INTERNATIONAL STANDARD

ISO/IEC 15408-2

Fourth edition
2022-08

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 2: Security functional components

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information —

Partie 2: Composants fonctionnels de sécurité

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

Reference number
ISO/IEC 15408-2:2022(E)

© ISO/IEC 2022

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2022 – All rights reserved

Contents

Page

Foreword ..... **xv**
Introduction ..... **xvii**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **3**
5 Overview **4**
5.1 General 4
5.2 Organization of this document 4
6 Functional requirements paradigm **5**
7 Security functional components **9**
7.1 Overview 9
7.1.1 General 9
7.1.2 Class structure 9
7.1.3 Family structure 10
7.1.4 Component structure 11
7.2 Component catalogue 13
8 Class FAU: Security audit **14**
8.1 Class description 14
8.2 Security audit automatic response (FAU_ARP) 15
8.2.1 Family behaviour 15
8.2.2 Components leveling and description 15
8.2.3 Management of FAU_ARP.1 15
8.2.4 Audit of FAU_ARP.1 15
8.2.5 FAU_ARP.1 Security alarms 15
8.3 Security audit data generation (FAU_GEN) 15
8.3.1 Family behaviour 15
8.3.2 Components leveling and description 15
8.3.3 Management of FAU_GEN.1, FAU_GEN.2 16
8.3.4 Audit of FAU_GEN.1, FAU_GEN.2 16
8.3.5 FAU_GEN.1 Audit data generation 16
8.3.6 FAU_GEN.2 User identity association 16
8.4 Security audit analysis (FAU_SAA) 17
8.4.1 Family behaviour 17
8.4.2 Components leveling and description 17
8.4.3 Management of FAU_SAA.1 17
8.4.4 Management of FAU_SAA.2 18
8.4.5 Management of FAU_SAA.3 18
8.4.6 Management of FAU_SAA.4 18
8.4.7 Audit of FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4 18
8.4.8 FAU_SAA.1 Potential violation analysis 18
8.4.9 FAU_SAA.2 Profile based anomaly detection 18
8.4.10 FAU_SAA.3 Simple attack heuristics 19
8.4.11 FAU_SAA.4 Complex attack heuristics 19
8.5 Security audit review (FAU_SAR) 20
8.5.1 Family behaviour 20
8.5.2 Components leveling and description 20
8.5.3 Management of FAU_SAR.1 20
8.5.4 Management of FAU_SAR.2, FAU_SAR.3 20
8.5.5 Audit of FAU_SAR.1 20
8.5.6 Audit of FAU_SAR.2 21

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

8.5.7 Audit of FAU_SAR.3 ... 21
8.5.8 FAU_SAR.1 Audit review ... 21
8.5.9 FAU_SAR.2 Restricted audit review ... 21
8.5.10 FAU_SAR.3 Selectable audit review ... 21
8.6 Security audit event selection (FAU_SEL) ... 22
8.6.1 Family behaviour ... 22
8.6.2 Components leveling and description ... 22
8.6.3 Management of FAU_SEL.1 ... 22
8.6.4 Audit of FAU_SEL.1 ... 22
8.6.5 FAU_SEL.1 Selective audit ... 22
8.7 Security audit data storage (FAU_STG) ... 22
8.7.1 Family behaviour ... 22
8.7.2 Components leveling and description ... 23
8.7.3 Management of FAU_STG.1 ... 23
8.7.4 Management of FAU_STG.2 ... 23
8.7.5 Management of FAU_STG.3 ... 23
8.7.6 Management of FAU_STG.4 ... 23
8.7.7 Management of FAU_STG.5 ... 23
8.7.8 Audit of FAU_STG.1 ... 24
8.7.9 Audit of FAU_STG.2, FAU_STG.3 ... 24
8.7.10 Audit of FAU_STG.4 ... 24
8.7.11 Audit of FAU_STG.5 ... 24
8.7.12 FAU_STG.1 Audit data storage location ... 24
8.7.13 FAU_STG.2 Protected audit data storage ... 24
8.7.14 FAU_STG.3 Guarantees of audit data availability ... 25
8.7.15 FAU_STG.4 Action in case of possible audit data loss ... 25
8.7.16 FAU_STG.5 Prevention of audit data loss ... 25

9 Class FCO: Communication ... 25
9.1 Class description ... 25
9.2 Non-repudiation of origin (FCO_NRO) ... 26
9.2.1 Family behaviour ... 26
9.2.2 Components leveling and description ... 26
9.2.3 Management of FCO_NRO.1, FCO_NRO.2 ... 26
9.2.4 Audit of FCO_NRO.1 ... 26
9.2.5 Audit of FCO_NRO.2 ... 27
9.2.6 FCO_NRO.1 Selective proof of origin ... 27
9.2.7 FCO_NRO.2 Enforced proof of origin ... 27
9.3 Non-repudiation of receipt (FCO_NRR) ... 28
9.3.1 Family behaviour ... 28
9.3.2 Components leveling and description ... 28
9.3.3 Management of FCO_NRR.1, FCO_NRR.2 ... 28
9.3.4 Audit of FCO_NRR.1 ... 28
9.3.5 Audit of FCO_NRR.2 ... 28
9.3.6 FCO_NRR.1 Selective proof of receipt ... 29
9.3.7 FCO_NRR.2 Enforced proof of receipt ... 29

10 Class FCS: Cryptographic support ... 29
10.1 Class description ... 29
10.2 Cryptographic key management (FCS_CKM) ... 30
10.2.1 Family behaviour ... 30
10.2.2 Components leveling and description ... 30
10.2.3 Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6 ... 31
10.2.4 Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6 ... 31
10.2.5 FCS_CKM.1 Cryptographic key generation ... 31
10.2.6 FCS_CKM.2 Cryptographic key distribution ... 32
10.2.7 FCS_CKM.3 Cryptographic key access ... 32
10.2.8 FCS_CKM.4 Cryptographic key destruction ... 32
10.2.9 FCS_CKM.5 Cryptographic key derivation ... 33

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

10.2.10 FCS_CKM.6 Timing and event of cryptographic key destruction ... 33
10.3 Cryptographic operation (FCS_COP) ... 33
10.3.1 Family behaviour ... 33
10.3.2 Components leveling and description ... 33
10.3.3 Management of FCS_COP.1 ... 34
10.3.4 Audit of FCS_COP.1 ... 34
10.3.5 FCS_COP.1 Cryptographic operation ... 34
10.4 Random bit generation (FCS_RBG) ... 34
10.4.1 Family behaviour ... 34
10.4.2 Components leveling and description ... 34
10.4.3 Management of FCS_RBG.1, FCS_RBG.2, FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6 ... 35
10.4.4 Audit of FCS_RBG.1, FCS_RBG.2 ... 35
10.4.5 Audit of FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6 ... 35
10.4.6 FCS_RBG.1 Random bit generation (RBG) ... 35
10.4.7 FCS_RBG.2 Random bit generation (external seeding) ... 36
10.4.8 FCS_RBG.3 Random bit generation (internal seeding – single source) ... 36
10.4.9 FCS_RBG.4 Random bit generation (internal seeding – multiple sources) ... 37
10.4.10 FCS_RBG.5 Random bit generation (combining noise sources) ... 37
10.4.11 FCS_RBG.6 Random bit generation service ... 37
10.5 Generation of random numbers (FCS_RNG) ... 37
10.5.1 Family behaviour ... 37
10.5.2 Components leveling and description ... 38
10.5.3 Management of FCS_RNG.1 ... 38
10.5.4 Audit of FCS_RNG.1 ... 38
10.5.5 FCS_RNG.1 Random number generation ... 38

11 Class FDP: User data protection ... 38
11.1 Class description ... 38
11.2 Access control policy (FDP_ACC) ... 40
11.2.1 Family behaviour ... 40
11.2.2 Components leveling and description ... 41
11.2.3 Management of FDP_ACC.1, FDP_ACC.2 ... 41
11.2.4 Audit of FDP_ACC.1, FDP_ACC.2 ... 41
11.2.5 FDP_ACC.1 Subset access control ... 41
11.2.6 FDP_ACC.2 Complete access control ... 41
11.3 Access control functions (FDP_ACF) ... 42
11.3.1 Family behaviour ... 42
11.3.2 Components leveling and description ... 42
11.3.3 Management of FDP_ACF.1 ... 42
11.3.4 Audit of FDP_ACF.1 ... 42
11.3.5 FDP_ACF.1 Security attribute-based access control ... 42
11.4 Data authentication (FDP_DAU) ... 43
11.4.1 Family behaviour ... 43
11.4.2 Components leveling and description ... 43
11.4.3 Management of FDP_DAU.1, FDP_DAU.2 ... 43
11.4.4 Audit of FDP_DAU.1 ... 43
11.4.5 Audit of FDP_DAU.2 ... 44
11.4.6 FDP_DAU.1 Basic Data Authentication ... 44
11.4.7 FDP_DAU.2 Data Authentication with Identity of Guarantor ... 44
11.5 Export from the TOE (FDP_ETC) ... 44
11.5.1 Family behaviour ... 44
11.5.2 Components leveling and description ... 45
11.5.3 Management of FDP_ETC.1 ... 45
11.5.4 Management of FDP_ETC.2 ... 45
11.5.5 Audit of FDP_ETC.1, FDP_ETC.2 ... 45
11.5.6 FDP_ETC.1 Export of user data without security attributes ... 45
11.5.7 FDP_ETC.2 Export of user data with security attributes ... 45
11.6 Information flow control policy (FDP_IFC) ... 46

