.1, FPR_ANO.2 97
13.1.5 FPR_ANO.1 Anonymität 97
13.1.6 FPR_ANO.2 Anonymität ohne Anforderung von Informationen 97
13.2 Pseudonymität (FPR_PSE) 97
13.2.1 Familienverhalten 97
13.2.2 Komponentenebenen 97
13.2.3 Management von FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 98
13.2.4 Audit von FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 98
13.2.5 FPR_PSE.1 Pseudonymität 98
13.2.6 FPR_PSE.2 Umkehrbare Pseudonymität 98
13.2.7 FPR_PSE.3 Alias-Pseudonymität 99
13.3 Unverknüpfbarkeit (FPR_UNL) 99
13.3.1 Familienverhalten 99
13.3.2 Komponentenebenen 99
13.3.3 Management von FPR_UNL.1 99
13.3.4 Audit von FPR_UNL.1 100
13.3.5 FPR_UNL.1 Unverknüpfbarkeit 100
13.4 Unbeobachtbarkeit (FPR_UNO) 100
13.4.1 Familienverhalten 100
13.4.2 Komponentenebenen 100
13.4.3 Management von FPR_UNO.1, FPR_UNO.2 100
13.4.4 Management von FPR_UNO.3 100
13.4.5 Management von FPR_UNO.4 101
13.4.6 Audit von FPR_UNO.1, FPR_UNO.2 101
13.4.7 Audit von FPR_UNO.3 101
13.4.8 Audit von FPR_UNO.4 101
13.4.9 FPR_UNO.1 Unbeobachtbarkeit 101
13.4.10 FPR_UNO.2 Zuweisung von Informationen mit Einfluss auf Unbeobachtbarkeit 101
13.4.11 FPR_UNO.3 Unbeobachtbarkeit ohne Anforderung von Informationen 102
13.4.12 FPR_UNO.4 Autorisierte Benutzerbeobachtbarkeit 102

14 Klasse FPT: Schutz der TSF 102
14.1 Sicherheit bei Ausfall (FPT_FLS) 103
14.1.1 Familienverhalten 103
14.1.2 Komponentenebenen 103
14.1.3 Management von FPT_FLS.1 104
14.1.4 Audit von FPT_FLS.1 104
14.1.5 FPT_FLS.1 Ausfall mit Beibehaltung des sicheren Zustands 104
14.2 Verfügbarkeit von exportierten TSF-Daten (FPT_ITA) 104
14.2.1 Familienverhalten 104
14.2.2 Komponentenebenen 104
14.2.3 Management von FPT_ITA.1 104
14.2.4 Audit von FPT_ITA.1 104
14.2.5 FPT_ITA.1 Inter-TSF-Verfügbarkeit innerhalb einer definierten Verfügbarkeitsmetrik 105
14.3 Vertraulichkeit der exportierten TSF-Daten (FPT_ITC) 105
14.3.1 Familienverhalten 105
14.3.2 Komponentenebenen 105

