DIN EN ISO/IEC 15408-2

DIN

ICS 35.030

Entwurf

Einsprüche bis 2019-12-11
Vorgesehen als Ersatz für
die 2011-03 zurückgezogene
Norm
DIN ISO/IEC 15408-2:2007-11

Informationstechnik – Sicherheitstechniken – Bewertungskriterien für die IT-Sicherheit – Teil 2: Sicherheitsfunktionskomponenten (ISO/IEC 15408-2:2008); Englische Fassung prEN ISO/IEC 15408-2:2019

Information technology –
Security techniques – Evaluation criteria for IT security –
Part 2: Security functional components (ISO/IEC 15408-2:2008);
English version prEN ISO/IEC 15408-2:2019

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 anglaise prEN ISO/IEC 15408-2:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-10-11 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 238 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

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 prEN ISO/IEC 15408-2:2019 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).

Dieser Europäische Norm-Entwurf enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die englische Originalfassung der ISO/IEC Norm.

Änderungen

Gegenüber der bereits 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.

Nationaler Anhang NA
(informativ)

Begriffe und Abkürzungen

3. Begriffe, Symbole und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 15408-1.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

Contents

Page

Foreword xviii
Introduction xx
1 Scope 1
2 Normative references 1
3 Terms and definitions, symbols and abbreviated terms 1
4 Overview 1
4.1 Organisation of this part of ISO/IEC 15408 1
5 Functional requirements paradigm 2
6 Security functional components 5
6.1 Overview 5
6.1.1 Class structure 5
6.1.2 Family structure 6
6.1.3 Component structure 8
6.2 Component catalogue 9
6.2.1 Component changes highlighting 10
7 Class FAU: Security audit 10
7.1 Security audit automatic response (FAU_ARP) 11
7.1.1 Family Behaviour 11
7.1.2 Component levelling 11
7.1.3 Management of FAU_ARP.1 11
7.1.4 Audit of FAU_ARP.1 11
7.1.5 FAU_ARP.1 Security alarms 11
7.2 Security audit data generation (FAU_GEN) 11
7.2.1 Family Behaviour 11
7.2.2 Component levelling 11
7.2.3 Management of FAU_GEN.1, FAU_GEN.2 11
7.2.4 Audit of FAU_GEN.1, FAU_GEN.2 11
7.2.5 FAU_GEN.1 Audit data generation 12
7.2.6 FAU_GEN.2 User identity association 12
7.3 Security audit analysis (FAU_SAA) 12
7.3.1 Family Behaviour 12
7.3.2 Component levelling 12
7.3.3 Management of FAU_SAA.1 13
7.3.4 Management of FAU_SAA.2 13
7.3.5 Management of FAU_SAA.3 13
7.3.6 Management of FAU_SAA.4 13
7.3.7 Audit of FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4 13
7.3.8 FAU_SAA.1 Potential violation analysis 13
7.3.9 FAU_SAA.2 Profile based anomaly detection 14
7.3.10 FAU_SAA.3 Simple attack heuristics 14
7.3.11 FAU_SAA.4 Complex attack heuristics 15
7.4 Security audit review (FAU_SAR) 15
7.4.1 Family Behaviour 15
7.4.2 Component levelling 15
7.4.3 Management of FAU_SAR.1 15
7.4.4 Management of FAU_SAR.2, FAU_SAR.3 15
7.4.5 Audit of FAU_SAR.1 15
7.4.6 Audit of FAU_SAR.2 16
7.4.7 Audit of FAU_SAR.3 16

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

7.4.8 FAU_SAR.1 Audit review 16
7.4.9 FAU_SAR.2 Restricted audit review 16
7.4.10 FAU_SAR.3 Selectable audit review 16
7.5 Security audit event selection (FAU_SEL) 16
7.5.1 Family Behaviour 16
7.5.2 Component levelling 17
7.5.3 Management of FAU_SEL.1 17
7.5.4 Audit of FAU_SEL.1 17
7.5.5 FAU_SEL.1 Selective audit 17
7.6 Security audit event storage (FAU_STG) 17
7.6.1 Family Behaviour 17
7.6.2 Component levelling 17
7.6.3 Management of FAU_STG.1 18
7.6.4 Management of FAU_STG.2 18
7.6.5 Management of FAU_STG.3 18
7.6.6 Management of FAU_STG.4 18
7.6.7 Audit of FAU_STG.1, FAU_STG.2 18
7.6.8 Audit of FAU_STG.3 18
7.6.9 Audit of FAU_STG.4 18
7.6.10 FAU_STG.1 Protected audit trail storage 18
7.6.11 FAU_STG.2 Guarantees of audit data availability 19
7.6.12 FAU_STG.3 Action in case of possible audit data loss 19
7.6.13 FAU_STG.4 Prevention of audit data loss 19

8 Class FCO: Communication 20
8.1 Non-repudiation of origin (FCO_NRO) 20
8.1.1 Family Behaviour 20
8.1.2 Component levelling 20
8.1.3 Management of FCO_NRO.1, FCO_NRO.2 20
8.1.4 Audit of FCO_NRO.1 20
8.1.5 Audit of FCO_NRO.2 21
8.1.6 FCO_NRO.1 Selective proof of origin 21
8.1.7 FCO_NRO.2 Enforced proof of origin 21
8.2 Non-repudiation of receipt (FCO_NRR) 22
8.2.1 Family Behaviour 22
8.2.2 Component levelling 22
8.2.3 Management of FCO_NRR.1, FCO_NRR.2 22
8.2.4 Audit of FCO_NRR.1 22
8.2.5 Audit of FCO_NRR.2 22
8.2.6 FCO_NRR.1 Selective proof of receipt 22
8.2.7 FCO_NRR.2 Enforced proof of receipt 23

9 Class FCS: Cryptographic support 24
9.1 Cryptographic key management (FCS_CKM) 24
9.1.1 Family Behaviour 24
9.1.2 Component levelling 24
9.1.3 Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 25
9.1.4 Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 25
9.1.5 FCS_CKM.1 Cryptographic key generation 25
9.1.6 FCS_CKM.2 Cryptographic key distribution 25
9.1.7 FCS_CKM.3 Cryptographic key access 25
9.1.8 FCS_CKM.4 Cryptographic key destruction 26
9.2 Cryptographic operation (FCS_COP) 26
9.2.1 Family Behaviour 26
9.2.2 Component levelling 26
9.2.3 Management of FCS_COP.1 26
9.2.4 Audit of FCS_COP.1 26
9.2.5 FCS_COP.1 Cryptographic operation 27

10 Class FDP: User data protection 27
10.1 Access control policy (FDP_ACC) 29

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

10.1.1 Family Behaviour 29
10.1.2 Component levelling 30
10.1.3 Management of FDP_ACC.1, FDP_ACC.2 30
10.1.4 Audit of FDP_ACC.1, FDP_ACC.2 30
10.1.5 FDP_ACC.1 Subset access control 30
10.1.6 FDP_ACC.2 Complete access control 30
10.2 Access control functions (FDP_ACF) 30
10.2.1 Family Behaviour 30
10.2.2 Component levelling 30
10.2.3 Management of FDP_ACF.1 31
10.2.4 Audit of FDP_ACF.1 31
10.2.5 FDP_ACF.1 Security attribute based access control 31
10.3 Data authentication (FDP_DAU) 32
10.3.1 Family Behaviour 32
10.3.2 Component levelling 32
10.3.3 Management of FDP_DAU.1, FDP_DAU.2 32
10.3.4 Audit of FDP_DAU.1 32
10.3.5 Audit of FDP_DAU.2 32
10.3.6 FDP_DAU.1 Basic Data Authentication 32
10.3.7 FDP_DAU.2 Data Authentication with Identity of Guarantor 33
10.4 Export from the TOE (FDP_ETC) 33
10.4.1 Family Behaviour 33
10.4.2 Component levelling 33
10.4.3 Management of FDP_ETC.1 33
10.4.4 Management of FDP_ETC.2 33
10.4.5 Audit of FDP_ETC.1, FDP_ETC.2 33
10.4.6 FDP_ETC.1 Export of user data without security attributes 34
10.4.7 FDP_ETC.2 Export of user data with security attributes 34
10.5 Information flow control policy (FDP_IFC) 34
10.5.1 Family Behaviour 34
10.5.2 Component levelling 35
10.5.3 Management of FDP_IFC.1, FDP_IFC.2 35
10.5.4 Audit of FDP_IFC.1, FDP_IFC.2 35
10.5.5 FDP_IFC.1 Subset information flow control 35
10.5.6 FDP_IFC.2 Complete information flow control 35
10.6 Information flow control functions (FDP_IFF) 35
10.6.1 Family Behaviour 35
10.6.2 Component levelling 36
10.6.3 Management of FDP_IFF.1, FDP_IFF.2 36
10.6.4 Management of FDP_IFF.3, FDP_IFF.4, FDP_IFF.5 36
10.6.5 Management of FDP_IFF.6 36
10.6.6 Audit of FDP_IFF.1, FDP_IFF.2, FDP_IFF.5 36
10.6.7 Audit of FDP_IFF.3, FDP_IFF.4, FDP_IFF.6 37
10.6.8 FDP_IFF.1 Simple security attributes 37
10.6.9 FDP_IFF.2 Hierarchical security attributes 37
10.6.10 FDP_IFF.3 Limited illicit information flows 38
10.6.11 FDP_IFF.4 Partial elimination of illicit information flows 39
10.6.12 FDP_IFF.5 No illicit information flows 39
10.6.13 FDP_IFF.6 Illicit information flow monitoring 39
10.7 Import from outside of the TOE (FDP_ITC) 39
10.7.1 Family Behaviour 39
10.7.2 Component levelling 39
10.7.3 Management of FDP_ITC.1, FDP_ITC.2 40
10.7.4 Audit of FDP_ITC.1, FDP_ITC.2 40
10.7.5 FDP_ITC.1 Import of user data without security attributes 40
10.7.6 FDP_ITC.2 Import of user data with security attributes 40
10.8 Internal TOE transfer (FDP_ITT) 41
10.8.1 Family Behaviour 41
10.8.2 Component levelling 41
10.8.3 Management of FDP_ITT.1, FDP_ITT.2 41

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

10.8.4 Management of FDP_ITT.3, FDP_ITT.4 42
10.8.5 Audit of FDP_ITT.1, FDP_ITT.2 42
10.8.6 Audit of FDP_ITT.3, FDP_ITT.4 42
10.8.7 FDP_ITT.1 Basic internal transfer protection 42
10.8.8 FDP_ITT.2 Transmission separation by attribute 42
10.8.9 FDP_ITT.3 Integrity monitoring 43
10.8.10 FDP_ITT.4 Attribute-based integrity monitoring 43
10.9 Residual information protection (FDP_RIP) 43
10.9.1 Family Behaviour 43
10.9.2 Component levelling 44
10.9.3 Management of FDP_RIP.1, FDP_RIP.2 44
10.9.4 Audit of FDP_RIP.1, FDP_RIP.2 44
10.9.5 FDP_RIP.1 Subset residual information protection 44
10.9.6 FDP_RIP.2 Full residual information protection 44
10.10 Rollback (FDP_ROL) 44
10.10.1 Family Behaviour 44
10.10.2 Component levelling 44
10.10.3 Management of FDP_ROL.1, FDP_ROL.2 45
10.10.4 Audit of FDP_ROL.1, FDP_ROL.2 45
10.10.5 FDP_ROL.1 Basic rollback 45
10.10.6 FDP_ROL.2 Advanced rollback 45
10.11 Stored data integrity (FDP_SDI) 46
10.11.1 Family Behaviour 46
10.11.2 Component levelling 46
10.11.3 Management of FDP_SDI.1 46
10.11.4 Management of FDP_SDI.2 46
10.11.5 Audit of FDP_SDI.1 46
10.11.6 Audit of FDP_SDI.2 46
10.11.7 FDP_SDI.1 Stored data integrity monitoring 46
10.11.8 FDP_SDI.2 Stored data integrity monitoring and action 47
10.12 Inter-TSF user data confidentiality transfer protection (FDP_UCT) 47
10.12.1 Family Behaviour 47
10.12.2 Component levelling 47
10.12.3 Management of FDP_UCT.1 47
10.12.4 Audit of FDP_UCT.1 47
10.12.5 FDP_UCT.1 Basic data exchange confidentiality 47
10.13 Inter-TSF user data integrity transfer protection (FDP_UIT) 48
10.13.1 Family Behaviour 48
10.13.2 Component levelling 48
10.13.3 Management of FDP_UIT.1, FDP_UIT.2, FDP_UIT.3 48
10.13.4 Audit of FDP_UIT.1 48
10.13.5 Audit of FDP_UIT.2, FDP_UIT.3 48
10.13.6 FDP_UIT.1 Data exchange integrity 49
10.13.7 FDP_UIT.2 Source data exchange recovery 49
10.13.8 FDP_UIT.3 Destination data exchange recovery 49