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

11.6.1 Family behaviour 46
11.6.2 Components leveling and description 46
11.6.3 Management of FDP_IFC.1, FDP_IFC.2 47
11.6.4 Audit of FDP_IFC.1, FDP_IFC.2 47
11.6.5 FDP_IFC.1 Subset information flow control 47
11.6.6 FDP_IFC.2 Complete information flow control 47
11.7 Information flow control functions (FDP_IFF) 47
11.7.1 Family behaviour 47
11.7.2 Components leveling and description 48
11.7.3 Management of FDP_IFF.1, FDP_IFF.2 48
11.7.4 Management of FDP_IFF.3, FDP_IFF.4, FDP_IFF.5 48
11.7.5 Management of FDP_IFF.6 49
11.7.6 Audit of FDP_IFF.1, FDP_IFF.2, FDP_IFF.5 49
11.7.7 Audit of FDP_IFF.3, FDP_IFF.4, FDP_IFF.6 49
11.7.8 FDP_IFF.1 Simple security attributes 49
11.7.9 FDP_IFF.2 Hierarchical security attributes 50
11.7.10 FDP_IFF.3 Limited illicit information flows 51
11.7.11 FDP_IFF.4 Partial elimination of illicit information flows 51
11.7.12 FDP_IFF.5 No illicit information flows 51
11.7.13 FDP_IFF.6 Illicit information flow monitoring 51
11.8 Information Retention Control (FDP_IRC) 52
11.8.1 Family behaviour 52
11.8.2 Components leveling and description 52
11.8.3 Management of FDP_IRC.1 53
11.8.4 Audit of FDP_IRC.1 53
11.8.5 FDP_IRC.1 Information retention control 53
11.9 Import from outside of the TOE (FDP_ITC) 53
11.9.1 Family behaviour 53
11.9.2 Components leveling and description 53
11.9.3 Management of FDP_ITC.1, FDP_ITC.2 54
11.9.4 Audit of FDP_ITC.1, FDP_ITC.2 54
11.9.5 FDP_ITC.1 Import of user data without security attributes 54
11.9.6 FDP_ITC.2 Import of user data with security attributes 54
11.10 Internal TOE transfer (FDP_ITT) 55
11.10.1 Family behaviour 55
11.10.2 Components leveling and description 55
11.10.3 Management of FDP_ITT.1, FDP_ITT.2 55
11.10.4 Management of FDP_ITT.3, FDP_ITT.4 56
11.10.5 Audit of FDP_ITT.1, FDP_ITT.2 56
11.10.6 Audit of FDP_ITT.3, FDP_ITT.4 56
11.10.7 FDP_ITT.1 Basic internal transfer protection 56
11.10.8 FDP_ITT.2 Transmission separation by attribute 56
11.10.9 FDP_ITT.3 Integrity monitoring 57
11.10.10 FDP_ITT.4 Attribute-based integrity monitoring 57
11.11 Residual information protection (FDP_RIP) 57
11.11.1 Family behaviour 57
11.11.2 Components leveling and description 58
11.11.3 Management of FDP_RIP.1, FDP_RIP.2 58
11.11.4 Audit of FDP_RIP.1, FDP_RIP.2 58
11.11.5 FDP_RIP.1 Subset residual information protection 58
11.11.6 FDP_RIP.2 Full residual information protection 58
11.12 Rollback (FDP_ROL) 59
11.12.1 Family behaviour 59
11.12.2 Components leveling and description 59
11.12.3 Management of FDP_ROL.1, FDP_ROL.2 59
11.12.4 Audit of FDP_ROL.1, FDP_ROL.2 59
11.12.5 FDP_ROL.1 Basic rollback 59

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

11.12.6 FDP_ROL.2 Advanced rollback 60
11.13 Stored data confidentiality (FDP_SDC) 60
11.13.1 Family behaviour 60
11.13.2 Components leveling and description 60
11.13.3 Management of FDP_SDC.1, FDP_SDC.2 60
11.13.4 Audit of FDP_SDC.1, FDP_SDC.2 61
11.13.5 FDP_SDC.1 Stored data confidentiality 61
11.13.6 FDP_SDC.2 Stored data confidentiality with dedicated method 61
11.14 Stored data integrity (FDP_SDI) 61
11.14.1 Family behaviour 61
11.14.2 Components leveling and description 61
11.14.3 Management of FDP_SDI.1 62
11.14.4 Management of FDP_SDI.2 62
11.14.5 Audit of FDP_SDI.1 62
11.14.6 Audit of FDP_SDI.2 62
11.14.7 FDP_SDI.1 Stored data integrity monitoring 62
11.14.8 FDP_SDI.2 Stored data integrity monitoring and action 62
11.15 Inter-TSF user data confidentiality transfer protection (FDP_UCT) 63
11.15.1 Family behaviour 63
11.15.2 Components leveling and description 63
11.15.3 Management of FDP_UCT.1 63
11.15.4 Audit of FDP_UCT.1 63
11.15.5 FDP_UCT.1 Basic data exchange confidentiality 63
11.16 Inter-TSF user data integrity transfer protection (FDP_UIT) 64
11.16.1 Family behaviour 64
11.16.2 Components leveling and description 64
11.16.3 Management of FDP_UIT.1, FDP_UIT.2, FDP_UIT.3 64
11.16.4 Audit of FDP_UIT.1 64
11.16.5 Audit of FDP_UIT.2, FDP_UIT.3 65
11.16.6 FDP_UIT.1 Data exchange integrity 65
11.16.7 FDP_UIT.2 Source data exchange recovery 65
11.16.8 FDP_UIT.3 Destination data exchange recovery 66

12 Class FIA: Identification and authentication 66
12.1 Class description 66
12.2 Authentication failures (FIA_AFL) 67
12.2.1 Family behaviour 67
12.2.2 Components leveling and description 67
12.2.3 Management of FIA_AFL.1 68
12.2.4 Audit of FIA_AFL.1 68
12.2.5 FIA_AFL.1 Authentication failure handling 68
12.3 Authentication proof of identity (FIA_API) 68
12.3.1 Family behaviour 68
12.3.2 Components leveling and description 68
12.3.3 Management of FIA_API.1 68
12.3.4 Audit of FIA_API.1 69
12.3.5 FIA_API.1 Authentication proof of identity 69
12.4 User attribute definition (FIA_ATD) 69
12.4.1 Family behaviour 69
12.4.2 Components leveling and description 69
12.4.3 Management of FIA_ATD.1 69
12.4.4 Audit of FIA_ATD.1 69
12.4.5 FIA_ATD.1 User attribute definition 69
12.5 Specification of secrets (FIA_SOS) 70
12.5.1 Family behaviour 70
12.5.2 Components leveling and description 70
12.5.3 Management of FIA_SOS.1 70
12.5.4 Management of FIA_SOS.2 70
12.5.5 Audit of FIA_SOS.1, FIA_SOS.2 70

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

12.5.6 FIA_SOS.1 Verification of secrets 70
12.5.7 FIA_SOS.2 TSF Generation of secrets 71
12.6 User authentication (FIA_UAU) 71
12.6.1 Family behaviour 71
12.6.2 Components leveling and description 71
12.6.3 Management of FIA_UAU.1 72
12.6.4 Management of FIA_UAU.2 72
12.6.5 Management of FIA_UAU.3, FIA_UAU.4, FIA_UAU.7 72
12.6.6 Management of FIA_UAU.5 72
12.6.7 Management of FIA_UAU.6 72
12.6.8 Management of FIA_UAU.7 72
12.6.9 Audit of FIA_UAU.1 72
12.6.10 Audit of FIA_UAU.2 73
12.6.11 Audit of FIA_UAU.3 73
12.6.12 Audit of FIA_UAU.4 73
12.6.13 Audit of FIA_UAU.5 73
12.6.14 Audit of FIA_UAU.6 73
12.6.15 Audit of FIA_UAU.7 73
12.6.16 FIA_UAU.1 Timing of authentication 73
12.6.17 FIA_UAU.2 User authentication before any action 74
12.6.18 FIA_UAU.3 Unforgeable authentication 74
12.6.19 FIA_UAU.4 Single-use authentication mechanisms 74
12.6.20 FIA_UAU.5 Multiple authentication mechanisms 74
12.6.21 FIA_UAU.6 Re-authenticating 75
12.6.22 FIA_UAU.7 Protected authentication feedback 75
12.7 User identification (FIA_UID) 75
12.7.1 Family behaviour 75
12.7.2 Components leveling and description 75
12.7.3 Management of FIA_UID.1 76
12.7.4 Management of FIA_UID.2 76
12.7.5 Audit of FIA_UID.1, FIA_UID.2 76
12.7.6 FIA_UID.1 Timing of identification 76
12.7.7 FIA_UID.2 User identification before any action 76
12.8 User-subject binding (FIA_USB) 77
12.8.1 Family behaviour 77
12.8.2 Components leveling and description 77
12.8.3 Management of FIA_USB.1 77
12.8.4 Audit of FIA_USB.1 77
12.8.5 FIA_USB.1 User-subject binding 77

13 Class FMT: Security management 78
13.1 Class description 78
13.2 Limited capabilities and availability (FMT_LIM) 79
13.2.1 Family behaviour 79
13.2.2 Components leveling and description 79
13.2.3 Management of FMT_LIM.1, FMT_LIM.2 80
13.2.4 Audit of FMT_LIM.1 80
13.2.5 FMT_LIM.1 Limited capabilities 80
13.2.6 FMT_LIM.2 Limited availability 80
13.3 Management of functions in TSF (FMT_MOF) 80
13.3.1 Family behaviour 80
13.3.2 Components leveling and description 80
13.3.3 Management of FMT_MOF.1 81
13.3.4 Audit of FMT_MOF.1 81
13.3.5 FMT_MOF.1 Management of security functions behaviour 81
13.4 Management of security attributes (FMT_MSA) 81
13.4.1 Family behaviour 81
13.4.2 Components leveling and description 81
13.4.3 Management of FMT_MSA.1 82

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

13.4.4 Management of FMT_MSA.2 ... 82
13.4.5 Management of FMT_MSA.3 ... 82
13.4.6 Management of FMT_MSA.4 ... 82
13.4.7 Audit of FMT_MSA.1 ... 82
13.4.8 Audit of FMT_MSA.2 ... 82
13.4.9 Audit of FMT_MSA.3 ... 82
13.4.10 Audit of FMT_MSA.4 ... 83
13.4.11 FMT_MSA.1 Management of security attributes ... 83
13.4.12 FMT_MSA.2 Secure security attributes ... 83
13.4.13 FMT_MSA.3 Static attribute initialization ... 83
13.4.14 FMT_MSA.4 Security attribute value inheritance ... 84
13.5 Management of TSF data (FMT_MTD) ... 84
13.5.1 Family behaviour ... 84
13.5.2 Components leveling and description ... 84
13.5.3 Management of FMT_MTD.1 ... 84
13.5.4 Management of FMT_MTD.2 ... 84
13.5.5 Management of FMT_MTD.3 ... 85
13.5.6 Audit of FMT_MTD.1 ... 85
13.5.7 Audit of FMT_MTD.2 ... 85
13.5.8 Audit of FMT_MTD.3 ... 85
13.5.9 FMT_MTD.1 Management of TSF data ... 85
13.5.10 FMT_MTD.2 Management of limits on TSF data ... 85
13.5.11 FMT_MTD.3 Secure TSF data ... 86
13.6 Revocation (FMT_REV) ... 86
13.6.1 Family behaviour ... 86
13.6.2 Components leveling and description ... 86
13.6.3 Management of FMT_REV.1 ... 86
13.6.4 Audit of FMT_REV.1 ... 86
13.6.5 FMT_REV.1 Revocation ... 86
13.7 Security attribute expiration (FMT_SAE) ... 87
13.7.1 Family behaviour ... 87
13.7.2 Components leveling and description ... 87
13.7.3 Management of FMT_SAE.1 ... 87
13.7.4 Audit of FMT_SAE.1 ... 87
13.7.5 FMT_SAE.1 Time-limited authorization ... 87
13.8 Specification of Management Functions (FMT_SMF) ... 88
13.8.1 Family behaviour ... 88
13.8.2 Components leveling and description ... 88
13.8.3 Management of FMT_SMF.1 ... 88
13.8.4 Audit of FMT_SMF.1 ... 88
13.8.5 FMT_SMF.1 Specification of Management Functions ... 88
13.9 Security management roles (FMT_SMR) ... 89
13.9.1 Family behaviour ... 89
13.9.2 Components leveling and description ... 89
13.9.3 Management of FMT_SMR.1 ... 89
13.9.4 Management of FMT_SMR.2 ... 89
13.9.5 Management of FMT_SMR.3 ... 89
13.9.6 Audit of FMT_SMR.1 ... 89
13.9.7 Audit of FMT_SMR.2 ... 89
13.9.8 Audit of FMT_SMR.3 ... 90
13.9.9 FMT_SMR.1 Security roles ... 90
13.9.10 FMT_SMR.2 Restrictions on security roles ... 90
13.9.11 FMT_SMR.3 Assuming roles ... 90

