DIN EN ISO/IEC 15408-2

ICS 35.030

Ersatz für
die 2011-03 zurückgezogene
Norm
DIN ISO/IEC 15408-2:2007-11

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

Information technology –
Security techniques –
Evaluation criteria for IT security –
Part 2: Security functional components (ISO/IEC 15408-2:2008);
German version EN ISO/IEC 15408-2:2020, only on CD-ROM

Technologies de l'information –
Techniques de sécurité –
Critères d'évaluation pour la sécurité TI –
Partie 2: Composants fonctionnels de sécurité (ISO/IEC 15408-2:2008);
Version allemande EN ISO/IEC 15408-2:2020, seulement en CD-ROM

Gesamtumfang 263 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

Nationales Vorwort

Der Text von ISO/IEC 15408-2:2008 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 15408-2:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Gremium ist der Arbeitskreis NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

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

Änderungen

Gegenüber der 2011-03 zurückgezogenen Norm DIN ISO/IEC 15408-2:2007-11 wurden folgende Änderungen vorgenommen:

a) redaktionelle Überarbeitung, insbesondere bezogen auf FDP_UTC, FDP_UIT, FDP_ACF.1.4, FAU_SEL.1.1, FPT_TST.1, FDP_ITT.4 und FPT_TEE;

b) Aktualisierung des technischen Inhalts.

Frühere Ausgaben

DIN ISO/IEC 15408-2: 2001-03, 2007-11

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 15408-2

März 2020

ICS 35.030

Deutsche Fassung

Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 2: Sicherheitsfunktionskomponenten (ISO/IEC 15408-2:2008)

Information technology —
Security techniques —
Evaluation criteria for IT security —
Part 2: Security functional components
(ISO/IEC 15408-2:2008)

Technologies de l'information —
Techniques de sécurité —
Critères d'évaluation pour la sécurité TI —
Partie 2: Composants fonctionnels de sécurité
(ISO/IEC 15408-2:2008)

Diese Europäische Norm wurde vom CEN am 2. März 2020 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

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**

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

Europäisches Vorwort

Der Text von ISO/IEC 15408-2:2008 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 15408-2:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis September 2020, und etwaige entgegenstehende nationale Normen müssen bis September 2020 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 15408-2:2008 wurde von CEN als EN ISO/IEC 15408-2:2020 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet.

Die Hauptaufgabe der gemeinsamen Technischen Komitees besteht in dem Erarbeiten von Internationalen Normen. Die von den Technischen Komitees angenommenen Norm-Entwürfe werden den Mitgliedsorganisationen zur Umfrage zur Verfügung gestellt. Für eine Veröffentlichung als Internationale Norm wird eine Zustimmung von mindestens 75 % der Mitgliedsländer, die abgestimmt haben, benötigt.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

ISO/IEC 15408-2 wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques*, erarbeitet. Der identische Text von ISO/IEC 15408 ist bei den am Common Criteria Project beteiligten Organisationen als Common Criteria for Information Technology Security Evaluation (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik) veröffentlicht. Die einheitliche XML-Quelle für beide Veröffentlichungen ist unter http://www.oc.ccn.cni.es/xml zu finden.

Diese dritte Fassung ersetzt die zweite Fassung (ISO/IEC 15408-2:2005), die technisch überarbeitet wurde.

ISO/IEC 15408 besteht unter dem allgemeinen Titel *Information technology — Security techniques — Evaluation criteria for IT security* aus den folgenden Teilen:

— *Part 1: Introduction and general model*

— *Part 2: Security functional components*

— *Part 3: Security assurance components*

Diese korrigierte Version von ISO/IEC 15408-2:2008 enthält verschiedene redaktionelle Korrekturen, die sich im Wesentlichen auf FDP_UTC, FDP_UIT, FDP_ACF.1.4, FAU_SEL.1.1, FPT_TST.1, FDP_ITT.4 und FPT_TEE beziehen.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

Rechtlicher Hinweis

Die unten aufgeführten Regierungsorganisationen haben zu der Entwicklung dieser Version der Common Criteria for Information Technology Security Evaluations beigetragen. Als gemeinsame Urheberrechtsinhaber an den Common Criteria for Information Technology Security Evaluations, Version 3.1 Teile 1 bis 3 (kurz CC 3.1), erteilen sie hiermit der ISO/IEC die nicht-exklusive Lizenz zur Verwendung der CC 3.1 für die weitere Entwicklung/Pflege der internationalen Norm ISO/IEC 15408. Diese Regierungsorganisationen behalten sich allerdings das Recht zur Nutzung, Vervielfältigung, zum Vertrieb sowie zur Übersetzung und Änderung der CC 3.1 nach Belieben vor.

Australien/Neuseeland:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Kanada:	Communications Security Establishment;
Frankreich:	Direction Centrale de la Sécurité des Systèmes d'Information;
Deutschland:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;
Niederlande:	Netherlands National Communications Security Agency;
Spanien:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
Vereinigtes Königreich:	Communications-Electronic Security Group;
USA:	The National Security Agency and the National Institute of Standards and Technology.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

Einleitung

Die in diesem Teil von ISO/IEC 15408 definierten Sicherheitsfunktionskomponenten sind die Grundlage für in Schutzprofilen (PPs) oder Sicherheitsvorgaben (ST) ausgedrückte Sicherheitsfunktionsanforderungen. Diese Anforderungen beschreiben das von einem Evaluierungsgegenstand (TOE) erwartete, gewünschte Sicherheitsverhalten und sind dafür ausgelegt, die in einem PP oder einer ST angegebenen Sicherheitszielsetzungen zu erfüllen. Diese Anforderungen beschreiben Sicherheitseigenschaften, die Benutzer durch direkte Interaktion (d. h. Eingaben, Ausgaben) mit der IT oder durch die IT-Antwort ermitteln können.

Sicherheitsfunktionskomponenten formulieren Sicherheitsanforderungen zur Abwehr von Bedrohungen in der angenommenen Betriebsumgebung des TOEs und/oder decken alle identifizierten organisatorischen Sicherheitspolitiken und Annahmen ab.

Zur Zielgruppe für diesen Teil von ISO/IEC 15408 gehören Verbraucher, Entwickler und Evaluatoren von sicheren IT-Produkten. ISO/IEC 15408-1:2009, Abschnitt 5 enthält zusätzliche Informationen zur Zielgruppe von ISO/IEC 15408 und zur Verwendung von ISO/IEC 15408 durch entsprechende Gruppen. Diese Gruppen können diesen Teil der ISO/IEC 15408 wie folgt verwenden:

a) Verbraucher, die diesen Teil von ISO/IEC 15408 beim Auswählen von Komponenten in der Formulierung von Funktionsanforderungen zur Erfüllung von in einem PP oder einer ST formulierten Sicherheitszielsetzung verwenden. ISO/IEC 15408-1:2009, Abschnitt 6 enthält weitere detaillierte Informationen zur Beziehung zwischen Sicherheitszielsetzungen und Sicherheitsanforderungen;

b) Entwickler, die mit der Erstellung eines TOEs auf tatsächliche oder angenommene Sicherheitsanforderungen von Verbrauchern reagieren, können in diesem Teil von ISO/IEC 15408 eine genormte Methode zum Verständnis dieser Anforderungen finden. Sie können auch den Inhalt dieses Teils der ISO/IEC 15408 als Grundlage für die weitere Definition der Sicherheitsfunktionalität und von Sicherheitsmechanismen des TOEs zur Einhaltung dieser Anforderungen verwenden;

c) Evaluatoren, die die in diesem Teil von ISO/IEC 15408 definierten Funktionsanforderungen dazu nutzen, zu verifizieren, dass die im PP oder in der ST definierten Funktionsanforderungen des TOEs die IT-Sicherheitszielsetzungen erfüllen und die alle Abhängigkeiten erfassen und als erfüllt nachweisen. Evaluatoren sollten diesen Teil von ISO/IEC 15408 unterstützend auch dazu verwenden, um festzustellen, ob ein TOE die angegebenen Anforderungen erfüllt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

1 Anwendungsbereich

Dieser Teil von ISO/IEC 15408 definiert die Anforderungen an Struktur und Inhalt der Sicherheitsfunktionskomponenten für die Sicherheitsevaluierung. Er enthält einen Katalog an Funktionskomponenten, der die häufigsten Sicherheitsfunktionsanforderungen vieler IT-Produkte abdeckt.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

3 Begriffe, Symbole und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Begriffe, Symbole und Abkürzungen nach ISO/IEC 15408-1.