11 Class FIA: Identification and authentication 50
11.1 Authentication failures (FIA_AFL) 51
11.1.1 Family Behaviour 51
11.1.2 Component levelling 51
11.1.3 Management of FIA_AFL.1 52
11.1.4 Audit of FIA_AFL.1 52
11.1.5 FIA_AFL.1 Authentication failure handling 52
11.2 User attribute definition (FIA_ATD) 52
11.2.1 Family Behaviour 52
11.2.2 Component levelling 52
11.2.3 Management of FIA_ATD.1 52
11.2.4 Audit of FIA_ATD.1 52
11.2.5 FIA_ATD.1 User attribute definition 53
11.3 Specification of secrets (FIA_SOS) 53

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

11.3.1 Family Behaviour 53
11.3.2 Component levelling 53
11.3.3 Management of FIA_SOS.1 53
11.3.4 Management of FIA_SOS.2 53
11.3.5 Audit of FIA_SOS.1, FIA_SOS.2 53
11.3.6 FIA_SOS.1 Verification of secrets 53
11.3.7 FIA_SOS.2 TSF Generation of secrets 54
11.4 User authentication (FIA_UAU) 54
11.4.1 Family Behaviour 54
11.4.2 Component levelling 54
11.4.3 Management of FIA_UAU.1 54
11.4.4 Management of FIA_UAU.2 55
11.4.5 Management of FIA_UAU.3, FIA_UAU.4, FIA_UAU.7 55
11.4.6 Management of FIA_UAU.5 55
11.4.7 Management of FIA_UAU.6 55
11.4.8 Audit of FIA_UAU.1 55
11.4.9 Audit of FIA_UAU.2 55
11.4.10 Audit of FIA_UAU.3 55
11.4.11 Audit of FIA_UAU.4 56
11.4.12 Audit of FIA_UAU.5 56
11.4.13 Audit of FIA_UAU.6 56
11.4.14 Audit of FIA_UAU.7 56
11.4.15 FIA_UAU.1 Timing of authentication 56
11.4.16 FIA_UAU.2 User authentication before any action 56
11.4.17 FIA_UAU.3 Unforgeable authentication 57
11.4.18 FIA_UAU.4 Single-use authentication mechanisms 57
11.4.19 FIA_UAU.5 Multiple authentication mechanisms 57
11.4.20 FIA_UAU.6 Re-authenticating 57
11.4.21 FIA_UAU.7 Protected authentication feedback 57
11.5 User identification (FIA_UID) 58
11.5.1 Family Behaviour 58
11.5.2 Component levelling 58
11.5.3 Management of FIA_UID.1 58
11.5.4 Management of FIA_UID.2 58
11.5.5 Audit of FIA_UID.1, FIA_UID.2 58
11.5.6 FIA_UID.1 Timing of identification 58
11.5.7 FIA_UID.2 User identification before any action 59
11.6 User-subject binding (FIA_USB) 59
11.6.1 Family Behaviour 59
11.6.2 Component levelling 59
11.6.3 Management of FIA_USB.1 59
11.6.4 Audit of FIA_USB.1 59
11.6.5 FIA_USB.1 User-subject binding 59

12 Class FMT: Security management 60
12.1 Management of functions in TSF (FMT_MOF) 61
12.1.1 Family Behaviour 61
12.1.2 Component levelling 61
12.1.3 Management of FMT_MOF.1 61
12.1.4 Audit of FMT_MOF.1 62
12.1.5 FMT_MOF.1 Management of security functions behaviour 62
12.2 Management of security attributes (FMT_MSA) 62
12.2.1 Family Behaviour 62
12.2.2 Component levelling 62
12.2.3 Management of FMT_MSA.1 62
12.2.4 Management of FMT_MSA.2 62
12.2.5 Management of FMT_MSA.3 63
12.2.6 Management of FMT_MSA.4 63
12.2.7 Audit of FMT_MSA.1 63
12.2.8 Audit of FMT_MSA.2 63

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

12.2.9 Audit of FMT_MSA.3 63
12.2.10 Audit of FMT_MSA.4 63
12.2.11 FMT_MSA.1 Management of security attributes 63
12.2.12 FMT_MSA.2 Secure security attributes 64
12.2.13 FMT_MSA.3 Static attribute initialisation 64
12.2.14 FMT_MSA.4 Security attribute value inheritance 64
12.3 Management of TSF data (FMT_MTD) 65
12.3.1 Family Behaviour 65
12.3.2 Component levelling 65
12.3.3 Management of FMT_MTD.1 65
12.3.4 Management of FMT_MTD.2 65
12.3.5 Management of FMT_MTD.3 65
12.3.6 Audit of FMT_MTD.1 65
12.3.7 Audit of FMT_MTD.2 65
12.3.8 Audit of FMT_MTD.3 65
12.3.9 FMT_MTD.1 Management of TSF data 65
12.3.10 FMT_MTD.2 Management of limits on TSF data 66
12.3.11 FMT_MTD.3 Secure TSF data 66
12.4 Revocation (FMT_REV) 66
12.4.1 Family Behaviour 66
12.4.2 Component levelling 66
12.4.3 Management of FMT_REV.1 66
12.4.4 Audit of FMT_REV.1 67
12.4.5 FMT_REV.1 Revocation 67
12.5 Security attribute expiration (FMT_SAE) 67
12.5.1 Family Behaviour 67
12.5.2 Component levelling 67
12.5.3 Management of FMT_SAE.1 67
12.5.4 Audit of FMT_SAE.1 67
12.5.5 FMT_SAE.1 Time-limited authorisation 67
12.6 Specification of Management Functions (FMT_SMF) 68
12.6.1 Family Behaviour 68
12.6.2 Component levelling 68
12.6.3 Management of FMT_SMF.1 68
12.6.4 Audit of FMT_SMF.1 68
12.6.5 FMT_SMF.1 Specification of Management Functions 68
12.7 Security management roles (FMT_SMR) 68
12.7.1 Family Behaviour 68
12.7.2 Component levelling 69
12.7.3 Management of FMT_SMR.1 69
12.7.4 Management of FMT_SMR.2 69
12.7.5 Management of FMT_SMR.3 69
12.7.6 Audit of FMT_SMR.1 69
12.7.7 Audit of FMT_SMR.2 69
12.7.8 Audit of FMT_SMR.3 69
12.7.9 FMT_SMR.1 Security roles 69
12.7.10 FMT_SMR.2 Restrictions on security roles 70
12.7.11 FMT_SMR.3 Assuming roles 70

13 Class FPR: Privacy 71
13.1 Anonymity (FPR_ANO) 71
13.1.1 Family Behaviour 71
13.1.2 Component levelling 71
13.1.3 Management of FPR_ANO.1, FPR_ANO.2 71
13.1.4 Audit of FPR_ANO.1, FPR_ANO.2 71
13.1.5 FPR_ANO.1 Anonymity 72
13.1.6 FPR_ANO.2 Anonymity without soliciting information 72
13.2 Pseudonymity (FPR_PSE) 72
13.2.1 Family Behaviour 72
13.2.2 Component levelling 72

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

13.2.3 Management of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 72
13.2.4 Audit of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 72
13.2.5 FPR_PSE.1 Pseudonymity 73
13.2.6 FPR_PSE.2 Reversible pseudonymity 73
13.2.7 FPR_PSE.3 Alias pseudonymity 73
13.3 Unlinkability (FPR_UNL) 74
13.3.1 Family Behaviour 74
13.3.2 Component levelling 74
13.3.3 Management of FPR_UNL.1 74
13.3.4 Audit of FPR_UNL.1 74
13.3.5 FPR_UNL.1 Unlinkability 74
13.4 Unobservability (FPR_UNO) 74
13.4.1 Family Behaviour 74
13.4.2 Component levelling 75
13.4.3 Management of FPR_UNO.1, FPR_UNO.2 75
13.4.4 Management of FPR_UNO.3 75
13.4.5 Management of FPR_UNO.4 75
13.4.6 Audit of FPR_UNO.1, FPR_UNO.2 75
13.4.7 Audit of FPR_UNO.3 75
13.4.8 Audit of FPR_UNO.4 75
13.4.9 FPR_UNO.1 Unobservability 75
13.4.10 FPR_UNO.2 Allocation of information impacting unobservability 76
13.4.11 FPR_UNO.3 Unobservability without soliciting information 76
13.4.12 FPR_UNO.4 Authorised user observability 76

14 Class FPT: Protection of the TSF 76
14.1 Fail secure (FPT_FLS) 77
14.1.1 Family Behaviour 77
14.1.2 Component levelling 78
14.1.3 Management of FPT_FLS.1 78
14.1.4 Audit of FPT_FLS.1 78
14.1.5 FPT_FLS.1 Failure with preservation of secure state 78
14.2 Availability of exported TSF data (FPT_ITA) 78
14.2.1 Family Behaviour 78
14.2.2 Component levelling 78
14.2.3 Management of FPT_ITA.1 78
14.2.4 Audit of FPT_ITA.1 78
14.2.5 FPT_ITA.1 Inter-TSF availability within a defined availability metric 78
14.3 Confidentiality of exported TSF data (FPT_ITC) 79
14.3.1 Family Behaviour 79
14.3.2 Component levelling 79
14.3.3 Management of FPT_ITC.1 79
14.3.4 Audit of FPT_ITC.1 79
14.3.5 FPT_ITC.1 Inter-TSF confidentiality during transmission 79
14.4 Integrity of exported TSF data (FPT_ITI) 79
14.4.1 Family Behaviour 79
14.4.2 Component levelling 79
14.4.3 Management of FPT_ITI.1 80
14.4.4 Management of FPT_ITI.2 80
14.4.5 Audit of FPT_ITI.1 80
14.4.6 Audit of FPT_ITI.2 80
14.4.7 FPT_ITI.1 Inter-TSF detection of modification 80
14.4.8 FPT_ITI.2 Inter-TSF detection and correction of modification 80
14.5 Internal TOE TSF data transfer (FPT_ITT) 81
14.5.1 Family Behaviour 81
14.5.2 Component levelling 81
14.5.3 Management of FPT_ITT.1 81
14.5.4 Management of FPT_ITT.2 81
14.5.5 Management of FPT_ITT.3 81
14.5.6 Audit of FPT_ITT.1, FPT_ITT.2 82

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

14.5.7 Audit of FPT_ITT.3 82
14.5.8 FPT_ITT.1 Basic internal TSF data transfer protection....82
14.5.9 FPT_ITT.2 TSF data transfer separation....82
14.5.10 FPT_ITT.3 TSF data integrity monitoring 82
14.6 TSF physical protection (FPT_PHP) 83
14.6.1 Family Behaviour....83
14.6.2 Component levelling 83
14.6.3 Management of FPT_PHP.1 83
14.6.4 Management of FPT_PHP.2 83
14.6.5 Management of FPT_PHP.3 83
14.6.6 Audit of FPT_PHP.1 83
14.6.7 Audit of FPT_PHP.2 84
14.6.8 Audit of FPT_PHP.3 84
14.6.9 FPT_PHP.1 Passive detection of physical attack....84
14.6.10 FPT_PHP.2 Notification of physical attack 84
14.6.11 FPT_PHP.3 Resistance to physical attack 84
14.7 Trusted recovery (FPT_RCV)....85
14.7.1 Family Behaviour....85
14.7.2 Component levelling 85
14.7.3 Management of FPT_RCV.1 85
14.7.4 Management of FPT_RCV.2, FPT_RCV.3 85
14.7.5 Management of FPT_RCV.4 85
14.7.6 Audit of FPT_RCV.1, FPT_RCV.2, FPT_RCV.3....85
14.7.7 Audit of FPT_RCV.4....85
14.7.8 FPT_RCV.1 Manual recovery....86
14.7.9 FPT_RCV.2 Automated recovery....86
14.7.10 FPT_RCV.3 Automated recovery without undue loss....86
14.7.11 FPT_RCV.4 Function recovery 87
14.8 Replay detection (FPT_RPL)....87
14.8.1 Family Behaviour....87
14.8.2 Component levelling 87
14.8.3 Management of FPT_RPL.1 87
14.8.4 Audit of FPT_RPL.1 87
14.8.5 FPT_RPL.1 Replay detection....87
14.9 State synchrony protocol (FPT_SSP)....88
14.9.1 Family Behaviour....88
14.9.2 Component levelling 88
14.9.3 Management of FPT_SSP.1, FPT_SSP.2 88
14.9.4 Audit of FPT_SSP.1, FPT_SSP.2 88
14.9.5 FPT_SSP.1 Simple trusted acknowledgement 88
14.9.6 FPT_SSP.2 Mutual trusted acknowledgement....88
14.10 Time stamps (FPT_STM)....89
14.10.1 Family Behaviour....89
14.10.2 Component levelling 89
14.10.3 Management of FPT_STM.1 89
14.10.4 Audit of FPT_STM.1....89
14.10.5 FPT_STM.1 Reliable time stamps....89
14.11 Inter-TSF TSF data consistency (FPT_TDC) 89
14.11.1 Family Behaviour....89
14.11.2 Component levelling 89
14.11.3 Management of FPT_TDC.1 89
14.11.4 Audit of FPT_TDC.1 89
14.11.5 FPT_TDC.1 Inter-TSF basic TSF data consistency 90
14.12 Testing of external entities (FPT_TEE)....90
14.12.1 Family Behaviour....90
14.12.2 Component levelling 90
14.12.3 Management of FPT_TEE.1....90
14.12.4 Audit of FPT_TEE.1....90
14.12.5 FPT_TEE.1 Testing of external entities 90
14.13 Internal TOE TSF data replication consistency (FPT_TRC) 91