14 Class FPR: Privacy ... 91
14.1 Class description ... 91
14.2 Anonymity (FPR_ANO) ... 91
14.2.1 Family behaviour ... 91
14.2.2 Components leveling and description ... 91

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

14.2.3 Management of FPR_ANO.1, FPR_ANO.2 92
14.2.4 Audit of FPR_ANO.1, FPR_ANO.2 92
14.2.5 FPR_ANO.1 Anonymity 92
14.2.6 FPR_ANO.2 Anonymity without soliciting information 92
14.3 Pseudonymity (FPR_PSE) 92
14.3.1 Family behaviour 92
14.3.2 Components leveling and description 92
14.3.3 Management of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 93
14.3.4 Audit of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 93
14.3.5 FPR_PSE.1 Pseudonymity 93
14.3.6 FPR_PSE.2 Reversible pseudonymity 93
14.3.7 FPR_PSE.3 Alias pseudonymity 94
14.4 Unlinkability (FPR_UNL) 94
14.4.1 Family behaviour 94
14.4.2 Components leveling and description 94
14.4.3 Management of FPR_UNL.1 95
14.4.4 Audit of FPR_UNL.1 95
14.4.5 FPR_UNL.1 Unlinkability of operations 95
14.5 Unobservability (FPR_UNO) 95
14.5.1 Family behaviour 95
14.5.2 Components leveling and description 95
14.5.3 Management of FPR_UNO.1, FPR_UNO.2 96
14.5.4 Management of FPR_UNO.3 96
14.5.5 Management of FPR_UNO.4 96
14.5.6 Audit of FPR_UNO.1, FPR_UNO.2 96
14.5.7 Audit of FPR_UNO.3 96
14.5.8 Audit of FPR_UNO.4 96
14.5.9 FPR_UNO.1 Unobservability 97
14.5.10 FPR_UNO.2 Allocation of information impacting unobservability 97
14.5.11 FPR_UNO.3 Unobservability without soliciting information 97
14.5.12 FPR_UNO.4 Authorized user observability 97

15 Class FPT: Protection of the TSF 98
15.1 Class description 98
15.2 TOE emanation (FPT_EMS) 100
15.2.1 Family behaviour 100
15.2.2 Components leveling and description 101
15.2.3 Management of FPT_EMS.1 101
15.2.4 Audit of FPT_EMS.1 101
15.2.5 FPT_EMS.1 Emanation of TSF and User data 101
15.3 Fail secure (FPT_FLS) 101
15.3.1 Family behaviour 101
15.3.2 Components leveling and description 102
15.3.3 Management of FPT_FLS.1 102
15.3.4 Audit of FPT_FLS.1 102
15.3.5 FPT_FLS.1 Failure with preservation of secure state 102
15.4 TSF initialization (FPT_INI) 102
15.4.1 Family behaviour 102
15.4.2 Components leveling and description 102
15.4.3 Management of FPT_INI.1 103
15.4.4 Audit of FPT_INI.1 103
15.4.5 FPT_INI.1 TSF initialization 103
15.5 Availability of exported TSF data (FPT_ITA) 103
15.5.1 Family behaviour 103
15.5.2 Components leveling and description 103
15.5.3 Management of FPT_ITA.1 104
15.5.4 Audit of FPT_ITA.1 104
15.5.5 FPT_ITA.1 Inter-TSF availability within a defined availability metric 104
15.6 Confidentiality of exported TSF data (FPT_ITC) 104

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.6.1 Family behaviour 104
15.6.2 Components leveling and description 104
15.6.3 Management of FPT_ITC.1 105
15.6.4 Audit of FPT_ITC.1 105
15.6.5 FPT_ITC.1 Inter-TSF confidentiality during transmission 105
15.7 Integrity of exported TSF data (FPT_ITI) 105
15.7.1 Family behaviour 105
15.7.2 Components leveling and description 105
15.7.3 Management of FPT_ITI.1 105
15.7.4 Management of FPT_ITI.2 106
15.7.5 Audit of FPT_ITI.1 106
15.7.6 Audit of FPT_ITI.2 106
15.7.7 FPT_ITI.1 Inter-TSF detection of modification 106
15.7.8 FPT_ITI.2 Inter-TSF detection and correction of modification 106
15.8 Internal TOE TSF data transfer (FPT_ITT) 107
15.8.1 Family behaviour 107
15.8.2 Components leveling and description 107
15.8.3 Management of FPT_ITT.1 107
15.8.4 Management of FPT_ITT.2 107
15.8.5 Management of FPT_ITT.3 108
15.8.6 Audit of FPT_ITT.1, FPT_ITT.2 108
15.8.7 Audit of FPT_ITT.3 108
15.8.8 FPT_ITT.1 Basic internal TSF data transfer protection 108
15.8.9 FPT_ITT.2 TSF data transfer separation 108
15.8.10 FPT_ITT.3 TSF data integrity monitoring 109
15.9 TSF physical protection (FPT_PHP) 109
15.9.1 Family behaviour 109
15.9.2 Components leveling and description 109
15.9.3 Management of FPT_PHP.1 110
15.9.4 Management of FPT_PHP.2 110
15.9.5 Management of FPT_PHP.3 110
15.9.6 Audit of FPT_PHP.1 110
15.9.7 Audit of FPT_PHP.2 110
15.9.8 Audit of FPT_PHP.3 110
15.9.9 FPT_PHP.1 Passive detection of physical attack 110
15.9.10 FPT_PHP.2 Notification of physical attack 111
15.9.11 FPT_PHP.3 Resistance to physical attack 111
15.10 Trusted recovery (FPT_RCV) 111
15.10.1 Family behaviour 111
15.10.2 Components leveling and description 111
15.10.3 Management of FPT_RCV.1 112
15.10.4 Management of FPT_RCV.2, FPT_RCV.3 112
15.10.5 Management of FPT_RCV.4 112
15.10.6 Audit of FPT_RCV.1, FPT_RCV.2, FPT_RCV.3 112
15.10.7 Audit of FPT_RCV.4 112
15.10.8 FPT_RCV.1 Manual recovery 112
15.10.9 FPT_RCV.2 Automated recovery 113
15.10.10 FPT_RCV.3 Automated recovery without undue loss 113
15.10.11 FPT_RCV.4 Function recovery 113
15.11 Replay detection (FPT_RPL) 114
15.11.1 Family behaviour 114
15.11.2 Components leveling and description 114
15.11.3 Management of FPT_RPL.1 114
15.11.4 Audit of FPT_RPL.1 114
15.11.5 FPT_RPL.1 Replay detection 114
15.12 State synchrony protocol (FPT_SSP) 115

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.12.1 Family behaviour 115
15.12.2 Components leveling and description 115
15.12.3 Management of FPT_SSP.1, FPT_SSP.2 115
15.12.4 Audit of FPT_SSP.1, FPT_SSP.2 115
15.12.5 FPT_SSP.1 Simple trusted acknowledgement 115
15.12.6 FPT_SSP.2 Mutual trusted acknowledgement 115
15.13 Time stamps (FPT_STM) 116
15.13.1 Family behaviour 116
15.13.2 Components leveling and description 116
15.13.3 Management of FPT_STM.1 116
15.13.4 Management of FPT_STM.2 116
15.13.5 Audit of FPT_STM.1 116
15.13.6 Audit of FPT_STM.2 116
15.13.7 FPT_STM.1 Reliable time stamps 117
15.13.8 FPT_STM.2 Time source 117
15.14 Inter-TSF TSF data consistency (FPT_TDC) 117
15.14.1 Family behaviour 117
15.14.2 Components leveling and description 117
15.14.3 Management of FPT_TDC.1 117
15.14.4 Audit of FPT_TDC.1 118
15.14.5 FPT_TDC.1 Inter-TSF basic TSF data consistency 118
15.15 Testing of external entities (FPT_TEE) 118
15.15.1 Family behaviour 118
15.15.2 Components leveling and description 118
15.15.3 Management of FPT_TEE.1 118
15.15.4 Audit of FPT_TEE.1 119
15.15.5 FPT_TEE.1 Testing of external entities 119
15.16 Internal TOE TSF data replication consistency (FPT_TRC) 119
15.16.1 Family behaviour 119
15.16.2 Components leveling and description 119
15.16.3 Management of FPT_TRC.1 119
15.16.4 Audit of FPT_TRC.1 120
15.16.5 FPT_TRC.1 Internal TSF consistency 120
15.17 TSF self-test (FPT_TST) 120
15.17.1 Family behaviour 120
15.17.2 Components leveling and description 120
15.17.3 Management of FPT_TST.1 121
15.17.4 Audit of FPT_TST.1 121
15.17.5 FPT_TST.1 TSF self-testing 121

16 Class FRU: Resource utilization 121
16.1 Class description 121
16.2 Fault tolerance (FRU_FLT) 122
16.2.1 Family behaviour 122
16.2.2 Components leveling and description 122
16.2.3 Management of FRU_FLT.1, FRU_FLT.2 122
16.2.4 Audit of FRU_FLT.1 122
16.2.5 Audit of FRU_FLT.2 122
16.2.6 FRU_FLT.1 Degraded fault tolerance 123
16.2.7 FRU_FLT.2 Limited fault tolerance 123
16.3 Priority of service (FRU_PRS) 123
16.3.1 Family behaviour 123
16.3.2 Components leveling and description 123
16.3.3 Management of FRU_PRS.1, FRU_PRS.2 123
16.3.4 Audit of FRU_PRS.1, FRU_PRS.2 124
16.3.5 FRU_PRS.1 Limited priority of service 124
16.3.6 FRU_PRS.2 Full priority of service 124
16.4 Resource allocation (FRU_RSA) 124
16.4.1 Family behaviour 124