14.3.3 Management von FPT_ITC.1 ... 105
14.3.4 Audit von FPT_ITC.1 ... 105
14.3.5 FPT_ITC.1 Inter-TSF-Vertraulichkeit während der Übertragung ... 105
14.4 Integrität exportierter TSF-Daten (FPT_ITI) ... 105
14.4.1 Familienverhalten ... 105
14.4.2 Komponentenebenen ... 106
14.4.3 Management von FPT_ITI.1 ... 106
14.4.4 Management von FPT_ITI.2 ... 106
14.4.5 Audit von FPT_ITI.1 ... 106
14.4.6 Audit von FPT_ITI.2 ... 106
14.4.7 FPT_ITI.1 Inter-TSF-Erkennung von Änderungen ... 106
14.4.8 FPT_ITI.2 Inter-TSF-Erkennung und Korrektur von Änderungen ... 107
14.5 Interne TOE-TSF-Datenübertragung (FPT_ITT) ... 107
14.5.1 Familienverhalten ... 107
14.5.2 Komponentenebenen ... 107
14.5.3 Management von FPT_ITT.1 ... 107
14.5.4 Management von FPT_ITT.2 ... 108
14.5.5 Management von FPT_ITT.3 ... 108
14.5.6 Audit von FPT_ITT.1, FPT_ITT.2 ... 108
14.5.7 Audit von FPT_ITT.3 ... 108
14.5.8 FPT_ITT.1 Einfacher Schutz der TSF-Daten bei interner Übertragung ... 108
14.5.9 FPT_ITT.2 Trennung des TSF-Datentransfers ... 108
14.5.10 FPT_ITT.3 Überwachung der Integrität von TSF-Daten ... 109
14.6 Physischer Schutz der TSF (FPT_PHP) ... 109
14.6.1 Familienverhalten ... 109
14.6.2 Komponentenebenen ... 109
14.6.3 Management von FPT_PHP.1 ... 110
14.6.4 Management von FPT_PHP.2 ... 110
14.6.5 Management von FPT_PHP.3 ... 110
14.6.6 Audit von FPT_PHP.1 ... 110
14.6.7 Audit von FPT_PHP.2 ... 110
14.6.8 Audit von FPT_PHP.3 ... 110
14.6.9 FPT_PHP.1 Passive Erkennung von physischen Angriffen ... 110
14.6.10 FPT_PHP.2 Mitteilung von physischen Angriffen ... 111
14.6.11 FPT_PHP.3 Widerstand gegen physische Angriffe ... 111
14.7 Vertrauenswürdige Wiederherstellung (FPT_RCV) ... 111
14.7.1 Familienverhalten ... 111
14.7.2 Komponentenebenen ... 111
14.7.3 Management von FPT_RCV.1 ... 112
14.7.4 Management von FPT_RCV.2, FPT_RCV.3 ... 112
14.7.5 Management von FPT_RCV.4 ... 112
14.7.6 Audit von FPT_RCV.1, FPT_RCV.2, FPT_RCV.3 ... 112
14.7.7 Audit von FPT_RCV.4 ... 112
14.7.8 FPT_RCV.1 Manuelle Wiederherstellung ... 112
14.7.9 FPT_RCV.2 Automatische Wiederherstellung ... 113
14.7.10 FPT_RCV.3 Automatische Wiederherstellung ohne übermäßigen Verlust ... 113
14.7.11 FPT_RCV.4 Funktionswiederherstellung ... 113
14.8 Erkennung von Wiederverwendung (FPT_RPL) ... 114
14.8.1 Familienverhalten ... 114
14.8.2 Komponentenebenen ... 114
14.8.3 Management von FPT_RPL.1 ... 114
14.8.4 Audit von FPT_RPL.1 ... 114
14.8.5 FPT_RPL.1 Erkennung von Wiederverwendung ... 114
14.9 Zustandssynchronitätsprotokoll (FPT_SSP) ... 115
14.9.1 Familienverhalten ... 115
14.9.2 Komponentenebenen ... 115
14.9.3 Management von FPT_SSP.1, FPT_SSP.2 ... 115
14.9.4 Audit von FPT_SSP.1, FPT_SSP.2 ... 115

14.9.5 FPT_SSP.1 Einfache vertrauenswürdige Bestätigung ... 115
14.9.6 FPT_SSP.2 Gegenseitige vertrauenswürdige Bestätigung ... 115
14.10 Zeitstempel (FPT_STM) ... 116
14.10.1 Familienverhalten ... 116
14.10.2 Komponentenebenen ... 116
14.10.3 Management von FPT_STM.1 ... 116
14.10.4 Audit von FPT_STM.1 ... 116
14.10.5 FPT_STM.1 Verlässliche Zeitstempel ... 116
14.11 Inter-TSF-TSF-Datenkonsistenz (FPT_TDC) ... 116
14.11.1 Familienverhalten ... 116
14.11.2 Komponentenebenen ... 116
14.11.3 Management von FPT_TDC.1 ... 117
14.11.4 Audit von FPT_TDC.1 ... 117
14.11.5 FPT_TDC.1 Einfache Inter-TSF-TSF-Datenkonsistenz ... 117
14.12 Prüfen von externen Entitäten (FPT_TEE) ... 117
14.12.1 Familienverhalten ... 117
14.12.2 Komponentenebenen ... 117
14.12.3 Management von FPT_TEE.1 ... 117
14.12.4 Audit von FPT_TEE.1 ... 118
14.12.5 FPT_TEE.1 Prüfen von externen Entitäten ... 118
14.13 Interne TOE-TSF-Datenreplizierungskonsistenz (FPT_TRC) ... 118
14.13.1 Familienverhalten ... 118
14.13.2 Komponentenebenen ... 118
14.13.3 Management von FPT_TRC.1 ... 118
14.13.4 Audit von FPT_TRC.1 ... 118
14.13.5 FPT_TRC.1 Interne TSF-Konsistenz ... 118
14.14 TSF-Selbstprüfung (FPT_TST) ... 119
14.14.1 Familienverhalten ... 119
14.14.2 Komponentenebenen ... 119
14.14.3 Management von FPT_TST.1 ... 119
14.14.4 Audit von FPT_TST.1 ... 119
14.14.5 FPT_TST.1 TSF-Prüfung ... 120