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

14.13.1 Family Behaviour 91
14.13.2 Component levelling 91
14.13.3 Management of FPT_TRC.1 91
14.13.4 Audit of FPT_TRC.1 91
14.13.5 FPT_TRC.1 Internal TSF consistency 91
14.14 TSF self test (FPT_TST) 92
14.14.1 Family Behaviour 92
14.14.2 Component levelling 92
14.14.3 Management of FPT_TST.1 92
14.14.4 Audit of FPT_TST.1 92
14.14.5 FPT_TST.1 TSF testing 92

15 Class FRU: Resource utilisation 93
15.1 Fault tolerance (FRU_FLT) 93
15.1.1 Family Behaviour 93
15.1.2 Component levelling 93
15.1.3 Management of FRU_FLT.1, FRU_FLT.2 93
15.1.4 Audit of FRU_FLT.1 93
15.1.5 Audit of FRU_FLT.2 93
15.1.6 FRU_FLT.1 Degraded fault tolerance 94
15.1.7 FRU_FLT.2 Limited fault tolerance 94
15.2 Priority of service (FRU_PRS) 94
15.2.1 Family Behaviour 94
15.2.2 Component levelling 94
15.2.3 Management of FRU_PRS.1, FRU_PRS.2 94
15.2.4 Audit of FRU_PRS.1, FRU_PRS.2 94
15.2.5 FRU_PRS.1 Limited priority of service 94
15.2.6 FRU_PRS.2 Full priority of service 95
15.3 Resource allocation (FRU_RSA) 95
15.3.1 Family Behaviour 95
15.3.2 Component levelling 95
15.3.3 Management of FRU_RSA.1 95
15.3.4 Management of FRU_RSA.2 95
15.3.5 Audit of FRU_RSA.1, FRU_RSA.2 96
15.3.6 FRU_RSA.1 Maximum quotas 96
15.3.7 FRU_RSA.2 Minimum and maximum quotas 96

16 Class FTA: TOE access 97
16.1 Limitation on scope of selectable attributes (FTA_LSA) 97
16.1.1 Family Behaviour 97
16.1.2 Component levelling 97
16.1.3 Management of FTA_LSA.1 97
16.1.4 Audit of FTA_LSA.1 97
16.1.5 FTA_LSA.1 Limitation on scope of selectable attributes 98
16.2 Limitation on multiple concurrent sessions (FTA_MCS) 98
16.2.1 Family Behaviour 98
16.2.2 Component levelling 98
16.2.3 Management of FTA_MCS.1 98
16.2.4 Management of FTA_MCS.2 98
16.2.5 Audit of FTA_MCS.1, FTA_MCS.2 98
16.2.6 FTA_MCS.1 Basic limitation on multiple concurrent sessions 98
16.2.7 FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions 99
16.3 Session locking and termination (FTA_SSL) 99
16.3.1 Family Behaviour 99
16.3.2 Component levelling 99
16.3.3 Management of FTA_SSL.1 99
16.3.4 Management of FTA_SSL.2 99
16.3.5 Management of FTA_SSL.3 99
16.3.6 Management of FTA_SSL.4 100
16.3.7 Audit of FTA_SSL.1, FTA_SSL.2 100
16.3.8 Audit of FTA_SSL.3 100

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

16.3.9 Audit of FTA_SSL.4 100
16.3.10 FTA_SSL.1 TSF-initiated session locking 100
16.3.11 FTA_SSL.2 User-initiated locking 100
16.3.12 FTA_SSL.3 TSF-initiated termination 101
16.3.13 FTA_SSL.4 User-initiated termination 101
16.4 TOE access banners (FTA_TAB) 101
16.4.1 Family Behaviour 101
16.4.2 Component levelling 101
16.4.3 Management of FTA_TAB.1 101
16.4.4 Audit of FTA_TAB.1 101
16.4.5 FTA_TAB.1 Default TOE access banners 101
16.5 TOE access history (FTA_TAH) 102
16.5.1 Family Behaviour 102
16.5.2 Component levelling 102
16.5.3 Management of FTA_TAH.1 102
16.5.4 Audit of FTA_TAH.1 102
16.5.5 FTA_TAH.1 TOE access history 102
16.6 TOE session establishment (FTA_TSE) 102
16.6.1 Family Behaviour 102
16.6.2 Component levelling 102
16.6.3 Management of FTA_TSE.1 103
16.6.4 Audit of FTA_TSE.1 103
16.6.5 FTA_TSE.1 TOE session establishment 103

17 Class FTP: Trusted path/channels 103
17.1 Inter-TSF trusted channel (FTP_ITC) 104
17.1.1 Family Behaviour 104
17.1.2 Component levelling 104
17.1.3 Management of FTP_ITC.1 104
17.1.4 Audit of FTP_ITC.1 104
17.1.5 FTP_ITC.1 Inter-TSF trusted channel 104
17.2 Trusted path (FTP_TRP) 105
17.2.1 Family Behaviour 105
17.2.2 Component levelling 105
17.2.3 Management of FTP_TRP.1 105
17.2.4 Audit of FTP_TRP.1 105
17.2.5 FTP_TRP.1 Trusted path 105

Annex A (normative) Security functional requirements application notes 107
A.1 Structure of the notes 107
A.1.1 Class structure 107
A.1.2 Family structure 108
A.1.3 Component structure 109
A.2 Dependency tables 109

Annex B (normative) Functional classes, families, and components 115

Annex C (normative) Class FAU: Security audit 116
C.1 Audit requirements in a distributed environment 116
C.2 Security audit automatic response (FAU_ARP) 117
C.2.1 User notes 117
C.2.2 FAU_ARP.1 Security alarms 117
C.3 Security audit data generation (FAU_GEN) 118
C.3.1 User notes 118
C.3.2 FAU_GEN.1 Audit data generation 119
C.3.3 FAU_GEN.2 User identity association 120
C.4 Security audit analysis (FAU_SAA) 120
C.4.1 User notes 120
C.4.2 FAU_SAA.1 Potential violation analysis 120
C.4.3 FAU_SAA.2 Profile based anomaly detection 121
C.4.4 FAU_SAA.3 Simple attack heuristics 122
C.4.5 FAU_SAA.4 Complex attack heuristics 122

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

C.5 Security audit review (FAU_SAR) 123
C.5.1 User notes 123
C.5.2 FAU_SAR.1 Audit review 124
C.5.3 FAU_SAR.2 Restricted audit review 124
C.5.4 FAU_SAR.3 Selectable audit review 124
C.6 Security audit event selection (FAU_SEL) 125
C.6.1 User notes 125
C.6.2 FAU_SEL.1 Selective audit 125
C.7 Security audit event storage (FAU_STG) 125
C.7.1 User notes 125
C.7.2 FAU_STG.1 Protected audit trail storage 126
C.7.3 FAU_STG.2 Guarantees of audit data availability 126
C.7.4 FAU_STG.3 Action in case of possible audit data loss 126
C.7.5 FAU_STG.4 Prevention of audit data loss 127

Annex D (normative) Class FCO: Communication 128
D.1 Non-repudiation of origin (FCO_NRO) 128
D.1.1 User notes 128
D.1.2 FCO_NRO.1 Selective proof of origin 129
D.1.3 FCO_NRO.2 Enforced proof of origin 129
D.2 Non-repudiation of receipt (FCO_NRR) 130
D.2.1 User notes 130
D.2.2 FCO_NRR.1 Selective proof of receipt 130
D.2.3 FCO_NRR.2 Enforced proof of receipt 131

Annex E (normative) Class FCS: Cryptographic support 132
E.1 Cryptographic key management (FCS_CKM) 133
E.1.1 User notes 133
E.1.2 FCS_CKM.1 Cryptographic key generation 134
E.1.3 FCS_CKM.2 Cryptographic key distribution 134
E.1.4 FCS_CKM.3 Cryptographic key access 134
E.1.5 FCS_CKM.4 Cryptographic key destruction 135
E.2 Cryptographic operation (FCS_COP) 135
E.2.1 User notes 135
E.2.2 FCS_COP.1 Cryptographic operation 136

Annex F (normative) Class FDP: User data protection 137
F.1 Access control policy (FDP_ACC) 140
F.1.1 User notes 140
F.1.2 FDP_ACC.1 Subset access control 140
F.1.3 FDP_ACC.2 Complete access control 141
F.2 Access control functions (FDP_ACF) 141
F.2.1 User notes 141
F.2.2 FDP_ACF.1 Security attribute based access control 141
F.3 Data authentication (FDP_DAU) 143
F.3.1 User notes 143
F.3.2 FDP_DAU.1 Basic Data Authentication 143
F.3.3 FDP_DAU.2 Data Authentication with Identity of Guarantor 143
F.4 Export from the TOE (FDP_ETC) 143
F.4.1 User notes 143
F.4.2 FDP_ETC.1 Export of user data without security attributes 144
F.4.3 FDP_ETC.2 Export of user data with security attributes 144
F.5 Information flow control policy (FDP_IFC) 145
F.5.1 User notes 145
F.5.2 FDP_IFC.1 Subset information flow control 146
F.5.3 FDP_IFC.2 Complete information flow control 146
F.6 Information flow control functions (FDP_IFF) 146
F.6.1 User notes 146
F.6.2 FDP_IFF.1 Simple security attributes 147
F.6.3 FDP_IFF.2 Hierarchical security attributes 148
F.6.4 FDP_IFF.3 Limited illicit information flows 149

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

F.6.5 FDP_IFF.4 Partial elimination of illicit information flows 149
F.6.6 FDP_IFF.5 No illicit information flows 150
F.6.7 FDP_IFF.6 Illicit information flow monitoring 150
F.7 Import from outside of the TOE (FDP_ITC) 151
F.7.1 User notes 151
F.7.2 FDP_ITC.1 Import of user data without security attributes 152
F.7.3 FDP_ITC.2 Import of user data with security attributes 152
F.8 Internal TOE transfer (FDP_ITT) 152
F.8.1 User notes 152
F.8.2 FDP_ITT.1 Basic internal transfer protection 153
F.8.3 FDP_ITT.2 Transmission separation by attribute 153
F.8.4 FDP_ITT.3 Integrity monitoring 153
F.8.5 FDP_ITT.4 Attribute-based integrity monitoring 154
F.9 Residual information protection (FDP_RIP) 155
F.9.1 User notes 155
F.9.2 FDP_RIP.1 Subset residual information protection 156
F.9.3 FDP_RIP.2 Full residual information protection 156
F.10 Rollback (FDP_ROL) 156
F.10.1 User notes 156
F.10.2 FDP_ROL.1 Basic rollback 157
F.10.3 FDP_ROL.2 Advanced rollback 157
F.11 Stored data integrity (FDP_SDI) 158
F.11.1 User notes 158
F.11.2 FDP_SDI.1 Stored data integrity monitoring 158
F.11.3 FDP_SDI.2 Stored data integrity monitoring and action 158
F.12 Inter-TSF user data confidentiality transfer protection (FDP_UCT) 158
F.12.1 User notes 158
F.12.2 FDP_UCT.1 Basic data exchange confidentiality 159
F.13 Inter-TSF user data integrity transfer protection (FDP_UIT) 159
F.13.1 User notes 159
F.13.2 FDP_UIT.1 Data exchange integrity 159
F.13.3 FDP_UIT.2 Source data exchange recovery 160
F.13.4 FDP_UIT.3 Destination data exchange recovery 160

Annex G (normative) Class FIA: Identification and authentication 161
G.1 Authentication failures (FIA_AFL) 162
G.1.1 User notes 162
G.1.2 FIA_AFL.1 Authentication failure handling 163
G.2 User attribute definition (FIA_ATD) 164
G.2.1 User notes 164
G.2.2 FIA_ATD.1 User attribute definition 164
G.3 Specification of secrets (FIA_SOS) 164
G.3.1 User notes 164
G.3.2 FIA_SOS.1 Verification of secrets 165
G.3.3 FIA_SOS.2 TSF Generation of secrets 165
G.4 User authentication (FIA_UAU) 165
G.4.1 User notes 165
G.4.2 FIA_UAU.1 Timing of authentication 165
G.4.3 FIA_UAU.2 User authentication before any action 166
G.4.4 FIA_UAU.3 Unforgeable authentication 166
G.4.5 FIA_UAU.4 Single-use authentication mechanisms 166
G.4.6 FIA_UAU.5 Multiple authentication mechanisms 167
G.4.7 FIA_UAU.6 Re-authenticating 167
G.4.8 FIA_UAU.7 Protected authentication feedback 168
G.5 User identification (FIA_UID) 168
G.5.1 User notes 168
G.5.2 FIA_UID.1 Timing of identification 168
G.5.3 FIA_UID.2 User identification before any action 168
G.6 User-subject binding (FIA_USB) 169
G.6.1 User notes 169