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

16.4.2 Components leveling and description 124
16.4.3 Management of FRU_RSA.1 125
16.4.4 Management of FRU_RSA.2 125
16.4.5 Audit of FRU_RSA.1, FRU_RSA.2 125
16.4.6 FRU_RSA.1 Maximum quotas 125
16.4.7 FRU_RSA.2 Minimum and maximum quotas 125

17 Class FTA: TOE access 126
17.1 Class description 126
17.2 Limitation on scope of selectable attributes (FTA_LSA) 126
17.2.1 Family behaviour 126
17.2.2 Components leveling and description 126
17.2.3 Management of FTA_LSA.1 127
17.2.4 Audit of FTA_LSA.1 127
17.2.5 FTA_LSA.1 Limitation on scope of selectable attributes 127
17.3 Limitation on multiple concurrent sessions (FTA_MCS) 127
17.3.1 Family behaviour 127
17.3.2 Components leveling and description 127
17.3.3 Management of FTA_MCS.1 128
17.3.4 Management of FTA_MCS.2 128
17.3.5 Audit of FTA_MCS.1, FTA_MCS.2 128
17.3.6 FTA_MCS.1 Basic limitation on multiple concurrent sessions 128
17.3.7 FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions 128
17.4 Session locking and termination (FTA_SSL) 129
17.4.1 Family behaviour 129
17.4.2 Components leveling and description 129
17.4.3 Management of FTA_SSL.1 129
17.4.4 Management of FTA_SSL.2 129
17.4.5 Management of FTA_SSL.3 129
17.4.6 Management of FTA_SSL.4 130
17.4.7 Audit of FTA_SSL.1, FTA_SSL.2 130
17.4.8 Audit of FTA_SSL.3 130
17.4.9 Audit of FTA_SSL.4 130
17.4.10 FTA_SSL.1 TSF-initiated session locking 130
17.4.11 FTA_SSL.2 User-initiated locking 130
17.4.12 FTA_SSL.3 TSF-initiated termination 131
17.4.13 FTA_SSL.4 User-initiated termination 131
17.5 TOE access banners (FTA_TAB) 131
17.5.1 Family behaviour 131
17.5.2 Components leveling and description 131
17.5.3 Management of FTA_TAB.1 131
17.5.4 Audit of FTA_TAB.1 132
17.5.5 FTA_TAB.1 Default TOE access banners 132
17.6 TOE access history (FTA_TAH) 132
17.6.1 Family behaviour 132
17.6.2 Components leveling and description 132
17.6.3 Management of FTA_TAH.1 132
17.6.4 Audit of FTA_TAH.1 132
17.6.5 FTA_TAH.1 TOE access history 132
17.7 TOE session establishment (FTA_TSE) 133
17.7.1 Family behaviour 133
17.7.2 Components leveling and description 133
17.7.3 Management of FTA_TSE.1 133
17.7.4 Audit of FTA_TSE.1 133
17.7.5 FTA_TSE.1 TOE session establishment 133

18 Class FTP: Trusted path/channels 134
18.1 Class description 134
18.2 Inter-TSF trusted channel (FTP_ITC) 135

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

18.2.1 Family behaviour 135
18.2.2 Components leveling and description 135
18.2.3 Management of FTP_ITC.1 135
18.2.4 Audit of FTP_ITC.1 135
18.2.5 FTP_ITC.1 Inter-TSF trusted channel 135
18.3 Trusted channel protocol (FTP_PRO) 136
18.3.1 Family behavior 136
18.3.2 Components leveling and description 136
18.3.3 Management of FTP_PRO.1 136
18.3.4 Management of FTP_PRO.2 136
18.3.5 Management of FTP_PRO.3 136
18.3.6 Audit of FTP_PRO.1 137
18.3.7 Audit of FTP_PRO.2 137
18.3.8 Audit of FTP_PRO.3 137
18.3.9 FTP_PRO.1 Trusted channel protocol 137
18.3.10 FTP_PRO.2 Trusted channel establishment 138
18.3.11 FTP_PRO.3 Trusted channel data protection 138
18.4 Trusted path (FTP_TRP) 139
18.4.1 Family behaviour 139
18.4.2 Components leveling and description 139
18.4.3 Management of FTP_TRP.1 139
18.4.4 Audit of FTP_TRP.1 139
18.4.5 FTP_TRP.1 Trusted path 139

Annex A (informative) **Security functional requirements (SFRs) structure of the application notes** **141**

Annex B (informative) **Dependency tables for security functional components** **144**

Annex C (normative) **Class FAU: Security audit — Application notes** **153**

Annex D (normative) **Class FCO: Communication — Application notes** **166**

Annex E (normative) **Class FCS: Cryptographic support — Application notes** **171**

Annex F (normative) **Class FDP: User data protection — Application notes** **181**

Annex G (normative) **Class FIA: Identification and authentication — Application notes** **208**

Annex H (normative) **Class FMT: Security management — Application notes** **218**

Annex I (normative) **Class FPR: Privacy — Application notes** **228**

Annex J (normative) **Class FPT: Protection of the TSF — Application notes** **240**

Annex K (normative) **Class FRU: Resource utilization — Application notes** **258**

Annex L (normative) **Class FTA: TOE access — Application notes** **263**

Annex M (normative) **Class FTP: Trusted path/channels- application notes** **269**

Bibliography **273**

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO 15408-2:2008), which has been technically revised.

The main changes are as follows:

— new security functional components have been introduced.

A list of all parts in the ISO/IEC 15408 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

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 (called CC), they hereby grant non-exclusive license to ISO/IEC to use CC in the continued development/maintenance of the ISO/IEC 15408 series of standards. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC as they see fit.

Australia	The Australian Signals Directorate
Canada	Communications Security Establishment
France	Agence Nationale 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
New Zealand	Government Communications Security Bureau
Republic of Korea	National Security Research Institute
Spain	Ministerio de Asuntos Económicos y Transformación Digital
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Introduction

Security functional components, as defined in this document, are the basis for the security functional requirements (SFRs) or components expressed in a Protection Profile (PP), PP-Module, functional package 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, PP-Module, functional package 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 allow for the expression of SFRs intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organizational security policies.

The audience for this document includes consumers, developers, and evaluators of secure IT products. ISO/IEC 15408-1:2022, 5.2, provides additional information on the target audience of the ISO/IEC 15408 series, and on the use of the ISO/IEC 15408 series by the groups that comprise the target audience. These groups use this document as follows:

a) consumers, who use this document when selecting components to express functional requirements which satisfy the security objectives expressed in a PP, PP-Module, functional package or ST. ISO/IEC 15408-1:20—, Clause 7, 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, will find a standardized method to understand those requirements in this document. They also use the contents of this document as a basis for further defining the TOE security functionality and mechanisms that conform with those requirements;

c) evaluators, who use the SFRs defined in this document in verifying that the TOE functional requirements expressed in the PP, PP-Module, functional package or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators use this document to assist in determining whether a given TOE satisfies stated requirements.

NOTE This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type 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.

The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 2: Security functional components

1 Scope

This document defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that meets the common security functionality requirements of many IT products.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 15408-1:2022, *Information security, cybersecurity and privacy protection— Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-3, *Information security, cybersecurity and privacy protection— Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information security, cybersecurity and privacy protection— Evaluation criteria for IT security — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, the terms, definitions, and abbreviated terms given in ISO/IEC 15408-1, ISO/IEC 15408-3, ISO/IEC 18045 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
identity
representation uniquely identifying an entity within the context of the target of evaluation (TOE)

EXAMPLE An example of such a representation is a string.

Note 1 to entry: Entities can be diverse such as a user, process, or disk. For a human user, the representation can be the full or abbreviated name or a unique pseudonym.

Note 2 to entry: An entity can have more than one identity.

3.2
inter TSF transfer
communication between the target of evaluation (TOE) and the security functionality of other trusted IT products

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

3.3
internal communication channel
communication channel between separated parts of the target of evaluation (TOE)

3.4
internal TOE transfer
communicating data between separated parts of the target of evaluation (TOE)

3.5
operation
⟨on an ISO/IEC 15408-2 component⟩ modification or repetition of a component by assignment, iteration, refinement, or selection

3.6
secret
information that is known only to authorized users and/or the TOE security functionality (TSF) in order to enforce a specific *security function policy (SFP)* (3.8)

3.7
secure state
state in which the TOE security functionality (TSF) data are consistent and the TSF continues correct enforcement of the security functional requirements (SFRs)

3.8
security function policy
SFP
set of rules describing specific security behaviour enforced by the TOE security functionality (TSF) and expressible as a set of security functional requirements (SFRs)

3.9
TOE resource
anything usable or consumable in the target of evaluation (TOE)

3.10
transfer outside of the TOE
target of evaluation (TOE) security functionality (TSF)-mediated communication of data to entities not under the control of the TSF

3.11
trusted channel
means by which a target of evaluation (TOE) security functionality (TSF) and another trusted IT product can communicate with necessary confidence

3.12
trusted path
means by which a user and a target of evaluation (TOE) security functionality (TSF) can communicate with the necessary confidence

Note 1 to entry: Communication typically implies the establishment of identification and authentication of both parties, as well as the concept of a user specific session which is integrity-protected.

Note 2 to entry: When the external entity is a trusted IT product, the notion of *trusted channel* (3.11) is used instead of trusted path.

Note 3 to entry: Both physical and logical aspects of secure communication can be considered as mechanisms for gaining confidence.

3.13
TSF data
data for the *operation* (3.5) of the target of evalution (TOE) upon which the enforcement of the security functional requirement (SFR) relies

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

3.14
user data
data received or produced by the target of evaluation (TOE), which is meaningful to some external entity, but which do not affect the *operation* (3.5) of the TOE security funtionality (TSF)

Note 1 to entry: Depending on the concept, this definition assumes that the same data created by users that has an actual impact on the operation of the TSF can be regarded as the *TSF data* (3.13).