4 Übersicht

ISO/IEC 15408 und die in ihr beschriebenen Sicherheitsfunktionsanforderungen sind nicht dazu bestimmt, eine endgültige Antwort auf alle Probleme der IT-Sicherheit zu geben. Vielmehr bietet ISO/IEC 15408 eine Reihe wohlverstandener Sicherheitsfunktionsanforderungen, die zur Erstellung vertrauenswürdiger Produkte mit Blick auf die Markterfordernisse verwendet werden können. Diese Sicherheitsfunktionsanforderungen werden als derzeitiger Stand der Technik bei Anforderungsspezifikation und Evaluierung dargestellt.

Dieser Teil von ISO/IEC 15408 versucht nicht, alle erdenklichen Sicherheitsfunktionsanforderungen einzuschließen, sondern enthält die zum Zeitpunkt der Veröffentlichung von den Autoren dieses Teils der ISO/IEC 15408 bekannten und als sinnvoll erachteten Anforderungen.

Da sich das Verständnis und die Bedürfnisse von Verbrauchern ändern können, müssen die Funktionsanforderungen dieses Teils von ISO/IEC 15408 gepflegt werden. Es wird davon ausgegangen, dass einige PP-/ST-Autoren Sicherheitsbedürfnisse haben können, die (noch) nicht von den Funktionsanforderungskomponenten dieses Teils von ISO/IEC 15408 abgedeckt sind. In solchen Fällen darf ein PP-/ST-Autor sich dazu entscheiden, eine nicht in ISO/IEC 15408 enthaltene Funktionsanforderung auszuwählen (bezeichnet als Erweiterbarkeit), wie in Anhang A und Anhang B von ISO/IEC 15408-1:2009 erläutert.

4.1 Aufbau dieses Teils von ISO/IEC 15408

Abschnitt 5 beschreibt das in den Sicherheitsfunktionsanforderungen dieses Teils von ISO/IEC 15408 verwendete Paradigma.

Abschnitt 6 stellt den Katalog der Funktionskomponenten dieses Teils von ISO/IEC 15408 vor während Abschnitt 7 bis Abschnitt 17die Funktionsklassen beschreiben.

Anhang A liefert Erklärungen für potentielle Benutzer der Funktionskomponenten, einschließlich einer vollständigen Tabelle mit Querverweisungen zu den Abhängigkeiten der Funktionskomponenten.

Anhang B bis Anhang M liefern Erklärungen zu den Funktionsklassen. Dieses Materials muss als normative Anweisungen zur Anwendung relevanter Operationen und Auswahl entsprechender Informationen zu Audit und Dokumentation betrachtet werden; die Verwendung des Hilfsverbs 'sollte' bedeutet, dass die Anweisung

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

eindeutig bevorzugt wird, aber auch andere Anweisungen gerechtfertigt sein können. Bei verschiedenen Optionen kann der PP-/ST-Autor frei wählen.

Autoren von PPs oder STs sollten für die entsprechenden Strukturen, Regeln und Leitlinien den Abschnitt 2 der ISO/IEC 15408-1:2009 zu Rate ziehen.

a) ISO/IEC 15408-1:2009, Abschnitt 3 definiert die in ISO/IEC 15408 verwendeten Begriffe.

b) ISO/IEC 15408-1:2009, Anhang A definiert die Struktur für STs.

c) ISO/IEC 15408-1:2009, Anhang B definiert die Struktur für PPs.

5 Paradigma für Funktionsanforderungen

Dieser Abschnitt beschreibt das in den Sicherheitsfunktionsanforderungen dieses Teils von ISO/IEC 15408 verwendete Paradigma. Behandelte Schlüsselbegriffe werden fett/kursiv hervorgehoben. Dieser Unterabschnitt ist nicht dazu bestimmt, irgendwelche Begriffe aus Abschnitt 3 von ISO/IEC 15408-1:2009 zu ersetzen oder abzulösen.

Dieser Teil von ISO/IEC 15408 ist ein Katalog an Sicherheitsfunktionskomponenten, die für einen **Evaluierungsgegenstand (TOE)** spezifiziert werden können. Ein TOE umfasst Software, Firmware und/oder Hardware, möglicherweise mit beigefügter Leitliniendokumentation für Benutzer und Administratoren. Ein TOE kann Ressourcen wie elektronische Speichermedien (z. B. Hauptspeicher, Plattenspeicher), Peripheriegeräte (z. B. Drucker) und Rechenkapazität (z. B. Prozessorzeit) enthalten; diese Ressourcen können zur Verarbeitung und Speicherung von Informationen verwendet werden und bilden das Subjekt der Evaluierung.

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

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

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

Der TOE kann ein monolithisches Produkt sein, das Hardware, Firmware und Software enthält.

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

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

a) Die SFRs des anderen „vertrauenswürdigen IT-Produkts“ und die SFRs des TOEs wurden verwaltungstechnisch abgestimmt und von dem anderen vertrauenswürdigen IT-Produkt wird angenommen, dass es seine SFRs korrekt durchsetzt (z. B. durch gesonderte Evaluierung). Informationsaustausche in dieser Situation werden **Inter-TSF-Übertragungen** genannt, da sie zwischen den TSFs einzelner vertrauenswürdiger Produkte stattfindet.

b) Das andere IT-Produkt ist möglicherweise nicht vertrauenswürdig und kann als „nicht vertrauenswürdiges IT-Produkt“ bezeichnet werden. Seine SFRs sind daher entweder unbekannt oder deren Implementation wird als nicht vertrauenswürdig erachtet. In dieser Situation werden durch die TSF-vermittelte Informationsaustausche als **Übertragungen außerhalb des TOEs** bezeichnet, da es keine TSFs (oder deren politischen Merkmale sind unbekannt) für das andere IT-Produkt gibt.

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

Benutzer befinden sich außerhalb des TOEs. Allerdings interagieren Benutzer mit dem TOE über die TSFIs, um die Ausführung von Diensten durch den TOE anzufragen, die den in den SFRs definierten Regeln entsprechen. Es gibt zwei Arten von Benutzern, die für diesen Teil von ISO/IEC 15408 von Interesse sind: **Menschliche Benutzer** und **externe IT-Entitäten**. Menschliche Benutzer können noch weiter unterschieden werden in **lokale menschliche Benutzer**, also Benutzer, die direkt mit dem TOE über TOE-Geräte (z. B. Arbeitsstationen) interagieren oder **entfernte menschliche Benutzer**, also Benutzer, die indirekt über ein anderes IT-Produkt mit dem TOE interagieren.

Eine Zeitspanne der Interaktion zwischen Benutzern und der TSF wird als **Sitzung** bezeichnet. Der Aufbau von Benutzersitzungen kann auf der Grundlage einer Vielzahl an Überlegungen gesteuert werden, beispielsweise: Benutzerauthentifizierung, Tageszeit, Zugriffsmethode auf den TOE und Anzahl der erlaubten gleichzeitigen Sitzungen (je Benutzer oder insgesamt).

Dieser Teil vonISO/IEC 15408 verwendet den Begriff **autorisiert**, um einen Benutzer zu kennzeichnen, der die zur Durchführung einer Operation erforderlichen Rechte und/oder Privilegien besitzt. Der Begriff **autorisierter Benutzer** bedeutet also, dass für diesen Benutzer die Ausführung einer bestimmten Operation oder einer Reihe von Operationen, entsprechend der Definition in den SFRs, erlaubt ist.

Um Anforderungen zu formulieren, die eine Trennung von Administratoraufgaben verlangen, besagen die relevanten Sicherheitsfunktionskomponenten (der Familie FMT_SMR) explizit, dass administrative **Rollen** erforderlich sind. Eine Rolle ist ein vordefinierter Regelwerk, der die zulässigen Interaktionen zwischen einem Benutzer in dieser Rolle und dem TOE festlegt. Ein TOE kann die Definition einer beliebigen Anzahl an Rollen unterstützen. Beispielsweise können zu den Rollen für einen sicheren Betrieb eines TOEs „Auditadministrator“ und „Benutzerkontenadministrator“ gehören.

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

TOE-Ressourcen können auf viele unterschiedliche Arten aufgebaut und verwendet werden. Allerdings trifft dieser Teil von ISO/IEC 15408 eine bestimmte Unterscheidung, die die Spezifizierung gewünschter Sicherheitseigenschaften ermöglicht. Alle Entitäten die aus Ressourcen hergestellt werden können, können auf eine von zwei Arten gekennzeichnet werden. Die Entitäten können aktiv sein, also der Grund für eine Aktion innerhalb des TOEs und Operationen auf der Grundlage von Informationen ausgeführt werden.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

Alternativ können Entitäten auch passiv sein und sind dann entweder der Container, aus dem die Informationen kommen oder in dem die Informationen gespeichert werden.

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

a) solche die im Namen eines autorisierten Benutzers agieren (z. B. UNIX-Prozesse);

b) solche, die als ein spezifischer Funktionsprozess agieren, der wiederum im Namen mehrerer Benutzer handeln kann (z. B. Funktionen in Client-Server-Architekturen); oder

c) solche, die als Teil des TOEs selbst agieren (z. B. Prozesse, die nicht im Namen eines Benutzers agieren).