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

G.6.2 FIA_USB.1 User-subject binding 169

Annex H (normative) Class FMT: Security management 170
H.1 Management of functions in TSF (FMT_MOF) 171
H.1.1 User notes 171
H.1.2 FMT_MOF.1 Management of security functions behaviour 172
H.2 Management of security attributes (FMT_MSA) 172
H.2.1 User notes 172
H.2.2 FMT_MSA.1 Management of security attributes 173
H.2.3 FMT_MSA.2 Secure security attributes 173
H.2.4 FMT_MSA.3 Static attribute initialisation 174
H.2.5 FMT_MSA.4 Security attribute value inheritance 174
H.3 Management of TSF data (FMT_MTD) 174
H.3.1 User notes 174
H.3.2 FMT_MTD.1 Management of TSF data 174
H.3.3 FMT_MTD.2 Management of limits on TSF data 175
H.3.4 FMT_MTD.3 Secure TSF data 175
H.4 Revocation (FMT_REV) 176
H.4.1 User notes 176
H.4.2 FMT_REV.1 Revocation 176
H.5 Security attribute expiration (FMT_SAE) 176
H.5.1 User notes 176
H.5.2 FMT_SAE.1 Time-limited authorisation 177
H.6 Specification of Management Functions (FMT_SMF) 177
H.6.1 User notes 177
H.6.2 FMT_SMF.1 Specification of Management Functions 177
H.7 Security management roles (FMT_SMR) 177
H.7.1 User notes 177
H.7.2 FMT_SMR.1 Security roles 178
H.7.3 FMT_SMR.2 Restrictions on security roles 178
H.7.4 FMT_SMR.3 Assuming roles 178

Annex I (normative) Class FPR: Privacy 179
I.1 Anonymity (FPR_ANO) 180
I.1.1 User notes 180
I.1.2 FPR_ANO.1 Anonymity 181
I.1.3 FPR_ANO.2 Anonymity without soliciting information 181
I.2 Pseudonymity (FPR_PSE) 182
I.2.1 User notes 182
I.2.2 FPR_PSE.1 Pseudonymity 183
I.2.3 FPR_PSE.2 Reversible pseudonymity 183
I.2.4 FPR_PSE.3 Alias pseudonymity 184
I.3 Unlinkability (FPR_UNL) 185
I.3.1 User notes 185
I.3.2 FPR_UNL.1 Unlinkability 186
I.4 Unobservability (FPR_UNO) 186
I.4.1 User notes 186
I.4.2 FPR_UNO.1 Unobservability 187
I.4.3 FPR_UNO.2 Allocation of information impacting unobservability 187
I.4.4 FPR_UNO.3 Unobservability without soliciting information 188
I.4.5 FPR_UNO.4 Authorised user observability 189

Annex J (normative) Class FPT: Protection of the TSF 190
J.1 Fail secure (FPT_FLS) 192
J.1.1 User notes 192
J.1.2 FPT_FLS.1 Failure with preservation of secure state 192
J.2 Availability of exported TSF data (FPT_ITA) 192
J.2.1 User notes 192
J.2.2 FPT_ITA.1 Inter-TSF availability within a defined availability metric 192
J.3 Confidentiality of exported TSF data (FPT_ITC) 193
J.3.1 User notes 193

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

J.3.2 FPT_ITC.1 Inter-TSF confidentiality during transmission 193
J.4 Integrity of exported TSF data (FPT_ITI) 193
J.4.1 User notes 193
J.4.2 FPT_ITI.1 Inter-TSF detection of modification 193
J.4.3 FPT_ITI.2 Inter-TSF detection and correction of modification 194
J.5 Internal TOE TSF data transfer (FPT_ITT) 194
J.5.1 User notes 194
J.5.2 Evaluator notes 194
J.5.3 FPT_ITT.1 Basic internal TSF data transfer protection 195
J.5.4 FPT_ITT.2 TSF data transfer separation 195
J.5.5 FPT_ITT.3 TSF data integrity monitoring 195
J.6 TSF physical protection (FPT_PHP) 195
J.6.1 User notes 195
J.6.2 FPT_PHP.1 Passive detection of physical attack 196
J.6.3 FPT_PHP.2 Notification of physical attack 196
J.6.4 FPT_PHP.3 Resistance to physical attack 196
J.7 Trusted recovery (FPT_RCV) 197
J.7.1 User notes 197
J.7.2 FPT_RCV.1 Manual recovery 198
J.7.3 FPT_RCV.2 Automated recovery 199
J.7.4 FPT_RCV.3 Automated recovery without undue loss 199
J.7.5 FPT_RCV.4 Function recovery 200
J.8 Replay detection (FPT_RPL) 200
J.8.1 User notes 200
J.8.2 FPT_RPL.1 Replay detection 200
J.9 State synchrony protocol (FPT_SSP) 201
J.9.1 User notes 201
J.9.2 FPT_SSP.1 Simple trusted acknowledgement 201
J.9.3 FPT_SSP.2 Mutual trusted acknowledgement 201
J.10 Time stamps (FPT_STM) 201
J.10.1 User notes 201
J.10.2 FPT_STM.1 Reliable time stamps 201
J.11 Inter-TSF TSF data consistency (FPT_TDC) 202
J.11.1 User notes 202
J.11.2 FPT_TDC.1 Inter-TSF basic TSF data consistency 202
J.12 Testing of external entities (FPT_TEE) 202
J.12.1 User notes 202
J.12.2 Evaluator notes 203
J.12.3 FPT_TEE.1 Testing of external entities 203
J.13 Internal TOE TSF data replication consistency (FPT_TRC) 204
J.13.1 User notes 204
J.13.2 FPT_TRC.1 Internal TSF consistency 204
J.14 TSF self test (FPT_TST) 204
J.14.1 User notes 204
J.14.2 FPT_TST.1 TSF testing 204

Annex K (normative) **Class FRU: Resource utilisation** 206
K.1 Fault tolerance (FRU_FLT) 206
K.1.1 User notes 206
K.1.2 FRU_FLT.1 Degraded fault tolerance 207
K.1.3 FRU_FLT.2 Limited fault tolerance 207
K.2 Priority of service (FRU_PRS) 207
K.2.1 User notes 207
K.2.2 FRU_PRS.1 Limited priority of service 208
K.2.3 FRU_PRS.2 Full priority of service 208
K.3 Resource allocation (FRU_RSA) 208
K.3.1 User notes 208
K.3.2 FRU_RSA.1 Maximum quotas 209
K.3.3 FRU_RSA.2 Minimum and maximum quotas 209

Annex L (normative) **Class FTA: TOE access** 211

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

L.1 Limitation on scope of selectable attributes (FTA_LSA) 211
L.1.1 User notes 211
L.1.2 FTA_LSA.1 Limitation on scope of selectable attributes 212
L.2 Limitation on multiple concurrent sessions (FTA_MCS) 212
L.2.1 User notes 212
L.2.2 FTA_MCS.1 Basic limitation on multiple concurrent sessions 212
L.2.3 FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions 212
L.3 Session locking and termination (FTA_SSL) 213
L.3.1 User notes 213
L.3.2 FTA_SSL.1 TSF-initiated session locking 213
L.3.3 FTA_SSL.2 User-initiated locking 214
L.3.4 FTA_SSL.3 TSF-initiated termination 214
L.3.5 FTA_SSL.4 User-initiated termination 214
L.4 TOE access banners (FTA_TAB) 214
L.4.1 User notes 214
L.4.2 FTA_TAB.1 Default TOE access banners 215
L.5 TOE access history (FTA_TAH) 215
L.5.1 User notes 215
L.5.2 FTA_TAH.1 TOE access history 215
L.6 TOE session establishment (FTA_TSE) 215
L.6.1 User notes 215
L.6.2 FTA_TSE.1 TOE session establishment 216

Annex M (normative) Class FTP: Trusted path/channels 217
M.1 Inter-TSF trusted channel (FTP_ITC) 217
M.1.1 User notes 217
M.1.2 FTP_ITC.1 Inter-TSF trusted channel 217
M.2 Trusted path (FTP_TRP) 218
M.2.1 User notes 218
M.2.2 FTP_TRP.1 Trusted path 218

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15408-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organisations as Common Criteria for Information Technology Security Evaluation. The common XML source for both publications can be found at http://www.oc.ccn.cni.es/xml

This third edition cancels and replaces the second edition (ISO/IEC 15408-2:2005), which has been technically revised.

ISO/IEC 15408 consists of the following parts, under the general title *Information technology — Security techniques — Evaluation criteria for IT security*:

— *Part 1: Introduction and general model*

— *Part 2: Security functional components*

— *Part 3: Security assurance components*

This corrected version of ISO/IEC 15408-2:2008 incorporates miscellaneous editorial corrections mainly related to FDP_UTC, FDP_UIT, FDP_ACF.1.4, FAU_SEL.1.1, FPT_TST.1, FDP_ITT.4, and FPT_TEE.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

Legal Notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations, version 3.1 Parts 1 through 3 (called CC 3.1), they hereby grant non-exclusive license to ISO/IEC to use CC 3.1 in the continued development/maintenance of the ISO/IEC 15408 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC 3.1 as they see fit.

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;
France:	Direction Centrale de la Sécurité des Systèmes d'Information;
Germany:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;
Netherlands:	Netherlands National Communications Security Agency;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

Introduction

Security functional components, as defined in this part of ISO/IEC 15408, are the basis for the security functional requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the IT or by the IT response to stimulus.

Security functional components express security requirements intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organisational security policies and assumptions.

The audience for this part of ISO/IEC 15408 includes consumers, developers, and evaluators of secure IT products. ISO/IEC 15408-1:2009, Clause 5 provides additional information on the target audience of ISO/IEC 15408, and on the use of ISO/IEC 15408 by the groups that comprise the target audience. These groups may use this part of ISO/IEC 5408 as follows:

a) Consumers, who use this part of ISO/IEC 15408 when selecting components to express functional requirements to satisfy the security objectives expressed in a PP or ST. ISO/IEC 15408-1:2009, Clause 6 provides more detailed information on the relationship between security objectives and security requirements.

b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, may find a standardised method to understand those requirements in this part of ISO/IEC 15408. They can also use the contents of this part of ISO/IEC 15408 as a basis for further defining the TOE security functionality and mechanisms that comply with those requirements.

c) Evaluators, who use the functional requirements defined in this part of ISO/IEC 15408 in verifying that the TOE functional requirements expressed in the PP or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators also should use this part of ISO/IEC 15408 to assist in determining whether a given TOE satisfies stated requirements.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

Information technology — Security techniques — Evaluation criteria for IT security —

Part 2:
Security functional components

1 Scope

This part of ISO/IEC 15408 defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms and definitions, symbols and abbreviated terms

For the purposes of this document, the terms, definitions, symbols and abbreviated terms given in ISO/IEC 15408-1 apply.

4 Overview

ISO/IEC 15408 and the associated security functional requirements described herein are not meant to be a definitive answer to all the problems of IT security. Rather, ISO/IEC 15408 offers a set of well understood security functional requirements that can be used to create trusted products reflecting the needs of the market. These security functional requirements are presented as the current state of the art in requirements specification and evaluation.

This part of ISO/IEC 15408 does not presume to include all possible security functional requirements but rather contains those that are known and agreed to be of value by this part of ISO/IEC 15408 authors at the time of release.

Since the understanding and needs of consumers may change, the functional requirements in this part of ISO/IEC 15408 will need to be maintained. It is envisioned that some PP/ST authors may have security needs not (yet) covered by the functional requirement components in this part of ISO/IEC 15408. In those cases the PP/ST author may choose to consider using functional requirements not taken from ISO/IEC 15408 (referred to as extensibility), as explained in Annexes A and B of ISO/IEC 15408-1:2009.

4.1 Organisation of this part of ISO/IEC 15408

Clause 5 describes the paradigm used in the security functional requirements of this part of ISO/IEC 15408.

Clause 6 introduces the catalogue of this part of ISO/IEC 15408 functional components while Clauses 7 through 17 describe the functional classes.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

Annex A provides explanatory information for potential users of the functional components including a complete cross reference table of the functional component dependencies.

Annex B through Annex M provide the explanatory information for the functional classes. This material must be seen as normative instructions on how to apply relevant operations and select appropriate audit or documentation information; the use of the auxiliary verb should means that the instruction is strongly preferred, but others may be justifiable. Where different options are given, the choice is left to the PP/ST author.

Those who author PPs or STs should refer to Clause 2 of ISO/IEC 15408-1:2009 for relevant structures, rules, and guidance:

a) ISO/IEC 15408-1:2009, Clause 3 defines the terms used in ISO/IEC 15408.

b) ISO/IEC 15408-1:2009, Annex A defines the structure for STs.

c) ISO/IEC 15408-1:2009, Annex B defines the structure for PPs.

5 Functional requirements paradigm

This clause describes the paradigm used in the security functional requirements of this part of ISO/IEC 15408. Key concepts discussed are highlighted in bold/italics. This subclause is not intended to replace or supersede any of the terms found in ISO/IEC 15408-1:2009, Clause 3.