4 Abbreviated terms

API	application programming interface
CD	compact disk
DAC	discretionary access control
DRBG	deterministic random bit generator
EMS	electromagnetic spectrum
GB	gigabyte
GHz	gigahertz
GUI	graphical user interface
HSM	hardware security module
HTTPS	hypertext transfer protocol secure
IOCTL	input output control
IP	internet protocol
IPsec	IP security (protocol)
LDAP	lightweight directory access protocol
MAC	mandatory access control
MB	megabyte
MBps	megabytes per second
OS	operating system
OTP	one-time programmable
PC	personal computer
PCI	peripheral component interconnect
PKI	public key infrastructure
PP	protection profile
RAM	random access memory
RBG	random bit generator
RNG	random number generator

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

RPC	remote procedure call
SFP	security function policy
SFR	security functional requirement
SSH	secure shell
ST	security target
TCP	transmission control protocol
TLS	transport layer security
TOE	target of evaluation
TSF	TOE security functionality
TSFI	TSF interface
USB	universal serial bus
VPN	virtual private network

5 Overview

5.1 General

The ISO/IEC 15408 series and the associated security functional requirements (SFRs) described in this document are not intended to be a definitive answer to all the problems of IT security. This document offers a set of well understood security functional components that can be used to specify trusted products reflecting the needs of the market. These security functional components are presented as the current state of the art in security requirements specification.

This document does not include all possible security functional components but contains those that are known and agreed to be of value by the contributors to this document.

Since the understanding and needs of consumers can change, the functional components in this document will need to be maintained. It is envisioned that some authors of PPs, PP-Modules, functional packages and STs can have security needs not covered by the security functional components in this document. In those cases, the author of a PP, PP-Module, functional package or ST may choose to consider using functional components and requirements that are not given in this document. The concepts of extensibility are explained in ISO/IEC 15408-1:2022, 8.4.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

5.2 Organization of this document

Clause 5 describes the paradigm used in the SFRs of this document.

Clause 7 introduces the catalogue of functional components, while Clauses 8 through 18 describe the functional classes.

Annex A provides explanatory information for potential users of the functional components.

Annex B provides a complete cross reference table of the functional component dependencies.

Annexes C through M provide the explanatory information for the functional classes. This material shall be seen as normative instructions on how to apply relevant operations and select appropriate audit or documentation information. Where different options are given, the choice is left to the PP, PP-Module, functional package and ST author.

© ISO/IEC 2022 – All rights reserved

Those who author PPs, PP-Modules, functional packages, or STs shall refer to ISO/IEC 15408-1:2022 for relevant structures, rules, and guidance, in particular:

a) ISO/IEC 15408-1:2022, Clause 3 defines the terms and definitions used in the ISO/IEC 15408 series;

b) ISO/IEC 15408-1:2022, Clause 7 describes how SFRs can be specified using the security functional components;

c) ISO/IEC 15408-1:2022, Clause 8 describes how security functional components are organized, and the operations that may be applied to them;

d) ISO/IEC 15408-1:2022, Annex A provides further information on the structure for security functional packages;

e) ISO/IEC 15408-1:2022, Annex B provides further information on the structure for PPs;

f) ISO/IEC 15408-1:2022, Annex C provides further information on the structure of PP-Modules and PP-Configurations;

g) ISO/IEC 15408-1:2022, Annex D provides further information on the structure for STs.

6 Functional requirements paradigm

This clause describes the paradigm used in the security functional components and the derivation of SFRs.

This document is a catalogue of security functional components that may be used for the specification of SFRs describing a TOE.

TOE evaluation is concerned primarily with ensuring that a defined set of 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 enforces. Each SFP specifies its scope of control, by defining the subjects, objects, resources or information, and operations to which it applies. All SFPs are implemented by the TOE Security Functionality (TSF) (see below), whose mechanisms enforce the rules defined in the SFRs and provide necessary capabilities.

Those portions of a TOE that are relied upon for the correct enforcement of the SFRs are collectively referred to as the 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 localized 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:

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

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 either 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 (API)], 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 document: 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 or remote human users, meaning they interact indirectly with the TOE through another IT product.

EXAMPLE 1

An example of a TOE device is a workstation.

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.

EXAMPLE 2

User authentication, time of day, method of accessing the TOE, and number of allowed concurrent sessions (per user or in total).

This document uses the term authorized to signify a user who possesses either the rights or privileges, or both that are necessary to perform an operation. The term authorized 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.

EXAMPLE 3

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 utilized in many different ways. However, this document makes a specific distinction that allows for the specification of desired security properties. All entities that can be created from resources can be characterized 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 authorized user;

EXAMPLE 4 UNIX processes.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

b) those acting as a specific functional process that may in turn act on behalf of multiple users;

EXAMPLE 5 Functions as can be found in client/server architectures.

c) those acting as part of the TOE itself.

EXAMPLE 6 Processes not acting on behalf of a user.

This document addresses the enforcement of the SFRs over types of subjects as those listed above.

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, a subject may also be acted on as an object.

EXAMPLE 7 An example of a subject is an inter-process communication.

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, can 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 in this document for the term "security attribute". However, no matter what the intended purpose of the attribute information, it can be necessary to have controls on attributes as dictated by the SFRs.

Data in a TOE is categorized 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. 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.

EXAMPLE 8

User data:

— The content of an electronic mail message can be user data.

TSF data:

— 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

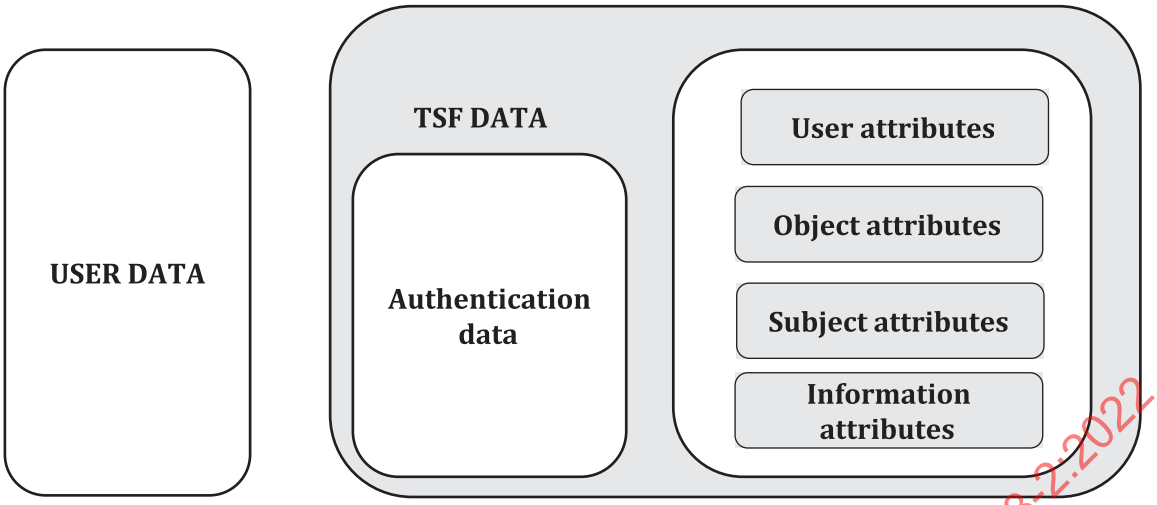


Figure 1 — Relationship between user data and TSF data

Two specific types of TSF data addressed by this document 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 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.

EXAMPLE 9

Examples of biometric authentication devices include fingerprint readers and retinal scanners.

The term secrets, as used in this document, while applicable to authentication data, is also intended to be applicable to other types of data that need to be kept secret in order to enforce a specific SFP.

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.

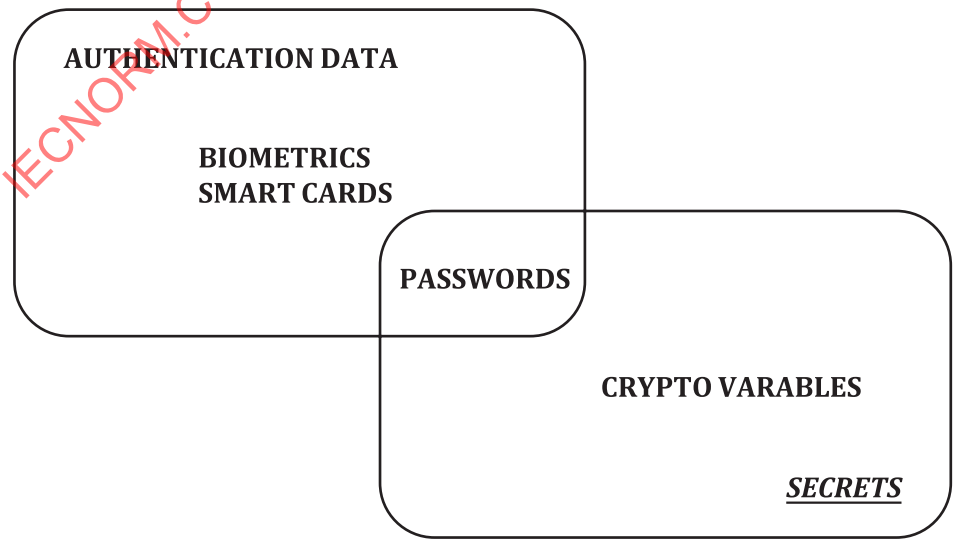


Figure 2 — Relationship between "authentication data" and "secrets"

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

7 Security functional components

7.1 Overview

7.1.1 General

This clause defines the content and presentation of the functional requirements of this document and provides guidance on the organization of the requirements for new, extended components that may be included in a PP, PP-Module, functional package or ST. As described in ISO/IEC 15408-1:2022, Clause 8, the functional components and requirements are expressed in classes, families, components and elements.

7.1.2 Class structure

7.1.2.1 General

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.

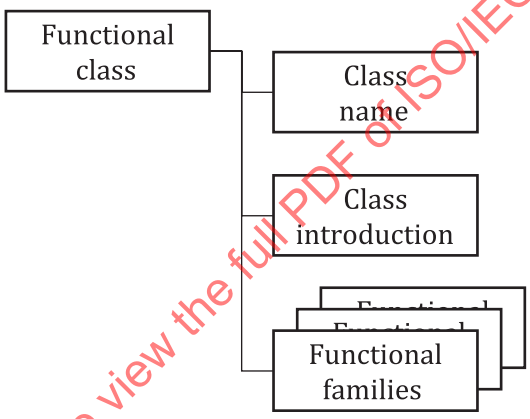


Figure 3 — Functional class structure

NOTE A functional class can contain multiple functional families.

7.1.2.2 Class name

The class name subclause provides information necessary to identify and categorize 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.

7.1.2.3 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 7.2.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

7.1.3 Family structure

7.1.3.1 General

Figure 4 illustrates the functional family structure in diagrammatic form.