Dieser Teil von ISO/IEC 15408 behandelt die Durchsetzung der SFRs über die oben aufgeführten Subjekttypen.

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

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

Von Regeln in den SFRs kontrollierte Benutzer, Subjekte, Information, Objekte, Sitzungen und Ressourcen können gewisse **Attribute** aufweisen, die Informationen zur Verwendung durch den TOE für seinen korrekten Betrieb enthalten. Einige Attribute, wie Dateinamen, können informativ oder zur Identifizierung individueller Ressourcen ausgelegt sein, während andere Attribute, wie Informationen zur Zugriffskontrolle spezifisch für die Durchsetzung der SFRs existieren. Diese letztgenannten Attribute werden allgemein als **„Sicherheitsattribute“** bezeichnet. Das Wort Attribut wird in diesem Teil von ISO/IEC 15408 an einigen Stellen als Kurzform für das Wort „Sicherheitsattribut“ verwendet. Unabhängig von der bestimmungsgemäßen Verwendung der Attributinformation können Kontrollen der Attribute entsprechend der Vorgaben der SFRs erforderlich sein.

Daten in einem TOE werden entweder als Benutzerdaten oder TSF-Daten eingestuft. Bild 1 stellt diese Beziehung dar. **Benutzerdaten** sind in TOEs gespeicherte Informationen, die von Benutzern in Übereinstimmung mit den SFRs bedient werden können und die für die TSF keine besondere Bedeutung haben. Der Inhalt einer E-Mail gehört beispielsweise zu den Benutzerdaten. TSF-Daten sind Informationen, die TSFs bei der Entscheidungsfindung gemäß den Anforderungen der SFRs verwenden. **TSF-Daten** dürfen von Benutzern beeinflusst werden, wenn dies von den SFRs erlaubt wird. Sicherheitsattribute, Authentisierungsdaten, interne TSF-Statusvariablen, die von den in den SFRs definierten Regeln oder zum Schutz der TSFs verwendet werden, und Einträge in Zugriffskontrolllisten sind Beispiele für TSF-Daten.

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

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

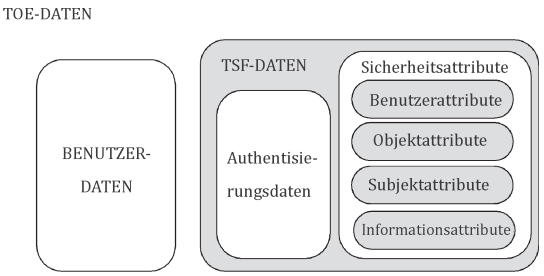

Bild 1 — Beziehung zwischen Benutzerdaten und TSF-Daten

Zwei bestimmte, in diesem Teil von ISO/IEC 15408 behandelte Attribute können identisch sein, müssen es aber nicht. Dabei handelt es sich um **Authentisierungsdaten** und **Sicherheitsinformationen**.

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

Der in diesem Teil von ISO/IEC 15408 verwendete Begriff Sicherheitsinformationen ist zwar auf Authentisierungsdaten anwendbar, soll aber auch auf andere Arten von Daten anwendbar sein, die geheim gehalten werden müssen um eine spezifische SFP durchzusetzen. Beispielsweise kann der Mechanismus eines vertrauenswürdigen Kanals, der zur Erhaltung der Vertraulichkeit bei der Übertragung von Informationen über den Kanal auf Kryptographie setzt, nur so stark sein, wie die verwendete Methode zur Geheimhaltung der kryptographischen Schlüssel vor unautorisierter Offenlegung.

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

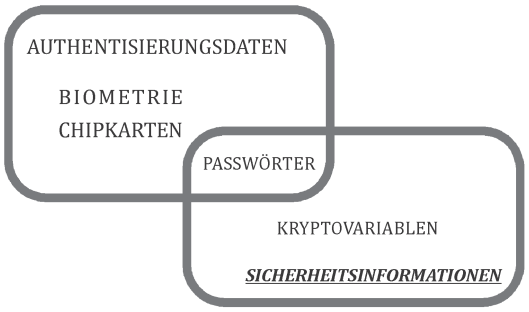

Bild 2 — Beziehung zwischen „Authentisierungsdaten“ und „Sicherheitsinformationen“

6 Sicherheitsfunktionskomponenten

6.1 Übersicht

Dieser Abschnitt definiert Inhalt und Darstellung der Funktionsanforderungen von ISO/IEC 15408 und bietet Leitlinien zur Organisation der Anforderungen an neue, in eine ST aufzunehmende Komponenten. Die Funktionsanforderungen werden in Klassen, Familien und Komponenten gefasst.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

6.1.1 Klassenstruktur

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

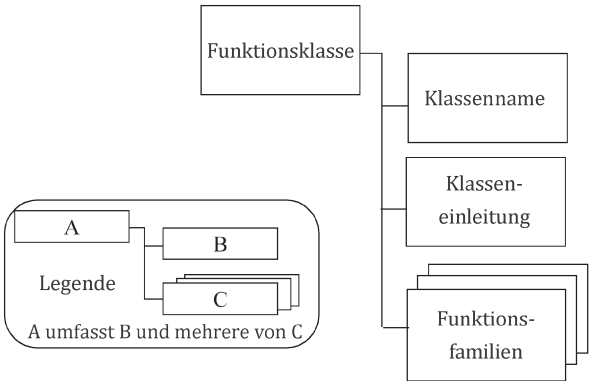

Bild 3 — Struktur der Funktionsklassen

6.1.1.1 Klassenname

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

6.1.1.2 Klasseneinleitung

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

Die Klasseneinleitung umfasst ein Bild mit der Beschreibung der Familien dieser Klasse und der Komponentenhierarchie in jeder Familie, entsprechend der Erklärungen in 6.2.

6.1.2 Familienstruktur

Bild 4 stellt die Struktur der Funktionsfamilien schematisch dar.

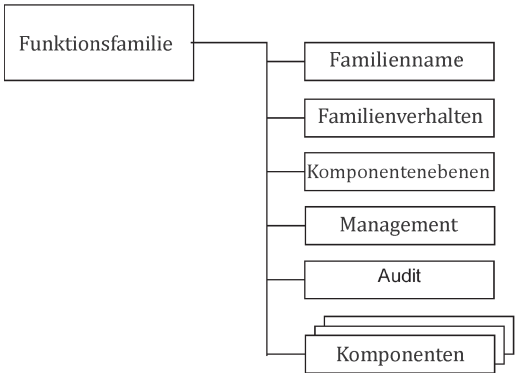

Bild 4 — Struktur der Funktionsfamilien

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

6.1.2.1 Familienname

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

6.1.2.2 Familienverhalten

Das Familienverhalten ist die ausformulierte Beschreibung der Funktionsfamilie mit Angabe der Sicherheitszielsetzungen und einer allgemeinen Beschreibung der Funktionsanforderungen. Diese werden im Folgenden ausführlicher beschrieben:

a) Die *Sicherheitszielsetzungen* der Familie behandeln ein Sicherheitsproblem, das mithilfe eines TOEs gelöst werden kann, der eine Komponente dieser Familie enthält.

b) Die Beschreibung der *Funktionsanforderungen* fasst alle in dieser Komponente (bzw. in diesen Komponenten) enthaltenen Anforderungen zusammen. Die Beschreibung richtet sich an Autoren von PPs, STs und Funktionspaketen, die bewerten möchten, ob die Familie für ihre spezifischen Anforderungen relevant ist.

6.1.2.3 Komponentenebenen

Funktionsfamilien enthalten eine oder mehrere Komponenten, bei der jede zur Einbindung in PPs, STs und Funktionspakete ausgewählt werden kann. Das Ziel dieses Unterabschnitts ist die Bereitstellung von Informationen für Benutzer zur Auswahl passender Funktionskomponenten, sobald die Familie als erforderlicher oder sinnvoller Teil ihrer Sicherheitsanforderungen identifiziert wurde.

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

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

Die Beschreibungen der Familien bieten, wie in 6.2 erklärt, eine grafische Übersicht der Komponentenhierarchie in einer Familie.

6.1.2.4 Management

Der Abschnitt *Management* enthält Informationen für die PP-/ST-Autoren, die bei Managementaktivitäten zu einer bestimmten Komponente zu beachten sind. Die Abschnitte verweisen auf Komponenten der Klasse Management (FMT) und bieten Leitlinien für potentielle Managementaktivitäten, die durch Operationen an diesen Komponenten angewendet werden können.

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

6.1.2.5 Audit

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

Beispielsweise könnte eine Auditanmerkung folgende Aktionen enthalten: Minimal – erfolgreiche Verwendung des Sicherheitsmechanismus; Einfach – jede Verwendung des Sicherheitsmechanismus und relevante Informationen zu den beteiligten Sicherheitsattributen; Detailliert – jede am Mechanismus durchgeführte Konfigurationsänderung, einschließlich der Konfigurationsistwerte vor und nach Änderung.