15 Klasse FRU: Verwendung von Ressourcen ... 120
15.1 Fehlertoleranz (FRU_FLT) ... 120
15.1.1 Familienverhalten ... 120
15.1.2 Komponentenebenen ... 121
15.1.3 Management von FRU_FLT.1, FRU_FLT.2 ... 121
15.1.4 Audit von FRU_FLT.1 ... 121
15.1.5 Audit von FRU_FLT.2 ... 121
15.1.6 FRU_FLT.1 Verminderte Fehlertoleranz ... 121
15.1.7 FRU_FLT.2 Begrenzte Fehlertoleranz ... 121
15.2 Priorität von Diensten (FRU_PRS) ... 121
15.2.1 Familienverhalten ... 121
15.2.2 Komponentenebenen ... 122
15.2.3 Management von FRU_PRS.1, FRU_PRS.2 ... 122
15.2.4 Audit von FRU_PRS.1, FRU_PRS.2 ... 122
15.2.5 FRU_PRS.1 Begrenzte Priorität von Diensten ... 122
15.2.6 FRU_PRS.2 Vollständige Priorität von Diensten ... 122
15.3 Ressourcenzuweisung (FRU_RSA) ... 123
15.3.1 Familienverhalten ... 123
15.3.2 Komponentenebenen ... 123
15.3.3 Management von FRU_RSA.1 ... 123
15.3.4 Management von FRU_RSA.2 ... 123
15.3.5 Audit von FRU_RSA.1, FRU_RSA.2 ... 123
15.3.6 FRU_RSA.1 Höchstquoten ... 123
15.3.7 FRU_RSA.2 Mindestquoten und Höchstquoten ... 124

16 Klasse FTA: TOE-Zugriff ... 124

16.1 Einschränkung des Umfangs auswählbarer Attribute (FTA_LSA) ... 125
16.1.1 Familienverhalten ... 125
16.1.2 Komponentenebenen ... 125
16.1.3 Management von FTA_LSA.1 ... 125
16.1.4 Audit von FTA_LSA.1 ... 125
16.1.5 FTA_LSA.1 Einschränkung des Umfangs auswählbarer Attribute ... 125
16.2 Einschränkung von mehreren gleichzeitigen Sitzungen (FTA_MCS) ... 125
16.2.1 Familienverhalten ... 125
16.2.2 Komponentenebenen ... 125
16.2.3 Management von FTA_MCS.1 ... 126
16.2.4 Management von FTA_MCS.2 ... 126
16.2.5 Audit von FTA_MCS.1, FTA_MCS.2 ... 126
16.2.6 FTA_MCS.1 Einfache Einschränkung von mehreren gleichzeitigen Sitzungen ... 126
16.2.7 FTA_MCS.2 Einschränkung von mehreren gleichzeitigen Sitzungen je Benutzerattribut ... 126
16.3 Sperren und Beenden von Sitzungen (FTA_SSL) ... 127
16.3.1 Familienverhalten ... 127
16.3.2 Komponentenebenen ... 127
16.3.3 Management von FTA_SSL.1 ... 127
16.3.4 Management von FTA_SSL.2 ... 127
16.3.5 Management von FTA_SSL.3 ... 127
16.3.6 Management von FTA_SSL.4 ... 127
16.3.7 Audit von FTA_SSL.1, FTA_SSL.2 ... 128
16.3.8 Audit von FTA_SSL.3 ... 128
16.3.9 Audit von FTA_SSL.4 ... 128
16.3.10 FTA_SSL.1 Durch die TSF ausgelöstes Sperren der Sitzung ... 128
16.3.11 FTA_SSL.2 Durch den Benutzer ausgelöstes Sperren ... 128
16.3.12 FTA_SSL.3 Durch die TSF ausgelöstes Beenden ... 129
16.3.13 FTA_SSL.4 Durch den Benutzer ausgelöstes Beenden ... 129
16.4 TOE-Zugriffsbanner (FTA_TAB) ... 129
16.4.1 Familienverhalten ... 129
16.4.2 Komponentenebenen ... 129
16.4.3 Management von FTA_TAB.1 ... 129
16.4.4 Audit von FTA_TAB.1 ... 130
16.4.5 FTA_TAB.1 Standard-TOE-Zugriffsbanner ... 130
16.5 TOE-Zugriffsverlauf (FTA_TAH) ... 130
16.5.1 Familienverhalten ... 130
16.5.2 Komponentenebenen ... 130
16.5.3 Management von FTA_TAH.1 ... 130
16.5.4 Audit von FTA_TAH.1 ... 130
16.5.5 FTA_TAH.1 TOE-Zugriffsverlauf ... 130
16.6 TOE-Sitzungsaufbau (FTA_TSE) ... 131
16.6.1 Familienverhalten ... 131
16.6.2 Komponentenebenen ... 131
16.6.3 Management von FTA_TSE.1 ... 131
16.6.4 Audit von FTA_TSE.1 ... 131
16.6.5 FTA_TSE.1 TOE-Sitzungsaufbau ... 131