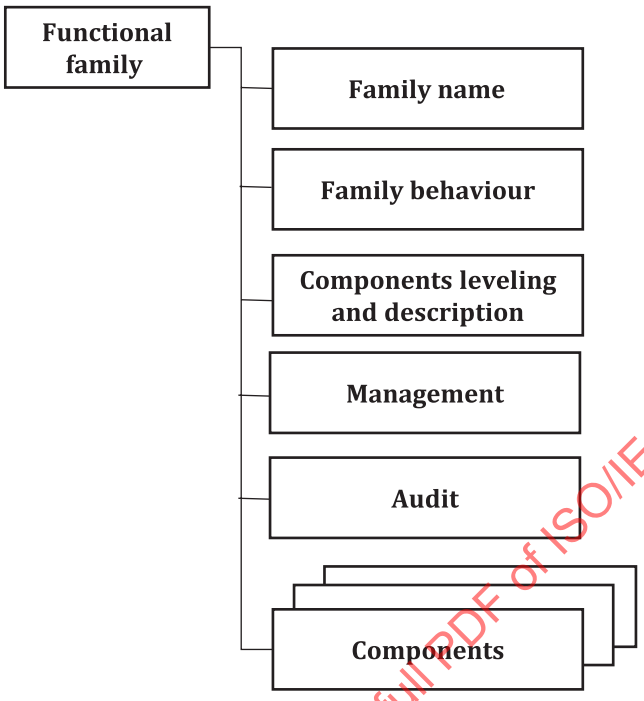


Figure 4 — Functional family structure

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

7.1.3.2 Family name

The family name subclause provides categorical and descriptive information necessary to identify and categorize 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 security components.

7.1.3.3 Family behaviour

The family behaviour subclause provides 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 SFRs derived from a component of this family;

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

7.1.3.4 Components leveling and description

Functional families contain one or more components, any one of which may be selected for inclusion in STs, PPs, PP-Modules or security functional packages. The goal of the components leveling and description subclause is to provide information to users in selecting an appropriate functional

© ISO/IEC 2022 – All rights reserved

component once the family has been identified as being a necessary or useful part of their security requirements.

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 be hierarchical. A component is hierarchical to another if it offers more security.

As explained in 7.2 the descriptions of the families provide a graphical overview of the hierarchy of the components in a family.

7.1.3.5 Management

The management subclauses contain information for ST, PP, PP-Module, or security functional package 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.

An 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.

7.1.3.6 Audit

The audit requirements subclauses contain auditable events for the authors to select, if requirements from the class FAU are included in the ST, PP, PP-Module, or security functional package. 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.

It can be observed that the categorization of auditable events is hierarchical.

EXAMPLE 1

An audit note can include actions that are:

— 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.

EXAMPLE 2

When Basic Audit Generation is needed, all auditable events identified as being both Minimal and Basic are included in the PP, PP-Module, functional package or 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 needed, all identified auditable events (Minimal, Basic and Detailed) are included in the PP, PP-Module, functional package or ST.

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

7.1.4 Component structure

7.1.4.1 General

Figure 5 illustrates the functional component structure.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

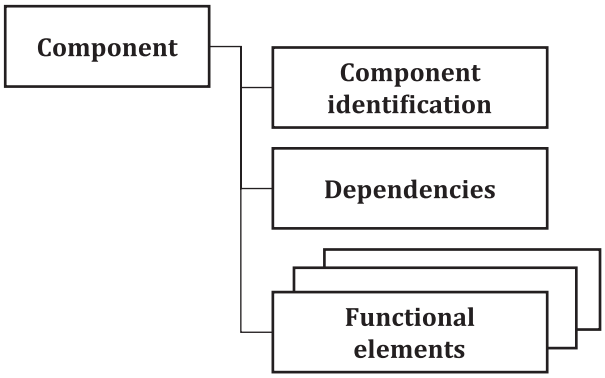


Figure 5 — Functional component structure

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

7.1.4.2 Component identification

The component identification subclause(s) provide descriptive information necessary to identify, categorize, 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 *unique short name*. A unique short form of the functional component name. This short name serves as the principal reference name for the categorization, 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.

7.1.4.3 Functional elements

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

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 shall be selected for inclusion in a PP, PP-Module, security functional package or an ST.

A unique short form of the functional element name is provided.

EXAMPLE

The component 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.

7.1.4.4 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.

© ISO/IEC 2022 – All rights reserved

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, i.e. only references to the other functional components that are required for this component to perform its job properly. The indirect dependencies, i.e. the dependencies that result from the depended upon components, can be found in Annex B of this document. It is noted that in some cases the dependency is optional in that a number of functional components are provided, where each one of them would be sufficient to satisfy the dependency.

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 document are normative and they shall be satisfied within a package, PP or ST. In situations where the indicated dependencies are not applicable, the author shall satisfy the dependency by providing a rationale why it is not applicable and may leave the depended upon component from the package, PP or ST.

7.2 Component catalogue

The grouping of the components in this document does not reflect any formal taxonomy.

This document contains classes of families and components, which are rough groupings on the basis of related function or purpose, presented in alphabetical order. At the start of each class is an informative figure that indicates the taxonomy of each class, indicating the families in each class and the components in each family. Figure 6 is a useful indicator of the hierarchical relationship that can 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.

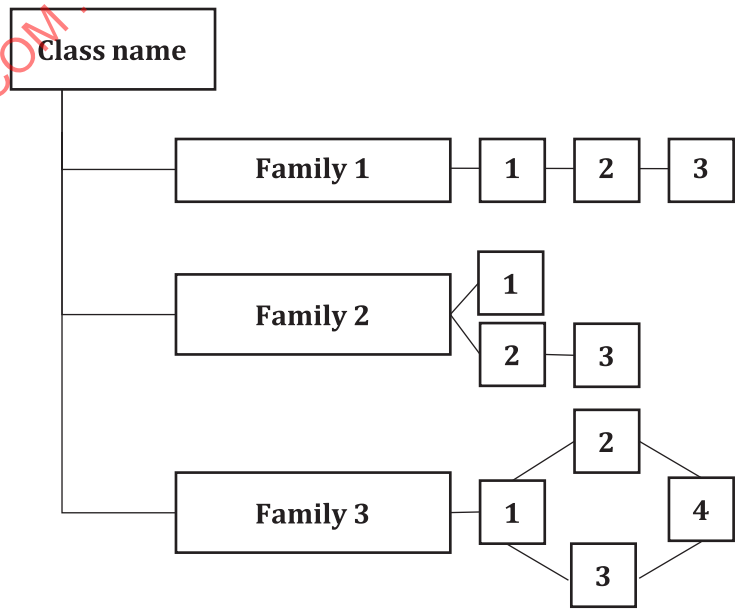


Figure 6 — Sample class decomposition diagram

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

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.

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.

8 Class FAU: Security audit

8.1 Class description

Security auditing involves recognizing, recording, storing, and analyzing 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 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex C provides explanatory information for this class and should be consulted when using the components identified in this class.

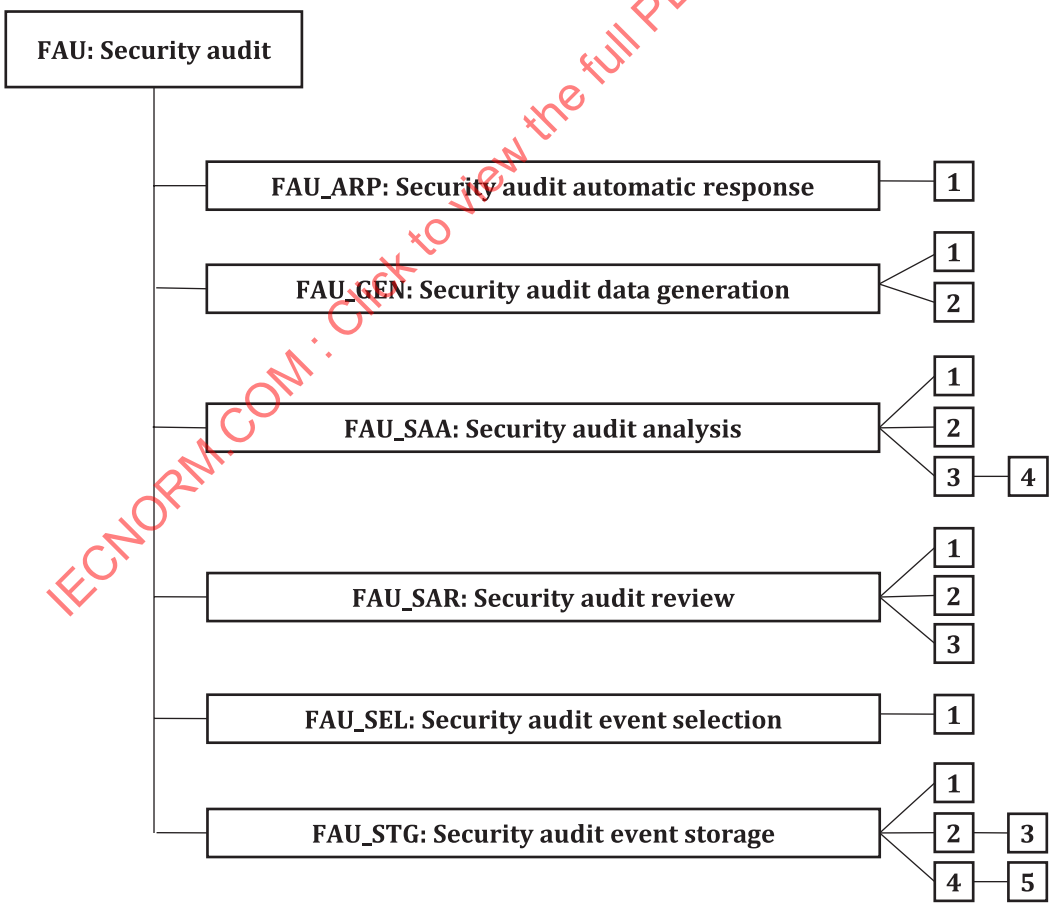


Figure 7 — FAU: Security audit class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

8.2 Security audit automatic response (FAU_ARP)

8.2.1 Family behaviour

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

8.2.2 Components leveling and description

Figure 8 shows the component leveling for this family.

Figure 8 — FAU_ARP: Component leveling

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

8.2.3 Management of FAU_ARP.1

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

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

8.2.4 Audit of FAU_ARP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

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

8.2.5 FAU_ARP.1 Security alarms

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1

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

8.3 Security audit data generation (FAU_GEN)

8.3.1 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.

8.3.2 Components leveling and description

Figure 9 shows the component leveling for this family.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Figure 9 — FAU_GEN: Component leveling

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.

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

8.3.3 Management of FAU_GEN.1, FAU_GEN.2

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

a) there are no management activities foreseen.