Es sollte beachtet werden, dass die Einstufung von auditierfähigen Ereignissen hierarchisch ist. Wenn beispielsweise einfache Auditgenerierung gewünscht ist, sollten alle als minimal und einfach identifizierten auditierfähigen Ereignisse über die entsprechenden Zuweisungsoperation in das PP/in die ST eingebunden werden; ausgenommen, wenn die höhere Ebene lediglich mehr Details als die niedrigere Ebene bereitstellt. Wenn detaillierte Auditgenerierung gewünscht ist, sollten alle auditierfähigen Ereignisse (minimal, einfach und detailliert) in das PP/in die ST eingebunden werden.

In der Klasse „FAU: Security audit“ werden die Regeln zum Steuern des Audits ausführlicher erklärt.

6.1.3 Komponentenstruktur

Bild 5 stellt die Struktur der Funktionskomponenten dar.

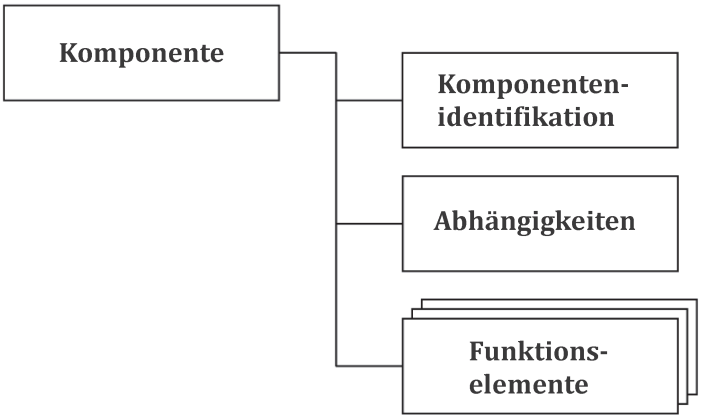

Bild 5 — Struktur der Funktionskomponenten

6.1.3.1 Komponentenidentifikation

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

Ein *eindeutiger Name*. Der Name spiegelt den Zweck der Komponente wider.

Ein *Kurzname*. Eine eindeutige Kurzform des Namens der Funktionskomponente. Dieser Kurzname dient als Hauptreferenzname zur Einstufung, Registrierung und Querverweisung der Komponente. Dieser Kurzname spiegelt die zugehörige Klasse und Familie der Komponente und die Komponentennummer innerhalb der Familie wider.

Eine *hierarchisch-zu-Liste*. Eine Liste anderer Komponenten, zu denen diese Komponente in einer hierarchischen Beziehung steht, und für die diese Komponente verwendet werden kann, Abhängigkeiten zu den aufgeführten Komponenten zu erfüllen.

6.1.3.2 Funktionselemente

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

Ein Funktionselement ist eine Sicherheitsfunktionsanforderung, die bei weiterer Aufteilung keine sinnvollen Evaluierungsergebnisse ergeben würde. Es ist die kleinste identifizierte und anerkannte Sicherheitsfunktionsanforderung in ISO/IEC 15408.

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

Es wird eine eindeutige Kurzform des Namens des Funktionselements bereitgestellt. Beispielsweise ist der Anforderungsname FDP_IFF.4.2 wie folgt zu interpretieren: F – Funktionsanforderung, DP – Klasse „Datenschutz Benutzer“ (en: DP = Data Protection), _IFF – Familie „Funktionen zur Informationsflusskontrolle“ (en: IFF = Information flow control functions), .4 – 4. Komponente namens „teilweise Vermeidung von unerlaubten Informationsflüssen”, .2 – 2. Element der Komponente.

6.1.3.3 Abhängigkeiten

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

Jede Funktionskomponente bietet eine vollständige Liste der Abhängigkeiten von anderen Funktions- und Sicherheitskomponenten. Einige Komponenten können auch „keine Abhängigkeiten“ auflisten. Die Komponenten, zu denen Abhängigkeiten bestehen, können wiederum selbst Abhängigkeiten zu anderen Komponenten haben. Die bereitgestellte Liste in den Komponenten umfasst nur direkte Abhängigkeiten. Das heißt, es gibt nur Verweisungen zu den für die korrekte Aufgabenausführung dieser Anforderung erforderlichen Funktionsanforderungen. Die indirekten Abhängigkeiten, also die aus den Abhängigkeiten anderer Komponenten entstehenden Abhängigkeiten, werden in Anhang A dieses Teils von ISO/IEC 15408 aufgeführt. Es wird darauf hingewiesen, dass die Abhängigkeit in einigen Fällen insofern optional ist, dass mehrere Funktionsanforderungen bereitgestellt werden, bei denen jede einzelne zur Erfüllung der Abhängigkeit ausreichen würde (siehe beispielsweise „FDP_UIT.1 Data exchange integrity“).

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

Die in diesem Teil von ISO/IEC 15408 angegebenen Abhängigkeiten sind normativ. Sie müssen innerhalb eines PPs/einer ST erfüllt werden. In bestimmten Situationen kann es vorkommen, dass die angegebenen Abhängigkeiten nicht anwendbar sein könnten. Der PP-/ST-Autor darf mit einer Begründung, warum die Abhängigkeit nicht anwendbar ist, die Komponente, zu der Abhängigkeit besteht, im Paket, im PP oder in der ST unberücksichtigt lassen.

6.2 Komponentenkatalog

Die Gruppierung von Komponenten in diesem Teil von ISO/IEC 15408 stellt keinerlei formale Taxonomie dar.

Dieser Teil von ISO/IEC 15408 enthält Klassen von Familien und Komponenten, die auf der Grundlage zusammenhängender Funktionen oder Zwecke grob gruppiert und in alphabetischer Reihenfolge dargestellt werden. Am Anfang jeder Klasse gibt es ein informatives Schaubild, das die Taxonomie jeder Klasse mit Darstellung der Familien jeder Klasse und den Komponenten jeder Familie aufzeigt. Das Schaubild ist ein sinnvoller Indikator der hierarchischen Beziehung, die möglicherweise zwischen den Komponenten besteht.

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

In jeder Klasse beschreibt ein Bild ähnlich dem Bild 6 die Hierarchie der Familie. Im Bild 6 enthält die erste Familie, Familie 1, drei hierarchische Komponenten, wobei Komponente 2 und Komponente 3 beide zur Erfüllung der Abhängigkeiten zu Komponente 1 verwendet werden können. Komponente 3 ist hierarchisch zu Komponente 2 und kann auch zur Erfüllung der Abhängigkeiten zu Komponente 2 verwendet werden.

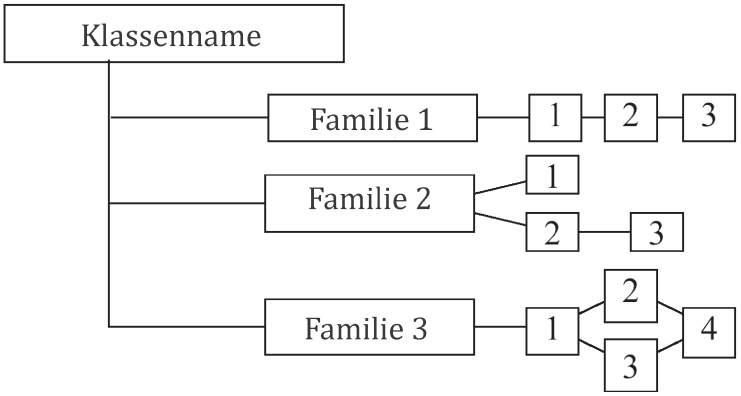

Bild 6 — Muster eines Klassenaufbaudiagramms

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

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

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

6.2.1 Hervorheben von Komponentenänderungen

Die Beziehung zwischen den Komponenten einer Familie wird durch **Fettmarkierung** hervorgehoben. Diese Fettmarkierung erfordert, dass alle neuen Anforderungen fett hervorgehoben werden. Für hierarchische Komponenten werden Anforderungen fett hervorgehoben, wenn sie über die Anforderungen der vorherigen Komponente hinaus erweitert oder geändert werden. Zusätzlich werden alle neuen oder erweiterten zulässigen über die vorherige Komponente hinausgehenden Operationen auch **fett** hervorgehoben.