17 Klasse FTP: Vertrauenswürdiger Pfad/vertrauenswürdige Kanäle ... 131
17.1 Vertrauenswürdiger Kanal Inter-TSF (FTP_ITC) ... 132
17.1.1 Familienverhalten ... 132
17.1.2 Komponentenebenen ... 132
17.1.3 Management von FTP_ITC.1 ... 132
17.1.4 Audit von FTP_ITC.1 ... 133
17.1.5 FTP_ITC.1 Vertrauenswürdiger Kanal Inter-TSF ... 133
17.2 Vertrauenswürdiger Pfad (FTP_TRP) ... 133
17.2.1 Familienverhalten ... 133
17.2.2 Komponentenebenen ... 133
17.2.3 Management von FTP_TRP.1 ... 134

17.2.4 Audit von FTP_TRP.1 134
17.2.5 FTP_TRP.1 Vertrauenswürdiger Pfad 134

Anhang A (normativ) Anwendungshinweise zu Sicherheitsfunktionsanforderungen 135
A.1 Aufbau der Hinweise 135
A.1.1 Klassenstruktur 135
A.1.2 Familienstruktur 136
A.1.3 Komponentenstruktur 136
A.2 Abhängigkeitstabellen 137

Anhang B (normativ) Funktionsklassen, Funktionsfamilien und Funktionskomponenten 144

Anhang C (normativ) Klasse FAU: Sicherheitsaudit 145
C.1 Auditanforderungen in einer verteilten Umgebung 145
C.2 Automatische Antwort beim Sicherheitsaudit (FAU_ARP) 146
C.2.1 Hinweise für Benutzer 146
C.2.2 FAU_ARP.1 Sicherheitsalarme 146
C.3 Datengenerierung beim Sicherheitsaudit (FAU_GEN) 147
C.3.1 Hinweise für Benutzer 147
C.3.2 FAU_GEN.1 Generierung von Auditdaten 148
C.3.3 FAU_GEN.2 Verknüpfung der Benutzeridentität 149
C.4 Sicherheitsauditanalyse (FAU_SAA) 149
C.4.1 Hinweise für Benutzer 149
C.4.2 FAU_SAA.1 Analyse potentieller Verstöße 150
C.4.3 FAU_SAA.2 Profilbasierte Erkennung von Anomalien 150
C.4.4 FAU_SAA.3 Einfache Angriffsheuristiken 151
C.4.5 FAU_SAA.4 Komplexe Angriffsheuristiken 152
C.5 Sicherheitsauditüberprüfung (FAU_SAR) 153
C.5.1 Hinweise für Benutzer 153
C.5.2 FAU_SAR.1 Auditüberprüfung 154
C.5.3 FAU_SAR.2 Beschränkte Auditüberprüfung 154
C.5.4 FAU_SAR.3 Auswählbare Auditüberprüfung 155
C.6 Sicherheitsaudit Ereignisauswahl (FAU_SEL) 155
C.6.1 Hinweise für Benutzer 155
C.6.2 FAU_SEL.1 Auswählbares Audit 155
C.7 Sicherheitsaudit Ereignisspeicherung (FAU_STG) 156
C.7.1 Hinweise für Benutzer 156
C.7.2 FAU_STG.1 Geschützte Speicherung des Audit-Trails 156
C.7.3 FAU_STG.2 Garantien zur Auditdatenverfügbarkeit 156
C.7.4 FAU_STG.3 Aktionen bei möglichem Auditdatenverlust 157
C.7.5 FAU_STG.4 Verhinderung von Auditdatenverlust 157

Anhang D (normativ) Klasse FCO: Kommunikation 159
D.1 Nichtabstreitbarkeit des Ursprungs (FCO_NRO) 159
D.1.1 Hinweise für Benutzer 159
D.1.2 FCO_NRO.1 Auswählbarer Ursprungsnachweis 160
D.1.3 FCO_NRO.2 Erzwungener Ursprungsnachweis 161
D.2 Nichtabstreitbarkeit des Empfangs (FCO_NRR) 161
D.2.1 Hinweise für Benutzer 161
D.2.2 FCO_NRR.1 Auswählbarer Empfangsnachweis 162
D.2.3 FCO_NRR.2 Erzwungener Empfangsnachweis 163

Anhang E (normativ) Klasse FCS: Kryptographische Unterstützung 164
E.1 Verwaltung kryptographischer Schlüssel (FCS_CKM) 165
E.1.1 Hinweise für Benutzer 165
E.1.2 FCS_CKM.1 Generierung kryptographischer Schlüssel 166
E.1.3 FCS_CKM.2 Verteilung kryptographischer Schlüssel 166
E.1.4 FCS_CKM.3 Zugriff auf kryptographische Schlüssel 167
E.1.5 FCS_CKM.4 Zerstörung kryptographischer Schlüssel 167
E.2 Kryptographische Operation (FCS_COP) 167