8.3.4 Audit of FAU_GEN.1, FAU_GEN.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

8.3.5 FAU_GEN.1 Audit data generation

Component relationships

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

The TSF shall be able to generate audit data 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;

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

FAU_GEN.1.2

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

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

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

8.3.6 FAU_GEN.2 User identity association

Component relationships

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification

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.

8.4 Security audit analysis (FAU_SAA)

8.4.1 Family behaviour

This family defines requirements for automated means that analyze 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.

8.4.2 Components leveling and description

Figure 10 shows the component leveling for this family.

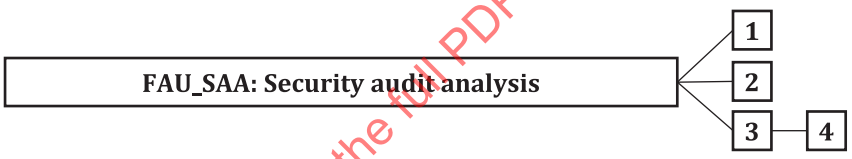


Figure 10 — FAU_SAA: Component leveling

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 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.

8.4.3 Management of FAU_SAA.1

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

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

8.4.4 Management of FAU_SAA.2

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

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

8.4.5 Management of FAU_SAA.3

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

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

8.4.6 Management of FAU_SAA.4

The following actions can 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 sequences of system events.

8.4.7 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, PP-Module, functional package or ST:

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

b) minimal: Automated responses performed by the tool.

8.4.8 FAU_SAA.1 Potential violation analysis

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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.

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*].

8.4.9 FAU_SAA.2 Profile based anomaly detection

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FAU_SAA.2.1

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

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*].

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.

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*].

8.4.10 FAU_SAA.3 Simple attack heuristics

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

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*].

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.

8.4.11 FAU_SAA.4 Complex attack heuristics

Component relationships

Hierarchical to: FAU_SAA.3 Simple attack heuristics

Dependencies: No dependencies.

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.

FAU_SAA.4.2

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

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*].

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.

8.5 Security audit review (FAU_SAR)

8.5.1 Family behaviour

This family defines the requirements for tools that are made available to authorized users to assist in the review of audit data.

8.5.2 Components leveling and description

Figure 11 shows the component leveling for this family.

Figure 11 — FAU_SAR: Component leveling

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

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.

8.5.3 Management of FAU_SAR.1

The following actions can 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.

8.5.4 Management of FAU_SAR.2, FAU_SAR.3

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

a) there are no management activities foreseen.

8.5.5 Audit of FAU_SAR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

8.5.6 Audit of FAU_SAR.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

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

8.5.7 Audit of FAU_SAR.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) detailed: The parameters used for the viewing.

8.5.8 FAU_SAR.1 Audit review

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

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

FAU_SAR.1.2

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

8.5.9 FAU_SAR.2 Restricted audit review

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1

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

8.5.10 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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*].

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

8.6 Security audit event selection (FAU_SEL)

8.6.1 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.

8.6.2 Components leveling and description

Figure 12 shows the component leveling for this family.

Figure 12 — FAU_SEL: Component leveling

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 author of a PP, PP-Module, functional package or ST.

8.6.3 Management of FAU_SEL.1

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

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

8.6.4 Audit of FAU_SEL.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

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

8.6.5 FAU_SEL.1 Selective audit

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

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*]

8.7 Security audit data storage (FAU_STG)

8.7.1 Family behaviour

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

8.7.2 Components leveling and description

Figure 13 shows the component leveling for this family.

Figure 13 — FAU_STG: Component leveling

FAU_STG.1 Audit data storage location, requires that the storage location(s) for audit data be specified.

FAU_STG.2 Protected audit data storage, requires that protections are placed on the audit data. It will be protected from unauthorized deletion and/or modification.

FAU_STG.3 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.4 Action in case of possible audit data loss specifies actions to be taken if a threshold on the stored audit data is exceeded.

FAU_STG.5 Prevention of audit data loss specifies actions to be taken in the case that audit data storage is full.

8.7.3 Management of FAU_STG.1

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

a) maintenance of remote audit storage locations.

8.7.4 Management of FAU_STG.2

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

a) there are no management activities foreseen.

8.7.5 Management of FAU_STG.3

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

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

8.7.6 Management of FAU_STG.4

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

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

8.7.7 Management of FAU_STG.5

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

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

8.7.8 Audit of FAU_STG.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Changes in the location of remote audit data storage.

8.7.9 Audit of FAU_STG.2, FAU_STG.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

8.7.10 Audit of FAU_STG.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

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

8.7.11 Audit of FAU_STG.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

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

8.7.12 FAU_STG.1 Audit data storage location

Component relationships

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FTP_ITC.1 Inter-TSF trusted channel

FAU_STG.1.1

The TSF shall be able to store generated audit data on the [selection: *TOE itself, transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC, [assignment: other storage location(s)]*.]

8.7.13 FAU_STG.2 Protected audit data storage

Component relationships

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation

FAU_STG.2.1

The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.2.2

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

8.7.14 FAU_STG.3 Guarantees of audit data availability

Component relationships

Hierarchical to: FAU_STG.2 Protected audit data storage

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.3.1

The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.3.2

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

FAU_STG.3.3

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

8.7.15 FAU_STG.4 Action in case of possible audit data loss

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_STG.2 Protected audit data storage

FAU_STG.4.1

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

8.7.16 FAU_STG.5 Prevention of audit data loss

Component relationships

Hierarchical to: FAU_STG.4 Action in case of possible audit data loss

Dependencies: FAU_STG.2 Protected audit data storage
FAU_GEN.1 Audit data generation

FAU_STG.5.1

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

9 Class FCO: Communication

9.1 Class description

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

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 14 shows the decomposition of the class.

Figure 14 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex D provides explanatory information for this class and should be consulted when using the components identified in this class.

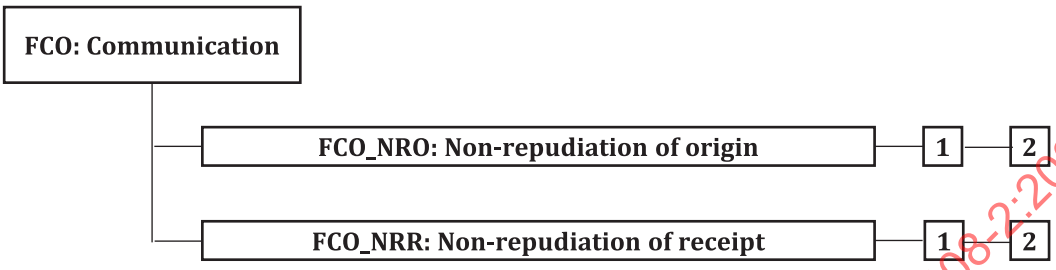


Figure 14 — FCO: Communication class decomposition

9.2 Non-repudiation of origin (FCO_NRO)

9.2.1 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.

9.2.2 Components leveling and description

Figure 15 shows the component leveling for this family.

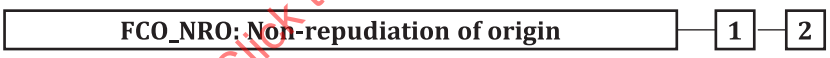


Figure 15 — FCO_NRO: Component leveling

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.

9.2.3 Management of FCO_NRO.1, FCO_NRO.2

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

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

9.2.4 Audit of FCO_NRO.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

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

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

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

9.2.5 Audit of FCO_NRO.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or 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.

9.2.6 FCO_NRO.1 Selective proof of origin

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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]*].

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.

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*].

9.2.7 FCO_NRO.2 Enforced proof of origin

Component relationships

Hierarchical to: FCO_NRO.1 Selective proof of origin

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.2.1

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

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.

FCO_NRO.2.3

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

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*].

9.3 Non-repudiation of receipt (FCO_NRR)

9.3.1 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.

9.3.2 Components leveling and description

Figure 16 shows the component leveling for this family.

Figure 16 — FCO_NRR: Component leveling

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.

9.3.3 Management of FCO_NRR.1, FCO_NRR.2

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

a) the management of changes to information types, fields, originator attributes and third-party recipients of evidence.

9.3.4 Audit of FCO_NRR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or 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.

9.3.5 Audit of FCO_NRR.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or 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.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

9.3.6 FCO_NRR.1 Selective proof of receipt

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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]*].

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.

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*].

9.3.7 FCO_NRR.2 Enforced proof of receipt

Component relationships

Hierarchical to: FCO_NRR.1 Selective proof of receipt

Dependencies: FIA_UID.1 Timing of identification

FCO_NRR.2.1

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

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.

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*].

10 Class FCS: Cryptographic support

10.1 Class description

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 can be in hardware, firmware and/or software.

The FCS: Cryptographic support class is composed of four families.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Figure 17 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex E provides explanatory information for this class and should be consulted when using the components identified in this class.

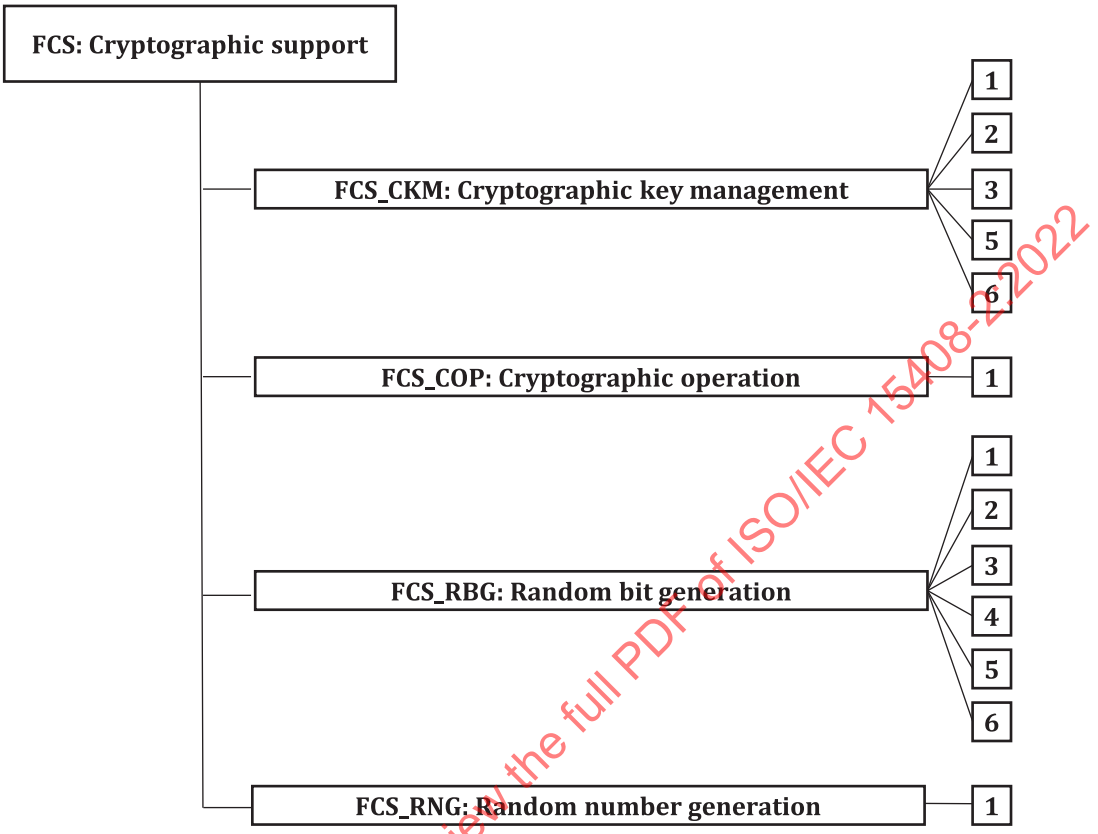


Figure 17 — FCS: Cryptographic support class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

10.2 Cryptographic key management (FCS_CKM)

10.2.1 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;

— cryptographic key derivation;

— timing and event of cryptographic key destruction.