7 Klasse FAU: Sicherheitsaudit

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

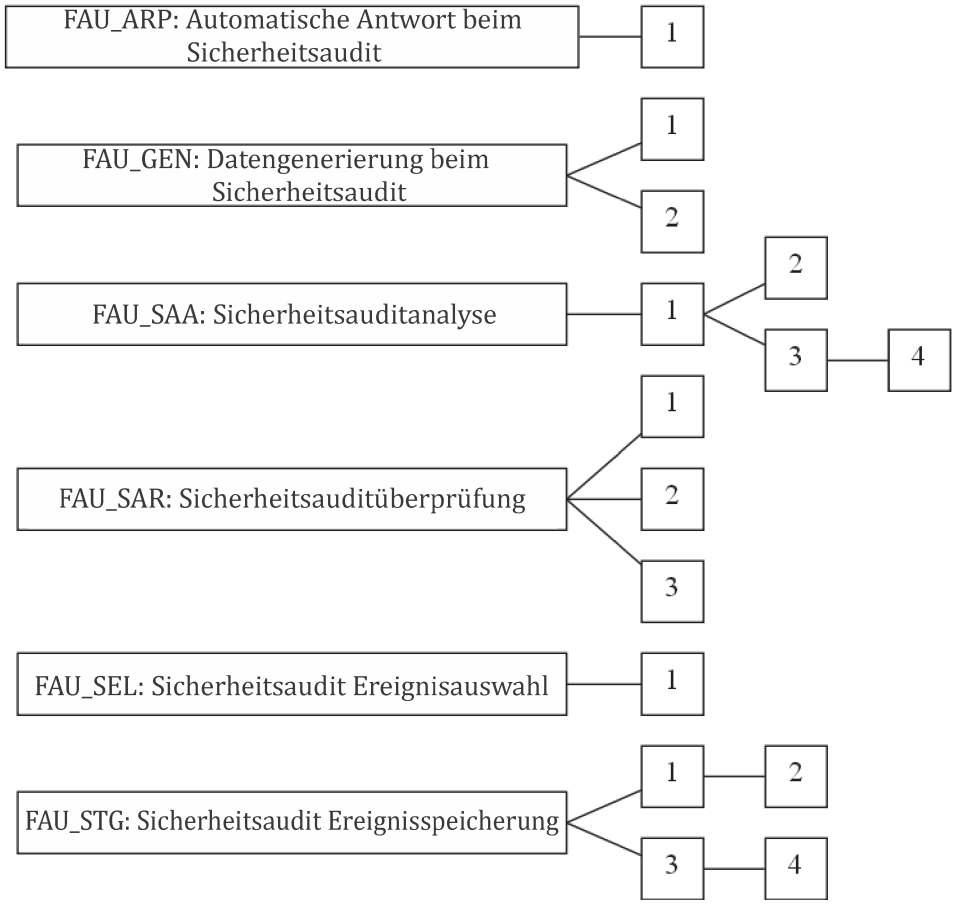

Bild 7 — FAU: Klassenaufbau Sicherheitsaudit

7.1 Automatische Antwort beim Sicherheitsaudit (FAU_ARP)

7.1.1 Familienverhalten

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

7.1.2 Komponentenebenen

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

7.1.3 Management von FAU_ARP.1

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

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

7.1.4 Audit von FAU_ARP.1

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

a) Minimal: Aktionen aufgrund von potentiellen Sicherheitsverstößen.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

7.1.5 FAU_ARP.1 Sicherheitsalarme

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_SAA.1 Potential violation analysis“

7.1.5.1 FAU_ARP.1.1

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

7.2 Datengenerierung beim Sicherheitsaudit (FAU_GEN)

7.2.1 Familienverhalten

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

7.2.2 Komponentenebenen

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

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

7.2.3 Management von FAU_GEN.1, FAU_GEN.2

Managementaktivitäten sind nicht vorgesehen.

7.2.4 Audit von FAU_GEN.1, FAU_GEN.2

Auditierfähige Ereignisse sind nicht vorgesehen.

7.2.5 FAU_GEN.1 Auditdatengenerierung

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FPT_STM.1 Reliable time stamps“

7.2.5.1 FAU_GEN.1.1

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

a) Einschaltung und Abschaltung der Auditfunktionen;

b) alle auditierfähigen Ereignisse für [Auswahl, eine auswählen: minimale, einfache, detaillierte, nicht spezifizierte] die Auditebene; und

c) [Zuweisung: *andere spezifisch definierte auditierfähige Ereignisse*].

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

7.2.5.2 FAU_GEN.1.2

Die TSF muss im Rahmen einer Auditaufzeichnung mindestens folgende Informationen aufzeichnen:

a) Datum und Uhrzeit des Ereignisses, Ereignisart, Subjektidentität (falls zutreffend) und Ergebnis (Erfolg oder Scheitern) des Ereignisses; und

b) für jede Auditereignisart auf der Grundlage der auditierfähigen Ereignisdefinitionen der in das PP/in die ST eingebundenen Funktionskomponenten, [Zuweisung: *andere auditrelevante Informationen*].

7.2.6 FAU_GEN.2 Verknüpfung der Benutzeridentität

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_GEN.1 Audit data generation“

„FIA_UID.1 Timing of identification“

7.2.6.1 FAU_GEN.2.1

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

7.3 Sicherheitsauditanalyse (FAU_SAA)

7.3.1 Familienverhalten

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

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

7.3.2 Komponentenebenen

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

Bei „FAU_SAA.2 Profile based anomaly detection“ enthält die TSF einzelne Profile zur Systemverwendung, wobei ein Profil die historischen Verwendungsmuster repräsentiert, die von Mitgliedern der Profilzielgruppe durchgeführt wurden. Eine Profilzielgruppe bezieht sich auf einen oder mehrere Einzelpersonen, die mit der TSF interagieren (z. B. einzelne Benutzer, Benutzer, die sich eine Gruppen ID oder ein Gruppenkonto teilen, unter einer zugewiesenen Rolle arbeitende Benutzer, Benutzer eines Gesamtsystems oder Netzwerkknotens). Jedes Mitglied einer Profilzielgruppe bekommt eine individuelle Verdachtswertung, die darstellt, wie gut die aktuelle Aktivität des Mitglieds mit den bekannten Verwendungsmustern im Profil übereinstimmt. Diese Analyse kann zur Laufzeit ausgeführt werden oder bei einer nachgelagerten Analyse im Batch-Modus.

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

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

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

7.3.3 Management von FAU_SAA.1

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

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

7.3.4 Management von FAU_SAA.2

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

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

7.3.5 Management von FAU_SAA.3

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

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

7.3.6 Management von FAU_SAA.4

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

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

b) Pflege (Löschen, Anpassen, Hinzufügen) der Menge von Systemereignisabfolgen.

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

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

a) Minimal: Aktivieren und Deaktivieren eines der Analysemechanismen;

b) Minimal: vom Tool automatisch ausgeführte Antworten.

7.3.8 FAU_SAA.1 Analyse potentieller Verstöße

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_GEN.1 Audit data generation“

7.3.8.1 FAU_SAA.1.1

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

7.3.8.2 FAU_SAA.1.2

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

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

b) [Zuweisung: *jede andere Regel*].

7.3.9 FAU_SAA.2 Profilbasierte Erkennung von Anomalien

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FIA_UID.1 Timing of identification“

7.3.9.1 FAU_SAA.2.1

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

7.3.9.2 FAU_SAA.2.2

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

7.3.9.3 FAU_SAA.2.3

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

7.3.10 FAU_SAA.3 Einfache Angriffsheuristiken

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: keine Abhängigkeiten

7.3.10.1 FAU_SAA.3.1

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

7.3.10.2 FAU_SAA.3.2

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

7.3.10.3 FAU_SAA.3.3

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

7.3.11 FAU_SAA.4 Komplexe Angriffsheuristiken

Hierarchisch zu: „FAU_SAA.3 Simple attack heuristics“

Abhängigkeiten: keine Abhängigkeiten

7.3.11.1 FAU_SAA.4.1

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

7.3.11.2 FAU_SAA.4.2

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

7.3.11.3 FAU_SAA.4.3

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

7.4 Sicherheitsauditüberprüfung (FAU_SAR)

7.4.1 Familienverhalten

Diese Familie definiert die Anforderungen an Audit-Tools, die für autorisierte Benutzer zur Unterstützung bei der Überprüfung von Auditdaten verfügbar sein sollten.

7.4.2 Komponentenebenen

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

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

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

7.4.3 Management von FAU_SAR.1

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

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

7.4.4 Management von FAU_SAR.2, FAU_SAR.3

Managementaktivitäten sind nicht vorgesehen.

7.4.5 Audit von FAU_SAR.1

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

a) Einfach: Lesen von Informationen aus den Auditaufzeichnungen.

7.4.6 Audit von FAU_SAR.2

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

a) Einfach: nicht erfolgreiche Leseversuche von Informationen aus den Auditaufzeichnungen.

7.4.7 Audit von FAU_SAR.3

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

a) Detailliert: die für die Einsicht verwendeten Parameter.