E.2.1 Hinweise für Benutzer ... 167
E.2.2 FCS_COP.1 Kryptographische Operation ... 168

Anhang F (normativ) Klasse FDP: Schutz von Benutzerdaten ... 169
F.1 Zugriffskontrollpolitik (FDP_ACC) ... 172
F.1.1 Hinweise für Benutzer ... 172
F.1.2 FDP_ACC.1 Zugriffskontrolle auf Teilmengen ... 173
F.1.3 FDP_ACC.2 Vollständige Zugriffskontrolle ... 174
F.2 Funktionen zur Zugriffskontrolle (FDP_ACF) ... 174
F.2.1 Hinweise für Benutzer ... 174
F.2.2 FDP_ACF.1 Zugriffskontrolle auf Grundlage von Sicherheitsattributen ... 175
F.3 Datenauthentifizierung (FDP_DAU) ... 176
F.3.1 Hinweise für Benutzer ... 176
F.3.2 FDP_DAU.1 Einfache Datenauthentifizierung ... 176
F.3.3 FDP_DAU.2 Datenauthentifizierung mit Identität des Garantiegebers ... 177
F.4 Export aus dem TOE (FDP_ETC) ... 177
F.4.1 Hinweise für Benutzer ... 177
F.4.2 FDP_ETC.1 Export von Benutzerdaten ohne Sicherheitsattribute ... 178
F.4.3 FDP_ETC.2 Export von Benutzerdaten mit Sicherheitsattributen ... 178
F.5 Informationsflusskontrollpolitik (FDP_IFC) ... 178
F.5.1 Hinweise für Benutzer ... 178
F.5.2 FDP_IFC.1 Informationsflusskontrolle auf Teilmengen ... 180
F.5.3 FDP_IFC.2 Vollständige Informationsflusskontrolle ... 180
F.6 Funktionen zur Informationsflusskontrolle (FDP_IFF) ... 181
F.6.1 Hinweise für Benutzer ... 181
F.6.2 FDP_IFF.1 Einfache Sicherheitsattribute ... 181
F.6.3 FDP_IFF.2 Hierarchische Sicherheitsattribute ... 182
F.6.4 FDP_IFF.3 Eingeschränkte unerlaubte Informationsflüsse ... 184
F.6.5 FDP_IFF.4 Teilweise Verhinderung von unerlaubten Informationsflüssen ... 184
F.6.6 FDP_IFF.5 Keine unerlaubten Informationsflüsse ... 185
F.6.7 FDP_IFF.6 Überwachung unerlaubter Informationsflüsse ... 185
F.7 Import von außerhalb des TOEs (FDP_ITC) ... 185
F.7.1 Hinweise für Benutzer ... 185
F.7.2 FDP_ITC.1 Import von Benutzerdaten ohne Sicherheitsattribute ... 187
F.7.3 FDP_ITC.2 Import von Benutzerdaten mit Sicherheitsattributen ... 187
F.8 Interne TOE-Übertragung (FDP_ITT) ... 187
F.8.1 Hinweise für Benutzer ... 187
F.8.2 FDP_ITT.1 Einfacher interner Übertragungsschutz ... 188
F.8.3 FDP_ITT.2 Trennung der Übertragung durch Attribut ... 188
F.8.4 FDP_ITT.3 Integritätsüberwachung ... 189
F.8.5 FDP_ITT.4 Attributbasierte Integritätsüberwachung ... 189
F.9 Restinformationsschutz (FDP_RIP) ... 190
F.9.1 Hinweise für Benutzer ... 190
F.9.2 FDP_RIP.1 Restinformationsschutz auf Teilmengen ... 191
F.9.3 FDP_RIP.2 Vollständiger Restinformationsschutz ... 192
F.10 Zurücksetzen (FDP_ROL) ... 192
F.10.1 Hinweise für Benutzer ... 192
F.10.2 FDP_ROL.1 Einfaches Zurücksetzen ... 192
F.10.3 FDP_ROL.2 Erweitertes Zurücksetzen ... 193
F.11 Integrität gespeicherter Daten (FDP_SDI) ... 193
F.11.1 Hinweise für Benutzer ... 193
F.11.2 FDP_SDI.1 Überwachung der Integrität gespeicherter Daten ... 194
F.11.3 FDP_SDI.2 Überwachung der Integrität gespeicherter Daten und Aktionen ... 194
F.12 Inter-TSF-Schutz der Vertraulichkeit von Benutzerdaten bei Übertragung (FDP_UCT) ... 194
F.12.1 Hinweise für Benutzer ... 194
F.12.2 FDP_UCT.1 Vertraulichkeit bei einfachem Datenaustausch ... 195
F.13 Inter-TSF-Schutz der Benutzerdatenintegrität bei Übertragung (FDP_UIT) ... 195
F.13.1 Hinweise für Benutzer ... 195