This part of ISO/IEC 15408 is a catalogue of security functional components that can be specified for a **Target of Evaluation (TOE)**. A TOE is a set of software, firmware and/or hardware possibly accompanied by user and administrator guidance documentation. A TOE may contain resources such as electronic storage media (e.g. main memory, disk space), peripheral devices (e.g. printers), and computing capacity (e.g. CPU time) that can be used for processing and storing information and is the subject of an evaluation.

TOE evaluation is concerned primarily with ensuring that a defined set of **security functional requirements (SFRs)** is enforced over the TOE resources. The SFRs define the rules by which the TOE governs access to and use of its resources, and thus information and services controlled by the TOE.

The SFRs may define multiple **Security Function Policies** (SFPs) to represent the rules that the TOE must enforce. Each such SFP must specify its **scope of control**, by defining the subjects, objects, resources or information, and operations to which it applies. All SFPs are implemented by the TSF (see below), whose mechanisms enforce the rules defined in the SFRs and provide necessary capabilities.

Those portions of a TOE that must be relied on for the correct enforcement of the SFRs are collectively referred to as the **TOE Security Functionality (TSF)**. The TSF consists of all hardware, software, and firmware of a TOE that is either directly or indirectly relied upon for security enforcement.

The TOE may be a monolithic product containing hardware, firmware, and software.

Alternatively a TOE may be a distributed product that consists internally of multiple separated parts. Each of these parts of the TOE provides a particular service for the TOE, and is connected to the other parts of the TOE through an **internal communication channel**. This channel can be as small as a processor bus, or may encompass a network internal to the TOE.

When the TOE consists of multiple parts, each part of the TOE may have its own part of the TSF which exchanges user and TSF data over internal communication channels with other parts of the TSF. This interaction is called **internal TOE transfer**. In this case the separate parts of the TSF abstractly form the composite TSF, which enforces the SFRs.

TOE interfaces may be localised to the particular TOE, or they may allow interaction with other IT products over **external communication channels**. These external interactions with other IT products may take two forms:

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

a) The SFRs of the other “trusted IT product” and the SFRs of the TOE have been administratively coordinated and the other trusted IT product is assumed to enforce its SFRs correctly (e. g. by being separately evaluated). Exchanges of information in this situation are called **inter-TSF transfers**, as they are between the TSFs of distinct trusted products.

b) The other IT product may not be trusted, it may be called an “untrusted IT product”. Therefore its SFRs are either unknown or their implementation is not viewed as trustworthy. TSF mediated exchanges of information in this situation are called **transfers outside of the TOE**, as there is no TSF (or its policy characteristics are unknown) on the other IT product.

The set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which resources are accessed that are mediated by the TSF, or information is obtained from the TSF, is referred to as the **TSF Interface (TSFI)**. The TSFI defines the boundaries of the TOE functionality that provide for the enforcement of the SFRs.

Users are outside of the TOE. However, in order to request that services be performed by the TOE that are subject to rules defined in the SFRs, users interact with the TOE through the TSFIs. There are two types of users of interest to this part of ISO/IEC 15408: **human users** and **external IT entities**. Human users may further be differentiated as **local human users**, meaning they interact directly with the TOE via TOE devices (e.g. workstations), or **remote human users**, meaning they interact indirectly with the TOE through another IT product.

A period of interaction between users and the TSF is referred to as a user **session**. Establishment of user sessions can be controlled based on a variety of considerations, for example: user authentication, time of day, method of accessing the TOE, and number of allowed concurrent sessions (per user or in total).

This part of ISO/IEC 15408 uses the term **authorised** to signify a user who possesses the rights and/or privileges necessary to perform an operation. The term **authorised user**, therefore, indicates that it is allowable for a user to perform a specific operation or a set of operations as defined by the SFRs.

To express requirements that call for the separation of administrator duties, the relevant security functional components (from family FMT_SMR) explicitly state that administrative **roles** are required. A role is a pre-defined set of rules establishing the allowed interactions between a user operating in that role and the TOE. A TOE may support the definition of any number of roles. For example, roles related to the secure operation of a TOE may include “Audit Administrator” and “User Accounts Administrator”.

TOEs contain **resources** that may be used for the processing and storing of information. The primary goal of the TSF is the complete and correct enforcement of the SFRs over the resources and information that the TOE controls.

TOE resources can be structured and utilised in many different ways. However, this part of ISO/IEC 15408 makes a specific distinction that allows for the specification of desired security properties. All entities that can be created from resources can be characterised in one of two ways. The entities may be active, meaning that they are the cause of actions that occur internal to the TOE and cause operations to be performed on information. Alternatively, the entities may be passive, meaning that they are either the container from which information originates or to which information is stored.

Active entities in the TOE that perform operations on objects are referred to as **subjects**. Several types of subjects may exist within a TOE:

a) those acting on behalf of an authorised user (e.g. UNIX processes);

b) those acting as a specific functional process that may in turn act on behalf of multiple users (e.g. functions as might be found in client/server architectures); or

c) those acting as part of the TOE itself (e.g. processes not acting on behalf of a user).

This part of ISO/IEC 15408 addresses the enforcement of the SFRs over types of subjects as those listed above.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

Passive entities in the TOE that contain or receive information and upon which subjects perform operations are called **objects**. In the case where a subject (an active entity) is the target of an operation (e.g. interprocess communication), a subject may also be acted on as an object.

Objects can contain **information**. This concept is required to specify information flow control policies as addressed in the FDP class.

Users, subjects, information, objects, sessions and resources controlled by rules in the SFRs may possess certain **attributes** that contain information that is used by the TOE for its correct operation. Some attributes, such as file names, may be intended to be informational or may be used to identify individual resources while others, such as access control information, may exist specifically for the enforcement of the SFRs. These latter attributes are generally referred to as "**security attributes**". The word attribute will be used as a shorthand in some places of this part of ISO/IEC 15408 for the word "security attribute". However, no matter what the intended purpose of the attribute information, it may be necessary to have controls on attributes as dictated by the SFRs.

Data in a TOE is categorised as either user data or TSF data. Figure 1 depicts this relationship. **User Data** is information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning. For example, the content of an electronic mail message is user data. TSF Data is information used by the TSF in making decisions as required by the SFRs. **TSF Data** may be influenced by users if allowed by the SFRs. Security attributes, authentication data, TSF internal status variables used by the rules defined in the SFRs or used for the protection of the TSF and access control list entries are examples of TSF data.

There are several SFPs that apply to data protection such as **access control SFPs** and **information flow control SFPs**. The mechanisms that implement access control SFPs base their policy decisions on attributes of the users, resources, subjects, objects, sessions, TSF status data and operations within the scope of control. These attributes are used in the set of rules that govern operations that subjects may perform on objects.

The mechanisms that implement information flow control SFPs base their policy decisions on the attributes of the subjects and information within the scope of control and the set of rules that govern the operations by subjects on information. The attributes of the information, which may be associated with the attributes of the container or may be derived from the data in the container, stay with the information as it is processed by the TSF.

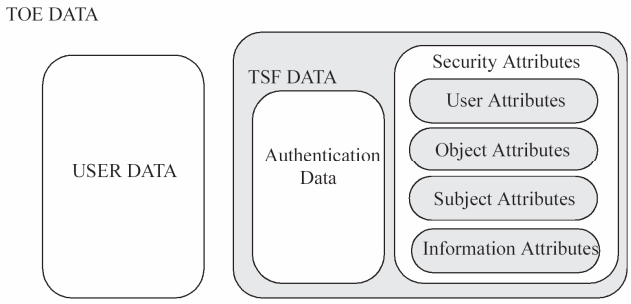

Figure 1 — Relationship between user data and TSF data

Two specific types of TSF data addressed by this part of ISO/IEC 15408 can be, but are not necessarily, the same. These are **authentication data** and **secrets**.

Authentication data is used to verify the claimed identity of a user requesting services from a TOE. The most common form of authentication data is the password, which depends on being kept secret in order to be an effective security mechanism. However, not all forms of authentication data need to be kept secret. Biometric authentication devices (e.g. fingerprint readers, retinal scanners) do not rely on the fact that the data is kept secret, but rather that the data is something that only one user possesses and that cannot be forged.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

The term secrets, as used in this part of ISO/IEC 15408, while applicable to authentication data, is intended to also be applicable to other types of data that must be kept secret in order to enforce a specific SFP. For example, a trusted channel mechanism that relies on cryptography to preserve the confidentiality of information being transmitted via the channel can only be as strong as the method used to keep the cryptographic keys secret from unauthorised disclosure.

Therefore, some, but not all, authentication data needs to be kept secret and some, but not all, secrets are used as authentication data. Figure 2 shows this relationship between secrets and authentication data. In the Figure the types of data typically encountered in the authentication data and the secrets subclauses are indicated.

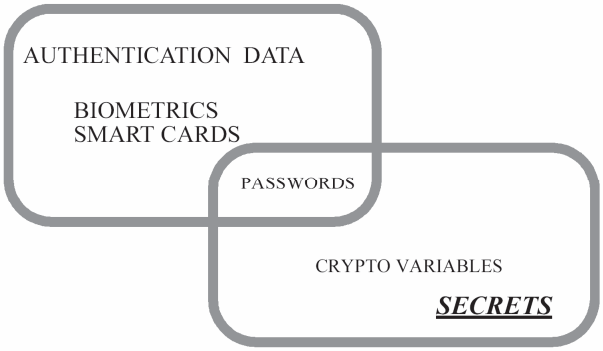

Figure 2 — Relationship between "authentication data" and "secrets"

6 Security functional components

6.1 Overview

This clause defines the content and presentation of the functional requirements of ISO/IEC 15408, and provides guidance on the organisation of the requirements for new components to be included in an ST. The functional requirements are expressed in classes, families, and components.

6.1.1 Class structure

Figure 3 illustrates the functional class structure in diagrammatic form. Each functional class includes a class name, class introduction, and one or more functional families.

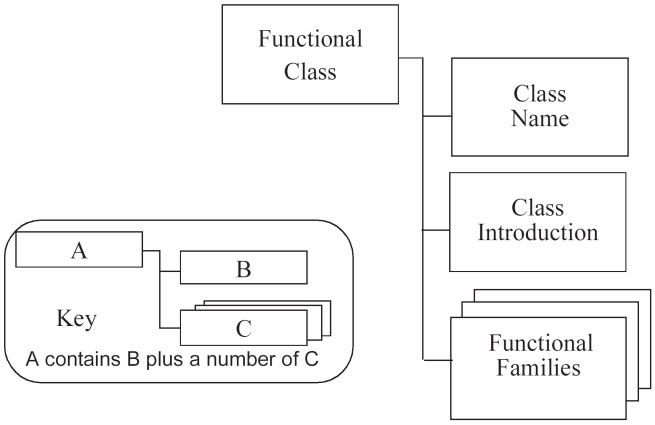

Figure 3 — Functional class structure

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

6.1.1.1 Class name

The class name subclause provides information necessary to identify and categorise a functional class. Every functional class has a unique name. The categorical information consists of a short name of three characters. The short name of the class is used in the specification of the short names of the families of that class.

6.1.1.2 Class introduction

The class introduction expresses the common intent or approach of those families to satisfy security objectives. The definition of functional classes does not reflect any formal taxonomy in the specification of the requirements.

The class introduction provides a figure describing the families in this class and the hierarchy of the components in each family, as explained in 6.2.

6.1.2 Family structure

Figure 4 illustrates the functional family structure in diagrammatic form.

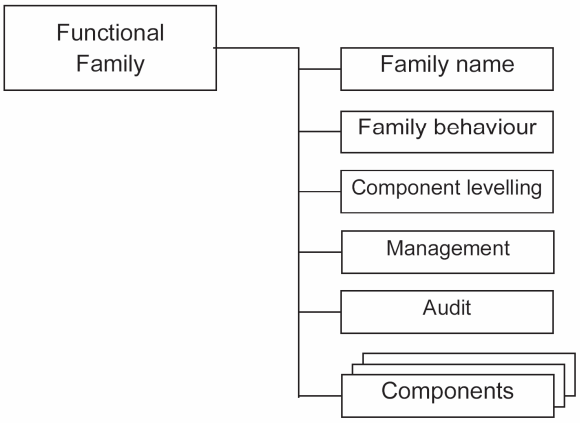

Figure 4 — Functional family structure

6.1.2.1 Family name

The family name subclause provides categorical and descriptive information necessary to identify and categorise a functional family. Every functional family has a unique name. The categorical information consists of a short name of seven characters, with the first three identical to the short name of the class followed by an underscore and the short name of the family as follows XXX_YYY. The unique short form of the family name provides the principal reference name for the components.

6.1.2.2 Family behaviour

The family behaviour is the narrative description of the functional family stating its security objective and a general description of the functional requirements. These are described in greater detail below:

a) The *security objectives* of the family address a security problem that may be solved with the help of a TOE that incorporates a component of this family;

b) The description of the *functional requirements* summarises all the requirements that are included in the component(s). The description is aimed at authors of PPs, STs and functional packages who wish to assess whether the family is relevant to their specific requirements.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

6.1.2.3 Component levelling

Functional families contain one or more components, any one of which can be selected for inclusion in PPs, STs and functional packages. The goal of this subclause is to provide information to users in selecting an appropriate functional component once the family has been identified as being a necessary or useful part of their security requirements.