7.4.8 FAU_SAR.1 Auditüberprüfung

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_GEN.1 Audit data generation“

7.4.8.1 FAU_SAR.1.1

Die TSF muss [Zuweisung: *autorisierte Benutzer*] die Möglichkeit zum Lesen von [Zuweisung: *Liste der Auditinformationen*] aus den Auditaufzeichnungen bieten.

7.4.8.2 FAU_SAR.1.2

Die TSF muss die Auditaufzeichnungen in einer für den Benutzer geeigneten Weise zur Interpretation der Informationen bereitstellen.

7.4.9 FAU_SAR.2 Beschränkte Auditüberprüfung

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_SAR.1 Audit review“

7.4.9.1 FAU_SAR.2.1

Die TSF muss allen Benutzern, außer den Benutzern mit explizit gewährtem Lesezugriff, den Lesezugriff auf die Auditaufzeichnungen verwehren.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

7.4.10 FAU_SAR.3 Auswählbare Auditüberprüfung

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_SAR.1 Audit review“

7.4.10.1 FAU_SAR.3.1

Die TSF muss die Fähigkeit zur Anwendung von [Zuweisung: *Methoden zur Auswahl und/oder Anordnung*] von Auditdaten auf der Grundlage von [Zuweisung: *Kriterien mit logischen Beziehungen*] bereitstellen.

7.5 Sicherheitsaudit Ereignisauswahl (FAU_SEL)

7.5.1 Familienverhalten

Diese Familie definiert Anforderungen zur Auswahl der Menge an Ereignissen, aus der Menge aller auditierfähigen Ereignisse, die während des TOE-Betriebs zu auditieren sind.

7.5.2 Komponentenebenen

„FAU_SEL.1 Selective audit“ erfordert die Fähigkeit zur Auswahl der Menge zu auditierender Ereignisse aus der Menge aller auditierfähigen Ereignisse, entsprechend Identifikation in „FAU_GEN.1 Audit data generation“, auf der Grundlage von durch den PP-/ST-Autor zu spezifizierenden Attributen.

7.5.3 Management von FAU_SEL.1

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

a) Pflege der Rechte zum Einsehen/Anpassen der Auditereignisse.

7.5.4 Audit von FAU_SEL.1

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

a) Minimal: alle während der Auditsammlungsfunktionen auftretenden Änderungen an der Auditkonfiguration.

7.5.5 FAU_SEL.1 Auswählbares Audit

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_GEN.1 Audit data generation“

„FMT_MTD.1 Management of TSF data“

7.5.5.1 FAU_SEL.1.1

Die TSF muss in der Lage sein, die Reihe Menge zu auditierender Ereignisse aus der Menge aller auditierfähigen Ereignisse auf der Grundlage folgender Attribute auszuwählen:

a) [Auswahl: *Objektidentität, Benutzeridentität, Subjektidentität, Host-Identität, Ereignisart*];

b) [Zuweisung: *Liste der zusätzlichen Attribute, auf denen die Auswählbarkeit des Audits basiert*].

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

7.6 Sicherheitsaudit Ereignisspeicherung (FAU_STG)

7.6.1 Familienverhalten

Diese Familie definiert die Anforderungen an die TSF, um einen sicheren Audit-Trail zu erstellen und zu pflegen. „Gespeicherte Auditaufzeichnungen“ bezieht sich auf die Datensätze innerhalb des Audit-Trails und nicht auf Auditaufzeichnungen, die durch Auswahl (über temporäre Speicherung) bereitgestellt wurden.

7.6.2 Komponentenebenen

Bei „FAU_STG.1 Protected audit trail storage“ werden Anforderungen an den Audit-Trail gestellt. Er wird vor unautorisierter Löschung und/oder Änderung geschützt.

„FAU_STG.2 Guarantees of audit data availability“ spezifiziert die von einer TSF verwalteten Garantien für Auditdaten für den Fall, dass ein unerwünschter Zustand eintritt.

„FAU_STG.3 Action in case of possible audit data loss“ legt Aktionen fest, die beim Überschreiten eines Schwellwerts des Audit-Trails auszuführen sind.

„FAU_STG.4 Prevention of audit data loss“ legt Aktionen fest für den Fall, dass der Audit-Trail voll ist.

7.6.3 Management von FAU_STG.1

Managementaktivitäten sind nicht vorgesehen.

7.6.4 Management von FAU_STG.2

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

a) Pflege der Parameter zur Steuerung der Fähigkeit zur Auditspeicherung.

7.6.5 Management von FAU_STG.3

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

a) Pflege des Schwellwerts;

b) Pflege (Löschen, Anpassen, Hinzufügen) von Aktionen die im Falle eines drohenden Versagens der Auditspeicherung auszuführen sind.

7.6.6 Management von FAU_STG.4

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

a) Pflege (Löschen, Anpassen, Hinzufügen) von Aktionen die im Falle eines Versagens der Auditspeicherung auszuführen sind.

7.6.7 Audit von FAU_STG.1, FAU_STG.2

Auditierfähige Ereignisse sind nicht vorgesehen.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

7.6.8 Audit von FAU_STG.3

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

a) Einfach: Aufgrund Überschreiten eines Schwellwerts ausgeführte Aktionen.

7.6.9 Audit von FAU_STG.4

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

a) Einfach: Aufgrund von Ausfall der Audit-Speicherung ausgeführte Aktionen.

7.6.10 FAU_STG.1 Geschützte Speicherung des Audit-Trails

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_GEN.1 Audit data generation“

7.6.10.1 FAU_STG.1.1

Die TSF muss die gespeicherten Auditaufzeichnungen im Audit-Trail vor unautorisiertem Löschen schützen.

7.6.10.2 FAU_STG.1.2

Die TSF muss in der Lage sein, unautorisierte Änderungen an den gespeicherten Auditaufzeichnungen im Audit-Trail zu [Auswahl, eine auswählen: *verhindern, erkennen*].

7.6.11 FAU_STG.2 Garantien zur Auditdatenverfügbarkeit

Hierarchisch zu: „FAU_STG.1 Protected audit trail storage“

Abhängigkeiten: „FAU_GEN.1 Audit data generation“

7.6.11.1 FAU_STG.2.1

Die TSF muss die gespeicherten Auditaufzeichnungen im Audit-Trail vor unautorisiertem Löschen schützen.

7.6.11.2 FAU_STG.2.2

Die TSF muss in der Lage sein, unautorisierte Änderungen an den gespeicherten Auditaufzeichnungen im Audit-Trail zu [Auswahl, eine auswählen: *verhindern, erkennen*].

7.6.11.3 FAU_STG.2.3

Die TSF muss sicherstellen, dass [Zuweisung: *Metrik für das Speichern von Auditaufzeichnungen*] gespeicherte Auditaufzeichnungen behalten werden, wenn folgende Bedingungen eintreten: [Auswahl: *Ausschöpfung der Auditspeicherung, Ausfall, Angriff*].

7.6.12 FAU_STG.3 Aktionen bei möglichem Auditdatenverlust

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FAU_STG.1 Protected audit trail storage“

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

7.6.12.1 FAU_STG.3.1

Die TSF muss [Zuweisung: *bei möglichem Fehler in der Auditspeicherung auszuführende Aktionen*], wenn der Audit-Trail [Zuweisung: *vordefinierte Grenze*] überschreitet.

7.6.13 FAU_STG.4 Verhinderung von Auditdatenverlust

Hierarchisch zu: „FAU_STG.3 Action in case of possible audit data loss“

Abhängigkeiten: „FAU_STG.1 Protected audit trail storage“

7.6.13.1 FAU_STG.4.1

Die TSF muss **[Auswahl, eine auswählen: *„auditierte Ereignisse ignorieren“, „auditierte Ereignisse verhindern, ausgenommen Ereignisse von autorisierten Benutzern mit besonderen Rechten“, „die ältesten gespeicherten Auditaufzeichnungen überschreiben“*] und** [Zuweisung: ***andere Aktionen*** *beim Fehler in der Auditspeicherung durchführen*], wenn der Audit-Trail **voll ist.**

8 Klasse FCO: Kommunikation

Diese Klasse bietet zwei Familien, die sich spezifisch mit der Identitätssicherung einer am Datenaustausch teilnehmenden Partei befassen. Diese Familien beziehen sich auf die Identitätssicherung des Absenders der übertragenen Information (Ursprungsnachweis) und die Identitätssicherung des Empfängers der übertragenen Information (Empfangsnachweis). Diese Familien stellen sicher, dass ein Absenders das Senden einer Nachricht und ein Empfänger das Empfangen einer Nachricht nicht abstreiten kann.