F.13.2 FDP_UIT.1 Datenaustauschintegrität ... 195
F.13.3 FDP_UIT.2 Wiederherstellung bei Quelldatenaustausch ... 196
F.13.4 FDP_UIT.3 Wiederherstellung bei Zieldatenaustausch ... 196

Anhang G (normativ) Klasse FIA: Identifikation und Authentifizierung ... 198
G.1 Authentifizierungsfehler (FIA_AFL) ... 199
G.1.1 Hinweise für Benutzer ... 199
G.1.2 FIA_AFL.1 Handhabung von Authentifizierungsfehlern ... 200
G.2 Definition von Benutzerattributen (FIA_ATD) ... 201
G.2.1 Hinweise für Benutzer ... 201
G.2.2 FIA_ATD.1 Definition von Benutzerattributen ... 201
G.3 Spezifikation von Sicherheitsinformationen (FIA_SOS) ... 201
G.3.1 Hinweise für Benutzer ... 201
G.3.2 FIA_SOS.1 Verifizierung von Sicherheitsinformationen ... 202
G.3.3 FIA_SOS.2 Generierung von Sicherheitsinformationen durch die TSF ... 202
G.4 Benutzerauthentifizierung (FIA_UAU) ... 203
G.4.1 Hinweise für Benutzer ... 203
G.4.2 FIA_UAU.1 Zeitpunkt der Authentifizierung ... 203
G.4.3 FIA_UAU.2 Benutzerauthentifizierung vor irgendeiner anderen Aktion ... 203
G.4.4 FIA_UAU.3 Fälschungssichere Authentifizierung ... 203
G.4.5 FIA_UAU.4 Einmaliger Authentifizierungsmechanismus ... 204
G.4.6 FIA_UAU.5 Mehrfachauthentifizierungsmechanismen ... 204
G.4.7 FIA_UAU.6 Erneute Authentifizierung ... 205
G.4.8 FIA_UAU.7 Geschützte Authentifizierungsrückmeldung ... 205
G.5 Benutzeridentifizierung (FIA_UID) ... 206
G.5.1 Hinweise für Benutzer ... 206
G.5.2 FIA_UID.1 Zeitpunkt der Identifizierung ... 206
G.5.3 FIA_UID.2 Benutzeridentifizierung vor irgendeiner anderen Aktion ... 206
G.6 Benutzer-Subjekt-Bindung (FIA_USB) ... 207
G.6.1 Hinweise für Benutzer ... 207
G.6.2 FIA_USB.1 Benutzer-Subjekt-Bindung ... 207

Anhang H (normativ) Klasse FMT: Sicherheitsmanagement ... 208
H.1 Management von Funktionen in der TSF (FMT_MOF) ... 209
H.1.1 Hinweise für Benutzer ... 209
H.1.2 FMT_MOF.1 Management des Verhaltens der Sicherheitsfunktionen ... 210
H.2 Management von Sicherheitsattributen (FMT_MSA) ... 210
H.2.1 Hinweise für Benutzer ... 210
H.2.2 FMT_MSA.1 Management von Sicherheitsattributen ... 211
H.2.3 FMT_MSA.2 Sichere Sicherheitsattribute ... 211
H.2.4 FMT_MSA.3 Statische Attributinitialisierung ... 212
H.2.5 FMT_MSA.4 Vererbung von Sicherheitsattributwerten ... 212
H.3 Management von TSF-Daten (FMT_MTD) ... 213
H.3.1 Hinweise für Benutzer ... 213
H.3.2 FMT_MTD.1 Management von TSF-Daten ... 213
H.3.3 FMT_MTD.2 Management von Grenzen auf TSF-Daten ... 213
H.3.4 FMT_MTD.3 Sichere TSF-Daten ... 214
H.4 Widerruf (FMT_REV) ... 214
H.4.1 Hinweise für Benutzer ... 214
H.4.2 FMT_REV.1 Widerruf ... 214
H.5 Ablauf von Sicherheitsattributen (FMT_SAE) ... 215
H.5.1 Hinweise für Benutzer ... 215
H.5.2 FMT_SAE.1 Befristete Autorisierung ... 215
H.6 Spezifizierung von Managementfunktionen (FMT_SMF) ... 216
H.6.1 Hinweise für Benutzer ... 216
H.6.2 FMT_SMF.1 Spezifizierung von Managementfunktionen ... 216
H.7 Sicherheitsmanagementrollen (FMT_SMR) ... 216
H.7.1 Hinweise für Benutzer ... 216
H.7.2 FMT_SMR.1 Sicherheitsrollen ... 217

H.7.3 FMT_SMR.2 Einschränkungen zu Sicherheitsrollen ... 217
H.7.4 FMT_SMR.3 Übernahme von Rollen ... 217