This subclause of the functional family description describes the components available, and their rationale. The exact details of the components are contained within each component.

The relationships between components within a functional family may or may not be hierarchical. A component is hierarchical to another if it offers more security.

As explained in 6.2 the descriptions of the families provide a graphical overview of the hierarchy of the components in a family.

6.1.2.4 Management

The *management* clauses contain information for the PP/ST authors to consider as management activities for a given component. The clauses reference components of the management class (FMT), and provide guidance regarding potential management activities that may be applied via operations to those components.

A PP/ST author may select the indicated management components or may include other management requirements not listed to detail management activities. As such the information should be considered informative.

6.1.2.5 Audit

The *audit* requirements contain auditable events for the PP/ST authors to select, if requirements from the class FAU: Security audit, are included in the PP/ST. These requirements include security relevant events in terms of the various levels of detail supported by the components of the Security audit data generation (FAU_GEN) family. For example, an audit note might include actions that are in terms of: Minimal - successful use of the security mechanism; Basic - any use of the security mechanism as well as relevant information regarding the security attributes involved; Detailed - any configuration changes made to the mechanism, including the actual configuration values before and after the change.

It should be observed that the categorisation of auditable events is hierarchical. For example, when Basic Audit Generation is desired, all auditable events identified as being both Minimal and Basic should be included in the PP/ST through the use of the appropriate assignment operation, except when the higher level event simply provides more detail than the lower level event. When Detailed Audit Generation is desired, all identified auditable events (Minimal, Basic and Detailed) should be included in the PP/ST.

In the class FAU: Security audit the rules governing the audit are explained in more detail.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

6.1.3 Component structure

Figure 5 illustrates the functional component structure.

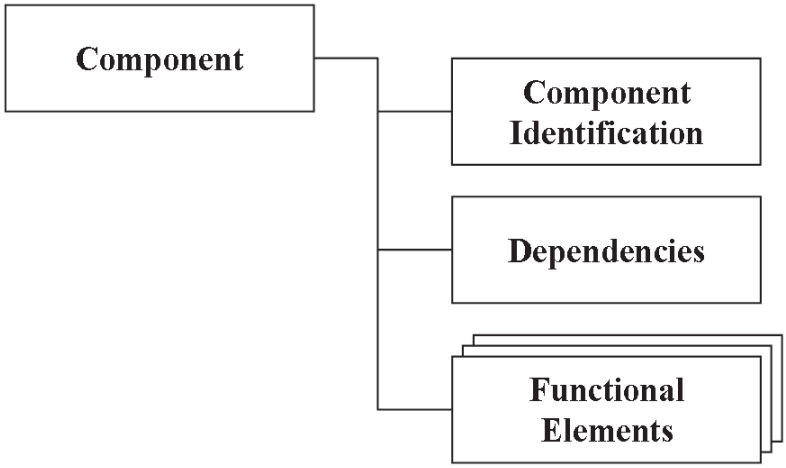

Figure 5 — Functional component structure

6.1.3.1 Component identification

The component identification subclause provides descriptive information necessary to identify, categorise, register and cross-reference a component. The following is provided as part of every functional component:

A *unique name*. The name reflects the purpose of the component.

A *short name*. A unique short form of the functional component name. This short name serves as the principal reference name for the categorisation, registration and cross-referencing of the component. This short name reflects the class and family to which the component belongs and the component number within the family.

A *hierarchical-to list*. A list of other components that this component is hierarchical to and for which this component can be used to satisfy dependencies to the listed components.

6.1.3.2 Functional elements

A set of elements is provided for each component. Each element is individually defined and is self-contained.

A functional element is a security functional requirement that if further divided would not yield a meaningful evaluation result. It is the smallest security functional requirement identified and recognised in ISO/IEC 15408.

When building packages, PPs and/or STs, it is not permitted to select only one or more elements from a component. The complete set of elements of a component must be selected for inclusion in a PP, ST or package.

A unique short form of the functional element name is provided. For example the requirement name FDP_IFF.4.2 reads as follows: F - functional requirement, DP - class “User data protection”, _IFF - family “Information flow control functions”, .4 - 4th component named “Partial elimination of illicit information flows”, .2 - 2nd element of the component.

6.1.3.3 Dependencies

Dependencies among functional components arise when a component is not self sufficient and relies upon the functionality of, or interaction with, another component for its own proper functioning.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

Each functional component provides a complete list of dependencies to other functional and assurance components. Some components may list “No dependencies”. The components depended upon may in turn have dependencies on other components. The list provided in the components will be the direct dependencies. That is only references to the functional requirements that are required for this requirement to perform its job properly. The indirect dependencies, that is the dependencies that result from the depended upon components can be found in Annex A of this part of ISO/IEC 15408. It is noted that in some cases the dependency is optional in that a number of functional requirements are provided, where each one of them would be sufficient to satisfy the dependency (see for example FDP_UIT.1 Data exchange integrity).

The dependency list identifies the minimum functional or assurance components needed to satisfy the security requirements associated with an identified component. Components that are hierarchical to the identified component may also be used to satisfy the dependency.

The dependencies indicated in this part of ISO/IEC 15408 are normative. They must be satisfied within a PP/ST. In specific situations the indicated dependencies might not be applicable. The PP/ST author, by providing the rationale why it is not applicable, may leave the depended upon component out of the package, PP or ST.

6.2 Component catalogue

The grouping of the components in this part of ISO/IEC 15408 does not reflect any formal taxonomy.

This part of ISO/IEC 15408 contains classes of families and components, which are rough groupings on the basis of related function or purpose, presented in alphabetic order. At the start of each class is an informative diagram that indicates the taxonomy of each class, indicating the families in each class and the components in each family. The diagram is a useful indicator of the hierarchical relationship that may exist between components.

In the description of the functional components, a subclause identifies the dependencies between the component and any other components.

In each class a figure describing the family hierarchy similar to Figure 6, is provided. In Figure 6 the first family, Family 1, contains three hierarchical components, where component 2 and component 3 can both be used to satisfy dependencies on component 1. Component 3 is hierarchical to component 2 and can also be used to satisfy dependencies on component 2.

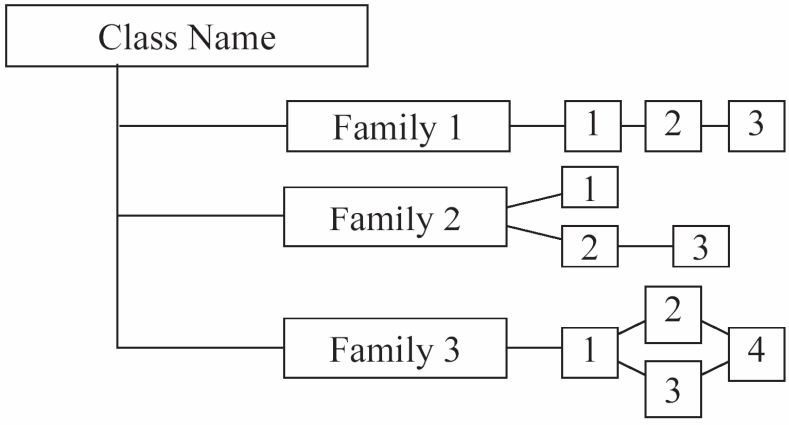

Figure 6 — Sample class decomposition diagram

In Family 2 there are three components not all of which are hierarchical. Components 1 and 2 are hierarchical to no other components. Component 3 is hierarchical to component 2, and can be used to satisfy dependencies on component 2, but not to satisfy dependencies on component 1.

In Family 3, components 2, 3, and 4 are hierarchical to component 1. Components 2 and 3 are both hierarchical to component 1, but non-comparable. Component 4 is hierarchical to both component 2 and component 3.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

These diagrams are meant to complement the text of the families and make identification of the relationships easier. They do not replace the “Hierarchical to:” note in each component that is the mandatory claim of hierarchy for each component.

6.2.1 Component changes highlighting

The relationship between components within a family is highlighted using a **bolding** convention. This bolding convention calls for the bolding of all new requirements. For hierarchical components, requirements are bolded when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using **bold** type.

7 Class FAU: Security audit

Security auditing involves recognising, recording, storing, and analysing information related to security relevant activities (i.e. activities controlled by the TSF). The resulting audit records can be examined to determine which security relevant activities took place and whom (which user) is responsible for them.

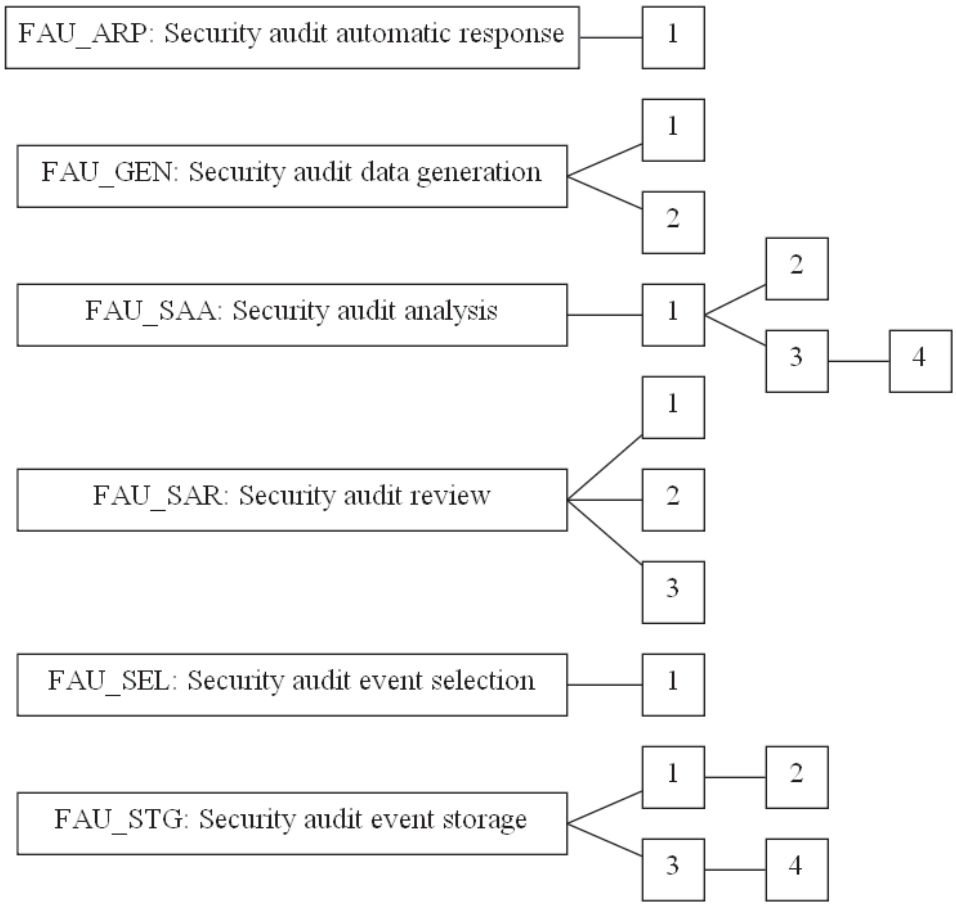

Figure 7 — FAU: Security audit class decomposition

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

7.1 Security audit automatic response (FAU_ARP)

7.1.1 Family Behaviour

This family defines the response to be taken in case of detected events indicative of a potential security violation.

7.1.2 Component levelling

At FAU_ARP.1 Security alarms, the TSF shall take actions in case a potential security violation is detected.

7.1.3 Management of FAU_ARP.1

The following actions could be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

7.1.4 Audit of FAU_ARP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Actions taken due to potential security violations.

7.1.5 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

7.1.5.1 FAU_ARP.1.1

The TSF shall take [assignment: *list of actions*] upon detection of a potential security violation.

7.2 Security audit data generation (FAU_GEN)

7.2.1 Family Behaviour

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

7.2.2 Component levelling

FAU_GEN.1 Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.

At FAU_GEN.2 User identity association, the TSF shall associate auditable events to individual user identities.

7.2.3 Management of FAU_GEN.1, FAU_GEN.2

There are no management activities foreseen.

7.2.4 Audit of FAU_GEN.1, FAU_GEN.2

There are no auditable events foreseen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

7.2.5 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

7.2.5.1 FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and

c) [assignment: *other specifically defined auditable events*].

7.2.5.2 FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

7.2.6 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

7.2.6.1 FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

7.3 Security audit analysis (FAU_SAA)

7.3.1 Family Behaviour

This family defines requirements for automated means that analyse system activity and audit data looking for possible or real security violations. This analysis may work in support of intrusion detection, or automatic response to a potential security violation.

The actions to be taken based on the detection can be specified using the Security audit automatic response (FAU_ARP) family as desired.

7.3.2 Component levelling

In FAU_SAA.1 Potential violation analysis, basic threshold detection on the basis of a fixed rule set is required.