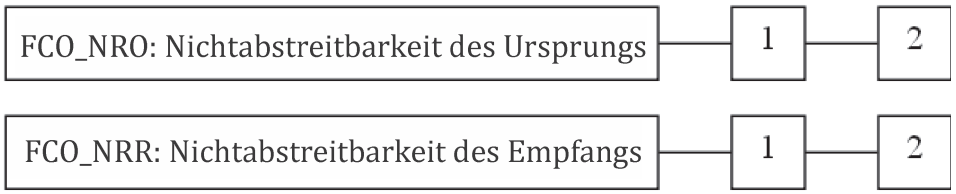

Bild 8 — FCO: Klassenaufbau Kommunikation

8.1 Nichtabstreitbarkeit des Ursprungs (FCO_NRO)

8.1.1 Familienverhalten

Nichtabstreitbarkeit des Ursprungs stellt sicher, dass der Absender der Information das Senden der Information nicht erfolgreich abstreiten kann. Diese Familie erfordert von der TSF die Bereitstellung einer Methode zur Sicherstellung, dass ein Subjekt, das während eines Datenaustauschs Informationen erhält einen Nachweis über die Herkunft der Information erhält. Dieser Nachweis kann anschließend entweder von diesem Subjekt oder anderen Subjekten verifiziert werden.

8.1.2 Komponentenebenen

„FCO_NRO.1 Selective proof of origin“ erfordert von der TSF den Subjekten die Möglichkeit zu geben, Beweise für die Herkunft von Informationen zu verlangen.

„FCO_NRO.2 Enforced proof of origin“ erfordert, dass die TSF immer einen Ursprungsnachweis der übertragenen Informationen generiert.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

8.1.3 Management von FCO_NRO.1, FCO_NRO.2

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

a) Management von Änderungen an Informationsarten, Feldern, Absenderattributen und Nachweisempfängern.

8.1.4 Audit von FCO_NRO.1

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

a) minimal: die Identität des Benutzers, der den Ursprungsnachweis angefragt hat, wird generiert;

b) minimal: der Aufruf des Dienstes zur Nichtabstreitbarkeit;

c) einfach: Identifizierung der Information, des Ziels und eine Kopie der vorgelegten Nachweise;

d) detailliert: die Identität des Benutzers, der die Verifizierung der Nachweise angefragt hat.

8.1.5 Audit von FCO_NRO.2

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

a) minimal: der Aufruf des Dienstes zur Nichtabstreitbarkeit;

b) einfach: Identifizierung der Information, des Ziels und eine Kopie der vorgelegten Nachweise wird bereitgestellt;

c) detailliert: die Identität des Benutzers, der die Verifizierung der Nachweise angefragt hat.

8.1.6 FCO_NRO.1 Auswählbarer Ursprungsnachweis

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FIA_UID.1 Timing of identification“

8.1.6.1 FCO_NRO.1.1

Die TSF muss in der Lage sein, einen Ursprungsnachweis für übertragene [Zuweisung: *Liste der Informationsarten*] auf Anfrage des [Auswahl: *Absenders, Empfängers, [Zuweisung: Liste von Dritten]*] zu generieren.

8.1.6.2 FCO_NRO.1.2

Die TSF muss in der Lage sein, sich auf die [Zuweisung: *Liste der Attribute*] des Informationsabsenders zu beziehen und auf die [Zuweisung: *Liste der Informationsfelder*] der für den Nachweis gültigen Information.

8.1.6.3 FCO_NRO.1.3

Die TSF muss eine Fähigkeit zum Verifizieren des Ursprungsnachweises der Information für vorgegebene [Auswahl: *Absender, Empfänger, [Zuweisung: Liste von Dritten]*] bereitstellen, vorausgesetzt [Zuweisung: *Einschränkungen zum Ursprungsnachweis*].

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

8.1.7 FCO_NRO.2 Erzwungener Ursprungsnachweis

Hierarchisch zu: „FCO_NRO.1 Selective proof of origin“

Abhängigkeiten: „FIA_UID.1 Timing of identification“

8.1.7.1 FCO_NRO.2.1

Die TSF muss **die Generierung** eines Ursprungsnachweises für übertragene [Zuweisung: *Liste der Informationsarten*] zu **jeder Zeit durchsetzen**.

8.1.7.2 FCO_NRO.2.2

Die TSF muss in der Lage sein, sich auf die [Zuweisung: *Liste der Attribute*] des Informationsabsenders zu beziehen und auf die [Zuweisung: *Liste der Informationsfelder*] der für den Nachweis gültigen Information.

8.1.7.3 FCO_NRO.2.3

Die TSF muss eine Fähigkeit zum Verifizieren des Ursprungsnachweises der Information für vorgegebene [Auswahl: *Absender, Empfänger, [Zuweisung: Liste von Dritten]*] bereitstellen, vorausgesetzt [Zuweisung: *Einschränkungen zum Ursprungsnachweis*].

8.2 Nichtabstreitbarkeit des Empfangs (FCO_NRR)

8.2.1 Familienverhalten

Nichtabstreitbarkeit des Empfangs stellt sicher, dass der Empfänger der Information den Empfang der Information nicht erfolgreich abstreiten kann. Diese Familie erfordert von der TSF die Bereitstellung einer Methode zur Sicherstellung, dass ein Subjekt, das während eines Datenaustauschs Informationen übermittelt einen Empfangsnachweis der Information erhält. Dieser Nachweis kann anschließend entweder von diesem Subjekt oder anderen Subjekten verifiziert werden.

8.2.2 Komponentenebenen

„FCO_NRR.1 Selective proof of receipt“ erfordert von der TSF den Subjekten die Möglichkeit zu geben, einen Nachweis über den Erhalt von Informationen zu verlangen.

„FCO_NRR.2 Enforced proof of receipt“ erfordert, dass die TSF immer einen Empfangsnachweis der empfangenen Informationen generiert.

8.2.3 Management von FCO_NRR.1, FCO_NRR.2

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

a) Management von Änderungen an Informationsarten, Feldern, Absenderattributen und dritten Nachweisempfängern.

8.2.4 Audit von FCO_NRR.1

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

a) minimal: die Identität des Benutzers, der den Empfangsnachweis angefragt hat, wird generiert;

b) minimal: der Aufruf des Dienstes zur Nichtabstreitbarkeit;

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

c) einfach: Identifizierung der Information, des Ziels und eine Ausfertigung des Nachweises wird bereitgestellt;

d) detailliert: die Identität des Benutzers, der die Verifizierung des Nachweises angefragt hat.

8.2.5 Audit von FCO_NRR.2

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

a) minimal: der Aufruf des Dienstes zur Nichtabstreitbarkeit;

b) einfach: Identifizierung der Information, des Ziels und eine Ausfertigung des Nachweises wird bereitgestellt;

c) detailliert: die Identität des Benutzers, der die Verifizierung des Nachweises angefragt hat.

8.2.6 FCO_NRR.1 Auswählbarer Empfangssnachweis

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: „FIA_UID.1 Timing of identification“

8.2.6.1 FCO_NRR.1.1

Die TSF muss in der Lage sein, einen Empfangsnachweis für empfangene [Zuweisung: *Liste der Informationsarten*] auf Anfrage des [Auswahl: *Absenders, Empfängers, [Zuweisung: Liste von Dritten]*] zu generieren.

8.2.6.2 FCO_NRR.1.2

Die TSF muss in der Lage sein, die [Zuweisung: *Liste der Attribute*] des Informationsempfängers und die [Zuweisung: *Liste der Informationsfelder*] der für den Nachweis gültigen Information in Beziehung zu setzen.

8.2.6.3 FCO_NRR.1.3

Die TSF muss in der Lage sein, den Nachweis des Erhalts von Informationen für vorgegebene [Auswahl: *Absender, Empfänger, [Zuweisung: Liste von Dritten]*] zu verifizieren, vorausgesetzt [Zuweisung: *Einschränkungen zum Empfangsnachweis*].

8.2.7 FCO_NRR.2 Erzwungener Empfangsnachweis

Hierarchisch zu: „FCO_NRR.1 Selective proof of receipt“

Abhängigkeiten: „FIA_UID.1 Timing of identification“

8.2.7.1 FCO_NRR.2.1

Die TSF muss **die Generierung** eines Empfangsnachweises für empfangene [Zuweisung: *Liste der Informationsarten*] zu **jeder Zeit durchsetzen**.

8.2.7.2 FCO_NRR.2.2

Die TSF muss in der Lage sein, die [Zuweisung: *Liste der Attribute*] des Informationsempfängers und die [Zuweisung: *Liste der Informationsfelder*] der für den Nachweis gültigen Information in Beziehung zu setzen.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 15408-2:2020-12

8.2.7.3 FCO_NRR.2.3

Die TSF muss in der Lage sein, den Nachweis des Erhalts von Informationen für vorgegebene [Auswahl: *Absender, Empfänger, [Zuweisung: Liste von Dritten]*] zu verifizieren, vorausgesetzt [Zuweisung: *Einschränkungen zum Empfangsnachweis*].