Anhang I (normativ) Klasse FPR: Privatsphäre ... 218
I.1 Anonymität (FPR_ANO) ... 219
I.1.1 Hinweise für Benutzer ... 219
I.1.2 FPR_ANO.1 Anonymität ... 220
I.1.3 FPR_ANO.2 Anonymität ohne Anforderung von Informationen ... 220
I.2 Pseudonymität (FPR_PSE) ... 221
I.2.1 Hinweise für Benutzer ... 221
I.2.2 FPR_PSE.1 Pseudonymität ... 222
I.2.3 FPR_PSE.2 Umkehrbare Pseudonymität ... 223
I.2.4 FPR_PSE.3 Alias-Pseudonymität ... 224
I.3 Unverknüpfbarkeit (FPR_UNL) ... 225
I.3.1 Hinweise für Benutzer ... 225
I.3.2 FPR_UNL.1 Unverknüpfbarkeit ... 225
I.4 Unbeobachtbarkeit (FPR_UNO) ... 226
I.4.1 Hinweise für Benutzer ... 226
I.4.2 FPR_UNO.1 Unbeobachtbarkeit ... 227
I.4.3 FPR_UNO.2 Zuweisung von Informationen mit Einfluss auf Unbeobachtbarkeit ... 227
I.4.4 FPR_UNO.3 Unbeobachtbarkeit ohne Anforderung von Informationen ... 228
I.4.5 FPR_UNO.4 Autorisierte Benutzerbeobachtbarkeit ... 229

Anhang J (normativ) Klasse FPT: Schutz der TSF ... 230
J.1 Sicherheit bei Ausfall (FPT_FLS) ... 232
J.1.1 Hinweise für Benutzer ... 232
J.1.2 FPT_FLS.1 Ausfall mit Beibehaltung des sicheren Zustands ... 232
J.2 Verfügbarkeit von exportierten TSF-Daten (FPT_ITA) ... 232
J.2.1 Hinweise für Benutzer ... 232
J.2.2 FPT_ITA.1 Inter-TSF-Verfügbarkeit innerhalb einer definierten Verfügbarkeitsmetrik ... 232
J.3 Vertraulichkeit der exportierten TSF-Daten (FPT_ITC) ... 233
J.3.1 Hinweise für Benutzer ... 233
J.3.2 FPT_ITC.1 Inter-TSF-Vertraulichkeit während der Übertragung ... 233
J.4 Integrität exportierter TSF-Daten (FPT_ITI) ... 233
J.4.1 Hinweise für Benutzer ... 233
J.4.2 FPT_ITI.1 Inter-TSF-Erkennung von Änderungen ... 233
J.4.3 FPT_ITI.2 Inter-TSF-Erkennung und Korrektur von Änderungen ... 234
J.5 Interne TOE-TSF-Datenübertragung (FPT_ITT) ... 235
J.5.1 Hinweise für Benutzer ... 235
J.5.2 Hinweise für Evaluatoren ... 235
J.5.3 FPT_ITT.1 Einfacher Schutz der TSF-Daten bei interner Übertragung ... 235
J.5.4 FPT_ITT.2 Trennung des TSF-Datentransfers ... 235
J.5.5 FPT_ITT.3 Überwachung der Integrität von TSF-Daten ... 235
J.6 Physischer Schutz der TSF (FPT_PHP) ... 236
J.6.1 Hinweise für Benutzer ... 236
J.6.2 FPT_PHP.1 Passive Erkennung von physischen Angriffen ... 236
J.6.3 FPT_PHP.2 Mitteilung von physischen Angriffen ... 237
J.6.4 FPT_PHP.3 Widerstand gegen physische Angriffe ... 237
J.7 Vertrauenswürdige Wiederherstellung (FPT_RCV) ... 238
J.7.1 Hinweise für Benutzer ... 238
J.7.2 FPT_RCV.1 Manuelle Wiederherstellung ... 239
J.7.3 FPT_RCV.2 Automatische Wiederherstellung ... 240
J.7.4 FPT_RCV.3 Automatische Wiederherstellung ohne übermäßigen Verlust ... 240
J.7.5 FPT_RCV.4 Funktionswiederherstellung ... 241
J.8 Erkennung von Wiederverwendung (FPT_RPL) ... 241
J.8.1 Hinweise für Benutzer ... 241
J.8.2 FPT_RPL.1 Erkennung von Wiederverwendung ... 241
J.9 Zustandssynchronitätsprotokoll (FPT_SSP) ... 242
J.9.1 Hinweise für Benutzer ... 242