In FAU_SAA.2 Profile based anomaly detection, the TSF maintains individual profiles of system usage, where a profile represents the historical patterns of usage performed by members of the profile target group. A profile target group refers to a group of one or more individuals (e.g. a single user, users who share a group ID or

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

group account, users who operate under an assigned role, users of an entire system or network node) who interact with the TSF. Each member of a profile target group is assigned an individual suspicion rating that represents how well that member's current activity corresponds to the established patterns of usage represented in the profile. This analysis can be performed at runtime or during a post-collection batch-mode analysis.

In FAU_SAA.3 Simple attack heuristics, the TSF shall be able to detect the occurrence of signature events that represent a significant threat to enforcement of the SFRs. This search for signature events may occur in real-time or during a post-collection batch-mode analysis.

In FAU_SAA.4 Complex attack heuristics, the TSF shall be able to represent and detect multi-step intrusion scenarios. The TSF is able to compare system events (possibly performed by multiple individuals) against event sequences known to represent entire intrusion scenarios. The TSF shall be able to indicate when a signature event or event sequence is found that indicates a potential violation of the enforcement of the SFRs.

7.3.3 Management of FAU_SAA.1

The following actions could be considered for the management functions in FMT:

a) maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.

7.3.4 Management of FAU_SAA.2

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users in the profile target group.

7.3.5 Management of FAU_SAA.3

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the subset of system events.

7.3.6 Management of FAU_SAA.4

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the subset of system events;

b) maintenance (deletion, modification, addition) of the set of sequence of system events.

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

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms;

b) Minimal: Automated responses performed by the tool.

7.3.8 FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

7.3.8.1 FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

7.3.8.2 FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;

b) [assignment: *any other rules*].

7.3.9 FAU_SAA.2 Profile based anomaly detection

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

7.3.9.1 FAU_SAA.2.1

The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: *the profile target group*].

7.3.9.2 FAU_SAA.2.2

The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.

7.3.9.3 FAU_SAA.2.3

The TSF shall be able to indicate a possible violation of the enforcement of the SFRs when a user's suspicion rating exceeds the following threshold conditions [assignment: *conditions under which anomalous activity is reported by the TSF*].

7.3.10 FAU_SAA.3 Simple attack heuristics

Hierarchical to: No other components.

Dependencies: No dependencies.

7.3.10.1 FAU_SAA.3.1

The TSF shall be able to maintain an internal representation of the following signature events [assignment: *a subset of system events*] that may indicate a violation of the enforcement of the SFRs.

7.3.10.2 FAU_SAA.3.2

The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].

7.3.10.3 FAU_SAA.3.3

The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when a system event is found to match a signature event that indicates a potential violation of the enforcement of the SFRs.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

7.3.11 FAU_SAA.4 Complex attack heuristics

Hierarchical to: FAU_SAA.3 Simple attack heuristics

Dependencies: No dependencies.

7.3.11.1 FAU_SAA.4.1

The TSF shall be able to maintain an internal representation of the following **event sequences of known intrusion scenarios [assignment: *list of sequences of system events whose occurrence are representative of known penetration scenarios*] and the following** signature events [assignment: *a subset of system events*] that may indicate a **potential** violation of the enforcement of the SFRs.

7.3.11.2 FAU_SAA.4.2

The TSF shall be able to compare the signature events **and event sequences** against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].

7.3.11.3 FAU_SAA.4.3

The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when system **activity** is found to match a signature event **or event sequence** that indicates a potential violation of the enforcement of the SFRs.

7.4 Security audit review (FAU_SAR)

7.4.1 Family Behaviour

This family defines the requirements for audit tools that should be available to authorised users to assist in the review of audit data.

7.4.2 Component levelling

FAU_SAR.1 Audit review, provides the capability to read information from the audit records.

FAU_SAR.2 Restricted audit review, requires that there are no other users except those that have been identified in FAU_SAR.1 Audit review that can read the information.

FAU_SAR.3 Selectable audit review, requires audit review tools to select the audit data to be reviewed based on criteria.

7.4.3 Management of FAU_SAR.1

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.

7.4.4 Management of FAU_SAR.2, FAU_SAR.3

There are no management activities foreseen.

7.4.5 Audit of FAU_SAR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Reading of information from the audit records.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

7.4.6 Audit of FAU_SAR.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Unsuccessful attempts to read information from the audit records.

7.4.7 Audit of FAU_SAR.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Detailed: the parameters used for the viewing.

7.4.8 FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

7.4.8.1 FAU_SAR.1.1

The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

7.4.8.2 FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

7.4.9 FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

7.4.9.1 FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

7.4.10 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

7.4.10.1 FAU_SAR.3.1

The TSF shall provide the ability to apply [assignment: *methods of selection and/or ordering*] of audit data based on [assignment: *criteria with logical relations*].

7.5 Security audit event selection (FAU_SEL)

7.5.1 Family Behaviour

This family defines requirements to select the set of events to be audited during TOE operation from the set of all auditable events.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

7.5.2 Component levelling

FAU_SEL.1 Selective audit, requires the ability to select the set of events to be audited from the set of all auditable events, identified in FAU_GEN.1 Audit data generation, based upon attributes to be specified by the PP/ST author.

7.5.3 Management of FAU_SEL.1

The following actions could be considered for the management functions in FMT:

a) maintenance of the rights to view/modify the audit events.

7.5.4 Audit of FAU_SEL.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: All modifications to the audit configuration that occur while the audit collection functions are operating.

7.5.5 FAU_SEL.1 Selective audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FMT_MTD.1 Management of TSF data

7.5.5.1 FAU_SEL.1.1

The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [selection: *object identity, user identity, subject identity, host identity, event type*]

b) [assignment: *list of additional attributes that audit selectivity is based upon*]

7.6 Security audit event storage (FAU_STG)

7.6.1 Family Behaviour

This family defines the requirements for the TSF to be able to create and maintain a secure audit trail. Stored audit records refers to those records within the audit trail, and not the audit records that have been retrieved (to temporary storage) through selection.

7.6.2 Component levelling

At FAU_STG.1 Protected audit trail storage, requirements are placed on the audit trail. It will be protected from unauthorised deletion and/or modification.

FAU_STG.2 Guarantees of audit data availability, specifies the guarantees that the TSF maintains over the audit data given the occurrence of an undesired condition.

FAU_STG.3 Action in case of possible audit data loss, specifies actions to be taken if a threshold on the audit trail is exceeded.

FAU_STG.4 Prevention of audit data loss, specifies actions in case the audit trail is full.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

7.6.3 Management of FAU_STG.1

There are no management activities foreseen.

7.6.4 Management of FAU_STG.2

The following actions could be considered for the management functions in FMT:

a) maintenance of the parameters that control the audit storage capability.

7.6.5 Management of FAU_STG.3

The following actions could be considered for the management functions in FMT:

a) maintenance of the threshold;

b) maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit storage failure.

7.6.6 Management of FAU_STG.4

The following actions could be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.

7.6.7 Audit of FAU_STG.1, FAU_STG.2

There are no auditable events foreseen.

7.6.8 Audit of FAU_STG.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Actions taken due to exceeding of a threshold.

7.6.9 Audit of FAU_STG.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Basic: Actions taken due to the audit storage failure.

7.6.10 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

7.6.10.1 FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

7.6.10.2 FAU_STG.1.2

The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

7.6.11 FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1 Protected audit trail storage

Dependencies: FAU_GEN.1 Audit data generation

7.6.11.1 FAU_STG.2.1

The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

7.6.11.2 FAU_STG.2.2

The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

7.6.11.3 FAU_STG.2.3

The TSF shall ensure that [assignment: *metric for saving audit records*] stored audit records will be maintained when the following conditions occur: [selection: *audit storage exhaustion, failure, attack*].

7.6.12 FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

7.6.12.1 FAU_STG.3.1

The TSF shall [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*].

7.6.13 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

7.6.13.1 FAU_STG.4.1

The TSF shall **[selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and** [assignment: ***other actions*** *to be taken in case of audit storage failure*] if the audit trail **is full.**

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

8 Class FCO: Communication

This class provides two families specifically concerned with assuring the identity of a party participating in a data exchange. These families are related to assuring the identity of the originator of transmitted information (proof of origin) and assuring the identity of the recipient of transmitted information (proof of receipt). These families ensure that an originator cannot deny having sent the message, nor can the recipient deny having received it.

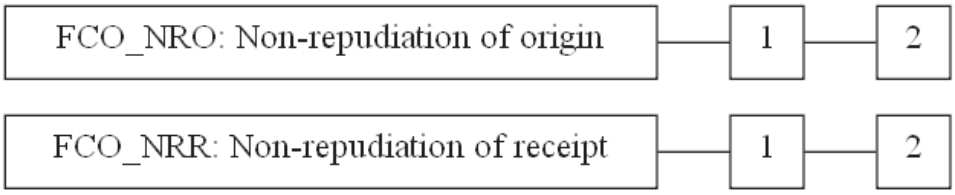

Figure 8 — FCO: Communication class decomposition

8.1 Non-repudiation of origin (FCO_NRO)

8.1.1 Family Behaviour

Non-repudiation of origin ensures that the originator of information cannot successfully deny having sent the information. This family requires that the TSF provide a method to ensure that a subject that receives information during a data exchange is provided with evidence of the origin of the information. This evidence can then be verified by either this subject or other subjects.

8.1.2 Component levelling

FCO_NRO.1 Selective proof of origin, requires the TSF to provide subjects with the capability to request evidence of the origin of information.

FCO_NRO.2 Enforced proof of origin, requires that the TSF always generate evidence of origin for transmitted information.

8.1.3 Management of FCO_NRO.1, FCO_NRO.2

The following actions could be considered for the management functions in FMT:

a) The management of changes to information types, fields, originator attributes and recipients of evidence.

8.1.4 Audit of FCO_NRO.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: The identity of the user who requested that evidence of origin would be generated.

b) Minimal: The invocation of the non-repudiation service.

c) Basic: Identification of the information, the destination, and a copy of the evidence provided.

d) Detailed: The identity of the user who requested a verification of the evidence.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

8.1.5 Audit of FCO_NRO.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: The invocation of the non-repudiation service.

b) Basic: Identification of the information, the destination, and a copy of the evidence provided.

c) Detailed: The identity of the user who requested a verification of the evidence.

8.1.6 FCO_NRO.1 Selective proof of origin

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

8.1.6.1 FCO_NRO.1.1

The TSF shall be able to generate evidence of origin for transmitted [assignment: *list of information types*] at the request of the [selection: *originator, recipient, [assignment: list of third parties]*].

8.1.6.2 FCO_NRO.1.2

The TSF shall be able to relate the [assignment: *list of attributes*] of the originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

8.1.6.3 FCO_NRO.1.3

The TSF shall provide a capability to verify the evidence of origin of information to [selection: *originator, recipient, [assignment: list of third parties]*] given [assignment: *limitations on the evidence of origin*].

8.1.7 FCO_NRO.2 Enforced proof of origin

Hierarchical to: FCO_NRO.1 Selective proof of origin

Dependencies: FIA_UID.1 Timing of identification

8.1.7.1 FCO_NRO.2.1

The TSF shall **enforce the generation of** evidence of origin for transmitted [assignment: *list of information types*] at **all times.**

8.1.7.2 FCO_NRO.2.2

The TSF shall be able to relate the [assignment: *list of attributes*] of the originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

8.1.7.3 FCO_NRO.2.3

The TSF shall provide a capability to verify the evidence of origin of information to [selection: *originator, recipient, [assignment: list of third parties]*] given [assignment: *limitations on the evidence of origin*].

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

8.2 Non-repudiation of receipt (FCO_NRR)

8.2.1 Family Behaviour

Non-repudiation of receipt ensures that the recipient of information cannot successfully deny receiving the information. This family requires that the TSF provide a method to ensure that a subject that transmits information during a data exchange is provided with evidence of receipt of the information. This evidence can then be verified by either this subject or other subjects.

8.2.2 Component levelling

FCO_NRR.1 Selective proof of receipt, requires the TSF to provide subjects with a capability to request evidence of the receipt of information.

FCO_NRR.2 Enforced proof of receipt, requires that the TSF always generate evidence of receipt for received information.

8.2.3 Management of FCO_NRR.1, FCO_NRR.2

The following actions could be considered for the management functions in FMT:

a) The management of changes to information types, fields, originator attributes and third parties recipients of evidence.

8.2.4 Audit of FCO_NRR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: The identity of the user who requested that evidence of receipt would be generated.

b) Minimal: The invocation of the non-repudiation service.

c) Basic: Identification of the information, the destination, and a copy of the evidence provided.

d) Detailed: The identity of the user who requested a verification of the evidence.

8.2.5 Audit of FCO_NRR.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: The invocation of the non-repudiation service.

b) Basic: Identification of the information, the destination, and a copy of the evidence provided.

c) Detailed: The identity of the user who requested a verification of the evidence.