9 Klasse FCS: Kryptographische Unterstützung

Die TSF kann zur Unterstützung bei der Erfüllung einiger hoher Sicherheitszielsetzungen kryptographische Funktionen einsetzen. Zu diesen gehören (ohne darauf begrenzt zu sein): Identifikation und Authentifizierung, Nichtabstreitbarkeit, vertrauenswürdiger Pfad, vertrauenswürdiger Kanal und Datentrennung. Diese Klasse wird verwendet, wenn kryptographische Funktionen im TOE implementiert sind; die Implementation könnte dabei über Hardware, Firmware und/oder Software erfolgen.

Die Klasse „FCS: Cryptographic support“ besteht aus zwei Familien: „Cryptographic key management“ (FCS_CKM) und „Cryptographic operation“ (FCS_COP). Die Familie „Cryptographic key management“ (FCS_CKM) behandelt die Verwaltung von kryptographischen Schlüsseln und die Familie „Cryptographic operation“ (FCS_COP) beschäftigt sich mit dem betriebsmäßigen Einsatz dieser kryptographischen Schlüssel.

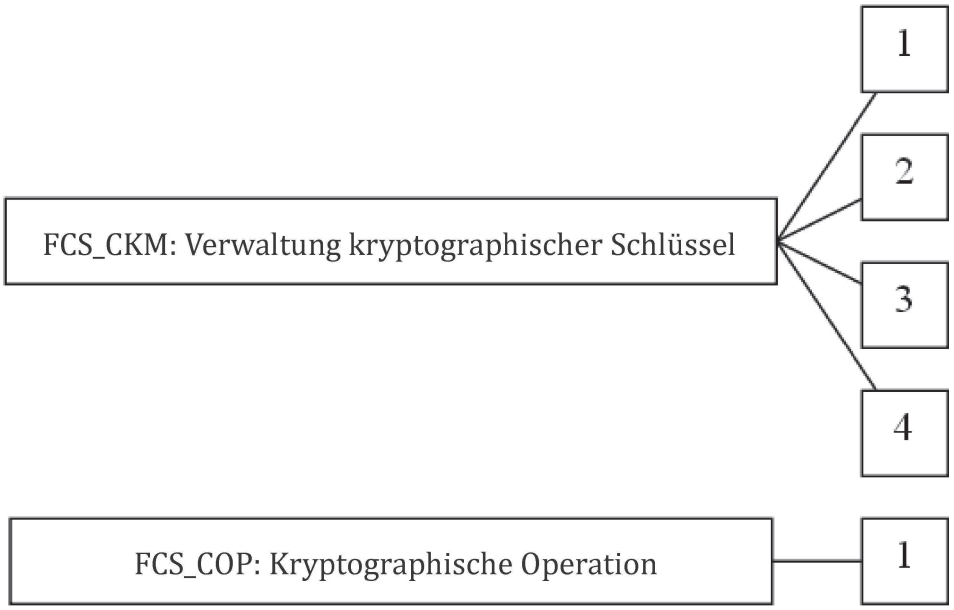

Bild 9 — FCS: Klassenaufbau Kryptographische Unterstützung

9.1 Verwaltung kryptographischer Schlüssel (FCS_CKM)

9.1.1 Familienverhalten

Kryptographische Schlüssel müssen über ihren gesamten Lebenszyklus verwaltet werden. Diese Familie ist für die Unterstützung dieses Lebenszyklus ausgelegt und definiert daher die Anforderungen an folgende Aktivitäten: Generierung kryptographischer Schlüssel, Verteilung kryptographischer Schlüssel, Zugriff auf kryptographische Schlüssel und Zerstörung kryptographischer Schlüssel. Bei Funktionsanforderungen an die Verwaltung von kryptographischen Schlüsseln sollte diese Familie eingebunden werden.

9.1.2 Komponentenebenen

„FCS_CKM.1 Cryptographic key generation“ erfordert die Generierung von kryptographischen Schlüsseln in Übereinstimmung mit einem spezifizierten Algorithmus und Schlüsselgrößen, die auf einer zugewiesenen Norm basieren können.

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

„FCS_CKM.2 Cryptographic key distribution“ erfordert die Verteilung von kryptographischen Schlüsseln in Übereinstimmung mit einer spezifizierten Verteilungsmethode, die auf einer zugewiesenen Norm basieren kann.

„FCS_CKM.3 Cryptographic key access“ erfordert den Zugriff auf kryptographische Schlüssel in Übereinstimmung mit einer spezifizierten Zugriffsmethode, die auf einer zugewiesenen Norm basieren kann.

„FCS_CKM.4 Cryptographic key destruction“ erfordert die Zerstörung von kryptographischen Schlüsseln in Übereinstimmung mit einer spezifizierten Zerstörungsmethode, die auf einer zugewiesenen Norm basieren kann.

9.1.3 Management von FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4

Managementaktivitäten sind nicht vorgesehen.

9.1.4 Audit von FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4

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

a) minimal: Erfolg und Scheitern der Aktivität;

b) einfach: Objektattribut(e) und Objektwert(e) ausschließlich aller sensiblen Informationen (z. B. geheime oder private Schlüssel).

9.1.5 FCS_CKM.1 Generierung kryptographischer Schlüssel

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: [„FCS_CKM.2 Cryptographic key distribution“ oder
„FCS_COP.1 Cryptographic operation“]
„FCS_CKM.4 Cryptographic key destruction“

9.1.5.1 FCS_CKM.1.1

Die TSF muss kryptographische Schlüssel in Übereinstimmung mit einem spezifizierten Algorithmus zur Generierung von kryptographischen Schlüsseln [Zuweisung: *Algorithmus zur Generierung von kryptographischen Schlüsseln*] und spezifizierten Größen kryptographischer Schlüssel [Zuweisung: *Größen kryptographischer Schlüssel*] generieren, die folgende Normen erfüllen: [Zuweisung: *Liste der Normen*].

9.1.6 FCS_CKM.2 Verteilung kryptographischer Schlüssel

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: [„FDP_ITC.1 Import of user data without security attributes“ oder
„FDP_ITC.2 Import of user data with security attributes“ oder
„FCS_CKM.1 Cryptographic key generation“]
„FCS_CKM.4 Cryptographic key destruction“

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12

9.1.6.1 FCS_CKM.2.1

Die TSF muss kryptographische Schlüssel in Übereinstimmung mit einer spezifizierten Verteilungsmethode für kryptographische Schlüssel [Zuweisung: *Verteilungsmethode für kryptographische Schlüssel*] verteilen, die folgende Normen erfüllt: [Zuweisung: *Liste der Normen*].

9.1.7 FCS_CKM.3 Zugriff auf kryptographische Schlüssel

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: [„FDP_ITC.1 Import of user data without security attributes“ oder

„FDP_ITC.2 Import of user data with security attributes“ oder

„FCS_CKM.1 Cryptographic key generation“]

„FCS_CKM.4 Cryptographic key destruction“

9.1.7.1 FCS_CKM.3.1

Die TSF muss [Zuweisung: *Art des Zugriffs auf kryptographische Schlüssel*] in Übereinstimmung mit einer spezifizierten Zugriffsmethode für kryptographische Schlüssel [Zuweisung: *Zugriffsmethode für kryptographische Schlüssel*] durchführen, die folgende Normen erfüllt: [Zuweisung: *Liste der Normen*].

9.1.8 FCS_CKM.4 Zerstörung kryptographischer Schlüssel

Hierarchisch zu: keinen anderen Komponenten.

Abhängigkeiten: [„FDP_ITC.1 Import of user data without security attributes“ oder

„FDP_ITC.2 Import of user data with security attributes“ oder

„FCS_CKM.1 Cryptographic key generation“]

9.1.8.1 FCS_CKM.4.1

Die TSF muss kryptographische Schlüssel in Übereinstimmung mit einer spezifizierten Zerstörungsmethode für kryptographische Schlüssel [Zuweisung: *Zerstörungsmethode für kryptographische Schlüssel*] zerstören, die folgende Normen erfüllt: [Zuweisung: *Liste der Normen*].

9.2 Kryptographische Operation (FCS_COP)

9.2.1 Familienverhalten

Zur korrekten Funktion einer kryptographischen Operation muss sie in Übereinstimmung mit einem spezifizierten Algorithmus und mit einem kryptographischen Schlüssel einer spezifizierten Größe durchgeführt werden. Bei Anforderungen an kryptographische Operationen sollte diese Familie eingebunden werden.

Zu üblichen kryptographischen Operationen gehören Datenverschlüsselung und/oder Datenentschlüsselung, Generierung digitaler Signaturen und/oder Verifizierung, Generierung von kryptographischen Prüfsummen, sichere Hash-Werte („Message Digest“), Verschlüsselung und Entschlüsselung kryptographischer Schlüssel und Übereinstimmung kryptographischer Schlüssel.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 15408-2:2020-12