J.9.2 FPT_SSP.1 Einfache vertrauenswürdige Bestätigung ... 242
J.9.3 FPT_SSP.2 Gegenseitige vertrauenswürdige Bestätigung ... 242
J.10 Zeitstempel (FPT_STM) ... 243
J.10.1 Hinweise für Benutzer ... 243
J.10.2 FPT_STM.1 Verlässliche Zeitstempel ... 243
J.11 Inter-TSF-TSF-Datenkonsistenz (FPT_TDC) ... 243
J.11.1 Hinweise für Benutzer ... 243
J.11.2 FPT_TDC.1 Einfache Inter-TSF-TSF-Datenkonsistenz ... 243
J.12 Prüfen von externen Entitäten (FPT_TEE) ... 244
J.12.1 Hinweise für Benutzer ... 244
J.12.2 Hinweise für Evaluatoren ... 244
J.12.3 FPT_TEE.1 Prüfen von externen Entitäten ... 244
J.13 Interne TOE-TSF-Datenreplizierungskonsistenz (FPT_TRC) ... 245
J.13.1 Hinweise für Benutzer ... 245
J.13.2 FPT_TRC.1 Interne TSF-Konsistenz ... 246
J.14 TSF-Selbstprüfung (FPT_TST) ... 246
J.14.1 Hinweise für Benutzer ... 246
J.14.2 FPT_TST.1 TSF-Prüfung ... 246

Anhang K (normativ) Klasse FRU: Verwendung von Ressourcen ... 248
K.1 Fehlertoleranz (FRU_FLT) ... 248
K.1.1 Hinweise für Benutzer ... 248
K.1.2 FRU_FLT.1 Verminderte Fehlertoleranz ... 249
K.1.3 FRU_FLT.2 Begrenzte Fehlertoleranz ... 249
K.2 Priorität von Diensten (FRU_PRS) ... 249
K.2.1 Hinweise für Benutzer ... 249
K.2.2 FRU_PRS.1 Begrenzte Priorität von Diensten ... 250
K.2.3 FRU_PRS.2 Vollständige Priorität von Diensten ... 250
K.3 Ressourcenzuweisung (FRU_RSA) ... 250
K.3.1 Hinweise für Benutzer ... 250
K.3.2 FRU_RSA.1 Höchstquoten ... 251
K.3.3 FRU_RSA.2 Mindestquoten und Höchstquoten ... 251

Anhang L (normativ) Klasse FTA: TOE-Zugriff ... 253
L.1 Einschränkung des Umfangs auswählbarer Attribute (FTA_LSA) ... 253
L.1.1 Hinweise für Benutzer ... 253
L.1.2 FTA_LSA.1 Einschränkung des Umfangs auswählbarer Attribute ... 254
L.2 Einschränkung von mehreren gleichzeitigen Sitzungen (FTA_MCS) ... 254
L.2.1 Hinweise für Benutzer ... 254
L.2.2 FTA_MCS.1 Einfache Einschränkung von mehreren gleichzeitigen Sitzungen ... 254
L.2.3 FTA_MCS.2 Einschränkung von mehreren gleichzeitigen Sitzungen je Benutzerattribut ... 255
L.3 Sperren und Beenden von Sitzungen (FTA_SSL) ... 255
L.3.1 Hinweise für Benutzer ... 255
L.3.2 FTA_SSL.1 Durch die TSF ausgelöstes Sperren der Sitzung ... 255
L.3.3 FTA_SSL.2 Durch den Benutzer ausgelöstes Sperren ... 256
L.3.4 FTA_SSL.3 Durch die TSF ausgelöstes Beenden ... 256
L.3.5 FTA_SSL.4 Durch den Benutzer ausgelöstes Beenden ... 257
L.4 TOE-Zugriffsbanner (FTA_TAB) ... 257
L.4.1 Hinweise für Benutzer ... 257
L.4.2 FTA_TAB.1 Standard-TOE-Zugriffsbanner ... 257
L.5 TOE-Zugriffsverlauf (FTA_TAH) ... 257
L.5.1 Hinweise für Benutzer ... 257
L.5.2 FTA_TAH.1 TOE-Zugriffsverlauf ... 257
L.6 TOE-Sitzungsaufbau (FTA_TSE) ... 258
L.6.1 Hinweise für Benutzer ... 258
L.6.2 FTA_TSE.1 TOE-Sitzungsaufbau ... 259

Anhang M (normativ) Klasse FTP: Vertrauenswürdiger Pfad/vertrauenswürdige Kanäle ... 260
M.1 Vertrauenswürdiger Kanal Inter-TSF (FTP_ITC) ... 260

M.1.1 Hinweise für Benutzer 260
M.1.2 FTP_ITC.1 Vertrauenswürdiger Kanal Inter-TSF 260
M.2 Vertrauenswürdiger Pfad (FTP_TRP) 261
M.2.1 Hinweise für Benutzer 261
M.2.2 FTP_TRP.1 Vertrauenswürdiger Pfad 261