8.2.6 FCO_NRR.1 Selective proof of receipt

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

8.2.6.1 FCO_NRR.1.1

The TSF shall be able to generate evidence of receipt for received [assignment: *list of information types*] at the request of the [selection: *originator, recipient, [assignment: list of third parties]*].

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

8.2.6.2 FCO_NRR.1.2

The TSF shall be able to relate the [assignment: *list of attributes*] of the recipient of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

8.2.6.3 FCO_NRR.1.3

The TSF shall provide a capability to verify the evidence of receipt of information to [selection: *originator, recipient, [assignment: list of third parties]*] given [assignment: *limitations on the evidence of receipt*].

8.2.7 FCO_NRR.2 Enforced proof of receipt

Hierarchical to: FCO_NRR.1 Selective proof of receipt

Dependencies: FIA_UID.1 Timing of identification

8.2.7.1 FCO_NRR.2.1

The TSF shall **enforce the generation of** evidence of receipt for received [assignment: *list of information types*] at **all times.**

8.2.7.2 FCO_NRR.2.2

The TSF shall be able to relate the [assignment: *list of attributes*] of the recipient of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

8.2.7.3 FCO_NRR.2.3

The TSF shall provide a capability to verify the evidence of receipt of information to [selection: *originator, recipient, [assignment: list of third parties]*] given [assignment: *limitations on the evidence of receipt*].

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

9 Class FCS: Cryptographic support

The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software.

The FCS: Cryptographic support class is composed of two families: Cryptographic key management (FCS_CKM) and Cryptographic operation (FCS_COP). The Cryptographic key management (FCS_CKM) family addresses the management aspects of cryptographic keys, while the Cryptographic operation (FCS_COP) family is concerned with the operational use of those cryptographic keys.

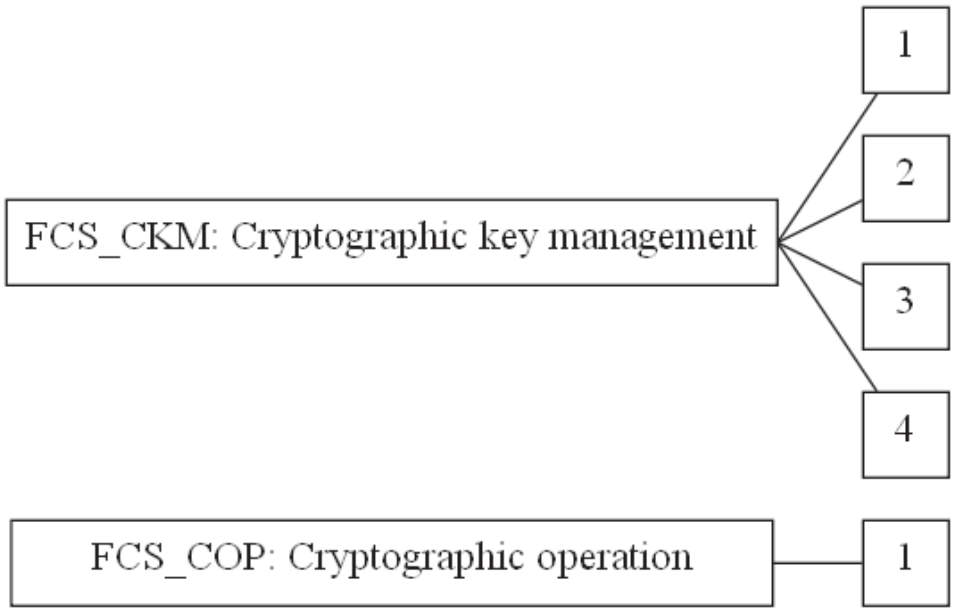

Figure 9 — FCS: Cryptographic support class decomposition

9.1 Cryptographic key management (FCS_CKM)

9.1.1 Family Behaviour

Cryptographic keys must be managed throughout their life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction. This family should be included whenever there are functional requirements for the management of cryptographic keys.

9.1.2 Component levelling

FCS_CKM.1 Cryptographic key generation, requires cryptographic keys to be generated in accordance with a specified algorithm and key sizes which can be based on an assigned standard.

FCS_CKM.2 Cryptographic key distribution, requires cryptographic keys to be distributed in accordance with a specified distribution method which can be based on an assigned standard.

FCS_CKM.3 Cryptographic key access, requires access to cryptographic keys to be performed in accordance with a specified access method which can be based on an assigned standard.

FCS_CKM.4 Cryptographic key destruction, requires cryptographic keys to be destroyed in accordance with a specified destruction method which can be based on an assigned standard.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

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

There are no management activities foreseen.

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

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure of the activity.

b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

9.1.5 FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

9.1.5.1 FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

9.1.6 FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

9.1.6.1 FCS_CKM.2.1

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method*] that meets the following: [assignment: *list of standards*].

9.1.7 FCS_CKM.3 Cryptographic key access

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

9.1.7.1 FCS_CKM.3.1

The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].

9.1.8 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

9.1.8.1 FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

9.2 Cryptographic operation (FCS_COP)

9.2.1 Family Behaviour

In order for a cryptographic operation to function correctly, the operation must be performed in accordance with a specified algorithm and with a cryptographic key of a specified size. This family should be included whenever there are requirements for cryptographic operations to be performed.

Typical cryptographic operations include data encryption and/or decryption, digital signature generation and/or verification, cryptographic checksum generation for integrity and/or verification of checksum, secure hash (message digest), cryptographic key encryption and/or decryption, and cryptographic key agreement.

9.2.2 Component levelling

FCS_COP.1 Cryptographic operation, requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

9.2.3 Management of FCS_COP.1

There are no management activities foreseen.

9.2.4 Audit of FCS_COP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Success and failure, and the type of cryptographic operation.

b) Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

9.2.5 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

9.2.5.1 FCS_COP.1.1

The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

10 Class FDP: User data protection

This class contains families specifying requirements related to protecting user data. FDP: User data protection is split into four groups of families (listed below) that address user data within a TOE, during import, export, and storage as well as security attributes directly related to user data.

The families in this class are organised into four groups:

a) User data protection security function policies:

- Access control policy (FDP_ACC); and
- Information flow control policy (FDP_IFC).

Components in these families permit the PP/ST author to name the user data protection security function policies and define the scope of control of the policy, necessary to address the security objectives. The names of these policies are meant to be used throughout the remainder of the functional components that have an operation that calls for an assignment or selection of an "access control SFP" or an "information flow control SFP". The rules that define the functionality of the named access control and information flow control SFPs will be defined in the Access control functions (FDP_ACF) and Information flow control functions (FDP_IFF) families (respectively).

b) Forms of user data protection:

- Access control functions (FDP_ACF);
- Information flow control functions (FDP_IFF);
- Internal TOE transfer (FDP_ITT);
- Residual information protection (FDP_RIP);
- Rollback (FDP_ROL); and
- Stored data integrity (FDP_SDI).

c) Off-line storage, import and export:

- Data authentication (FDP_DAU);

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

- Export from the TOE (FDP_ETC);
- Import from outside of the TOE (FDP_ITC).

Components in these families address the trustworthy transfer into or out of the TOE.

d) Inter-TSF communication:

- Inter-TSF user data confidentiality transfer protection (FDP_UCT); and
- Inter-TSF user data integrity transfer protection (FDP_UIT).

Components in these families address communication between the TSF of the TOE and another trusted IT product.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11

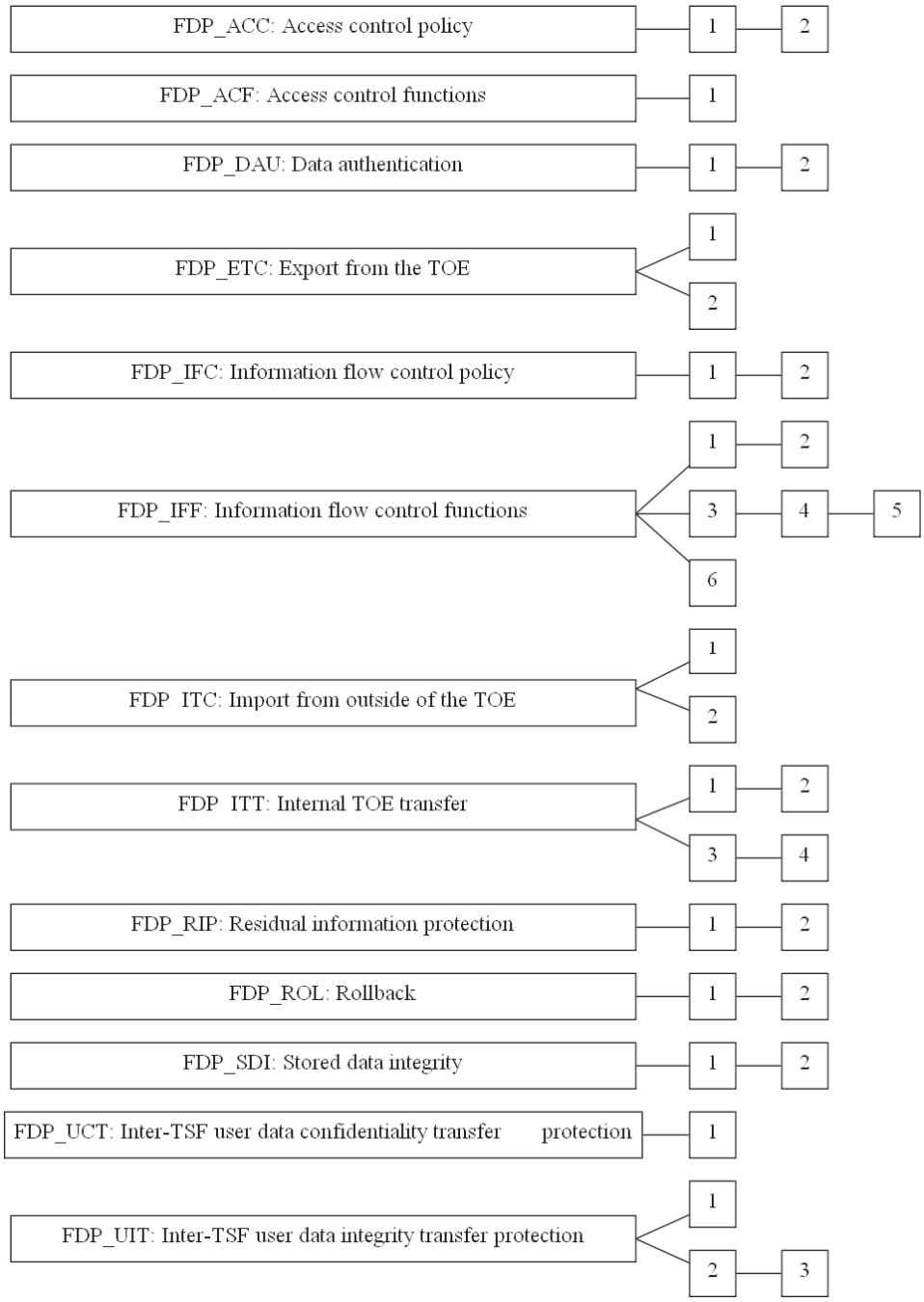

Figure 10 — FDP: User data protection class decomposition

10.1 Access control policy (FDP_ACC)

10.1.1 Family Behaviour

This family identifies the access control SFPs (by name) and defines the scope of control of the policies that form the identified access control portion of the SFRs related to the SFP. This scope of control is characterised by three sets: the subjects under control of the policy, the objects under control of the policy, and the operations among controlled subjects and controlled objects that are covered by the policy. The criteria allows multiple policies to exist, each having a unique name. This is accomplished by iterating components from this family once for each named access control policy. The rules that define the functionality of an access control SFP will be defined by other families such as Access control functions (FDP_ACF) and Export from the TOE (FDP_ETC). The names of the access control SFPs identified here in Access control

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-2:2019-11

policy (FDP_ACC) are meant to be used throughout the remainder of the functional components that have an operation that calls for an assignment or selection of an “access control SFP.”

10.1.2 Component levelling

FDP_ACC.1 Subset access control, requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE.

FDP_ACC.2 Complete access control, requires that each identified access control SFP cover all operations on subjects and objects covered by that SFP. It further requires that all objects and operations protected by the TSF are covered by at least one identified access control SFP.

10.1.3 Management of FDP_ACC.1, FDP_ACC.2

There are no management activities foreseen.

10.1.4 Audit of FDP_ACC.1, FDP_ACC.2

There are no auditable events foreseen.

10.1.5 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

10.1.5.1 FDP_ACC.1.1

The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

10.1.6 FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

10.1.6.1 FDP_ACC.2.1

The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and* ***objects***] **and all** operations among subjects and objects covered by the **SFP.**

10.1.6.2 FDP_ACC.2.2

The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

10.2 Access control functions (FDP_ACF)

10.2.1 Family Behaviour

This family describes the rules for the specific functions that can implement an access control policy named in Access control policy (FDP_ACC). Access control policy (FDP_ACC) specifies the scope of control of the policy.

10.2.2 Component levelling

This family addresses security attribute usage and characteristics of policies. The component within this family is meant to be used to describe the rules for the function that implements the SFP as identified in Access

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-2:2019-11