This family should be included whenever there are functional requirements for the management of cryptographic keys.

10.2.2 Components leveling and description

Figure 18 shows the component leveling for this family.

© ISO/IEC 2022 – All rights reserved

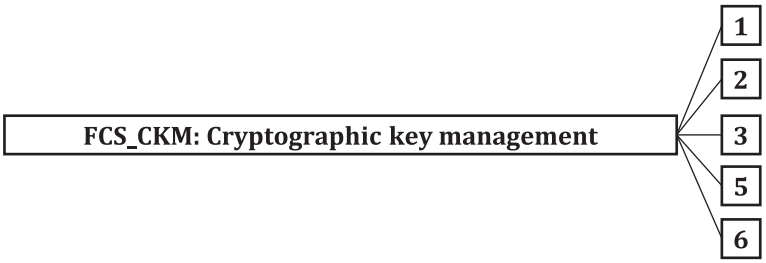


Figure 18 — FCS_CKM: Component leveling

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.5 Cryptographic key derivation, requires that the methods, standards, and parameters for key-derivation are specified.

FCS_CKM.6 Timing and event of cryptographic key destruction, requires cryptographic keys to be destroyed in accordance with specified destruction methods which can be based on an assigned standard.

NOTE Previous editions of this document specified FCS_CKM.4 which has been deprecated in this edition of this document. In order to preserve consistency when applying different editions of this document, the component number has not been re-used.

10.2.3 Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6

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

a) there are no management activities foreseen.

10.2.4 Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Success and failure of the activity;

b) basic: The object attribute(s), and object value(s) excluding any sensitive information.

10.2.5 FCS_CKM.1 Cryptographic key generation

Component relationships

Hierarchical to: No other components.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction

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*].

10.2.6 FCS_CKM.2 Cryptographic key distribution

Component relationships

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 or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access

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*].

10.2.7 FCS_CKM.3 Cryptographic key access

Component relationships

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 or FCS_CKM.5 Cryptographic key derivation]

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*].

10.2.8 FCS_CKM.4 Cryptographic key destruction

The component has been deprecated. See FCS_CKM.6 Timing and event of cryptographic key destruction instead.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

10.2.9 FCS_CKM.5 Cryptographic key derivation

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.5.1

The TSF shall derive cryptographic keys [assignment: *key type*] from [assignment: *input parameters*] in accordance with a specified key derivation algorithm [assignment: *key derivation algorithm*] and specified cryptographic key sizes [assignment: *list of key sizes*] that meet the following: [assignment*: list of standards*].

NOTE See E.2.6. for information on using this component.

10.2.10 FCS_CKM.6 Timing and event of cryptographic key destruction

Component relationships

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.6.1

The TSF shall destroy [assignment: *list of cryptographic keys (including keying material)*] when [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction]*].

FCS_CKM.6.2

The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

10.3 Cryptographic operation (FCS_COP)

10.3.1 Family behaviour

In order for a cryptographic operation to function correctly, the operation shall 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.

10.3.2 Components leveling and description

Figure 19 shows the component leveling for this family.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Figure 19 — FCS_COP: Component leveling

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.

10.3.3 Management of FCS_COP.1

The following actions can be considered for the management functions in FCS:

a) there are no management activities foreseen.

10.3.4 Audit of FCS_COP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or 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.

10.3.5 FCS_COP.1 Cryptographic operation

Component relationships

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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access

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*].

10.4 Random bit generation (FCS_RBG)

10.4.1 Family behaviour

Components in this family address the requirements for random bit/number generation.

10.4.2 Components leveling and description

Figure 20 shows the component leveling for this family.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Figure 20 — FCS_RBG: Component leveling

FCS_RBG.1 Random bit generation (RBG) requires random bit generation to be performed in accordance with selected standards. It also specifies whether the initial seeding is done via an internal or external noise source, as well as when and how an RBG's state is updated.

FCS_RBG.2 Random bit generation (external seeding) gives requirements for seeding by an external (outside the TOE) entropy source.

FCS_RBG.3 Random bit generation (internal seeding – single source) gives requirements for seeding using a TSF entropy source.

FCS_RBG.4 Random bit generation (internal seeding – multiple sources) gives requirements for seeding using multiple TSF entropy sources.

FCS_RBG.5 Random bit generation (combining noise sources) gives requirements for combining multiple entropy sources (multiple internal sources, internal and external).

FCS_RBG.6 Random bit generation service requires random numbers to be supplied over an external interface as a service to other entities.

10.4.3 Management of FCS_RBG.1, FCS_RBG.2, FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6

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

a) there are no management activities foreseen.

10.4.4 Audit of FCS_RBG.1, FCS_RBG.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Failure of the randomization process, failure to initialize or reseed (as supported by the technology).

10.4.5 Audit of FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

10.4.6 FCS_RBG.1 Random bit generation (RBG)

Component relationships

Hierarchical to: No other components.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Dependencies:	[FCS_RBG.2 Random bit generation (external seeding), or FCS_RBG.3 Random bit generation (internal seeding – single source)] FPT_FLS.1 Failure with preservation of secure state FPT_TST.1 TSF self-testing

FCS_RBG.1.1

The TSF shall perform deterministic random bit generation services using [assignment: *RBG algorithm*] in accordance with [assignment: *list of standards*] after initialization with a seed.

FCS_RBG.1.2

The TSF shall use a [selection: *TSF noise source* [assignment: *name of noise source*], *TSF interface for seeding*] for initialized seeding.

FCS_RBG.1.3

The TSF shall update the RBG state by [selection: *reseeding, uninstantiating and re-instantiating*] using a [selection: *TSF noise source* [assignment: *name of noise source*], TSF interface for seeding] in the following situations: [selection:

— ***never;***

— ***on demand;***

— ***on the condition: [assignment: condition];***

— ***after [assignment: time]]***

in accordance with [assignment: *list of standards*].

10.4.7 FCS_RBG.2 Random bit generation (external seeding)

Component relationships

Hierarchical to:	No other components.
Dependencies:	FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.2.1

The TSF shall be able to accept a minimum input of [assignment: *minimum input length greater than zero*] from a TSF interface for the purpose of seeding.

10.4.8 FCS_RBG.3 Random bit generation (internal seeding – single source)

Component relationships

Hierarchical to:	No other components.
Dependencies:	FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.3.1

The TSF shall be able to seed the RBG using a [selection: choose one of: *TSF software-based noise source, TSF hardware-based noise source*][assignment: name of noise source] with a minimum of [assignment: *number of bits*] bits of min-entropy.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

10.4.9 FCS_RBG.4 Random bit generation (internal seeding – multiple sources)

Component relationships

Hierarchical to:	No other components.
Dependencies:	FCS_RBG.1 Random bit generation (RBG) FCS_RBG.5 Random bit generation (combining noise sources)

FCS_RBG.4.1

The TSF shall be able to seed the RBG using **[selection: *[assignment: number] TSF software-based noise source(s), [assignment: number] TSF hardware-based noise source(s)*]**.

10.4.10 FCS_RBG.5 Random bit generation (combining noise sources)

Component relationships

Hierarchical to:	No other components.
Dependencies:	FCS_RBG.1 Random bit generation (RBG) [FCS_RBG.2 Random bit generation (external seeding), or FCS_RBG.3 Random bit generation (internal seeding – single source), or FCS_RBG.4 Random bit generation (internal seeding – multiple sources)]

FCS_RBG.5.1

The TSF shall [assignment: *combining operation*] [selection: *output from TSF noise source(s), input from TSF interface(s) for seeding*)] to create the entropy input into the derivation function as defined in [assignment: *list of standards*], resulting in a minimum of [assignment: *number of bits*] bits of min-entropy.

10.4.11 FCS_RBG.6 Random bit generation service

Component relationships

Hierarchical to:	No other components.
Dependencies:	FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.6.1

The TSF shall provide a [selection: *hardware, software, [assignment: other interface type]*] interface to make the RBG output, as specified in FCS_RBG.1 Random bit generation (RBG), available as a service to entities outside of the TOE.

10.5 Generation of random numbers (FCS_RNG)

10.5.1 Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

10.5.2 Components leveling and description

Figure 21 shows the component leveling for this family.

Figure 21 — FCS_RNG: Component leveling

FCS_RNG.1 Random number generation requires that random numbers meet a defined quality metric.

10.5.3 Management of FCS_RNG.1

The following actions can be considered for the management functions in FCS_RNG.1:

a) there are no management activities foreseen.

10.5.4 Audit of FCS_RNG.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no actions defined to be auditable.

10.5.5 FCS_RNG.1 Random number generation

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1

The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2

The TSF shall provide [selection: *bits, octets of bits, numbers* [assignment: *format of the numbers*]] that meet [assignment: *a defined quality metric*].

11 Class FDP: User data protection

11.1 Class description

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 organized into four groups:

a) user data protection SFPs:

— Access control policy (FDP_ACC);

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

— Information flow control policy (FDP_IFC).

Components in these families permit the author of a PP, PP-Module, functional package or ST to name the user data protection SFPs 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);

— Information Retention Control (FDP_IRC)

— Residual information protection (FDP_RIP);

— Rollback (FDP_ROL);

— Stored data confidentiality (FDP_SDC);

— Stored data integrity (FDP_SDI).

c) off-line storage, import and export:

— Data authentication (FDP_DAU);

— 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);

— 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.

Figure 22 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex F provides explanatory information for this class and should be consulted when using the components identified in this class.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

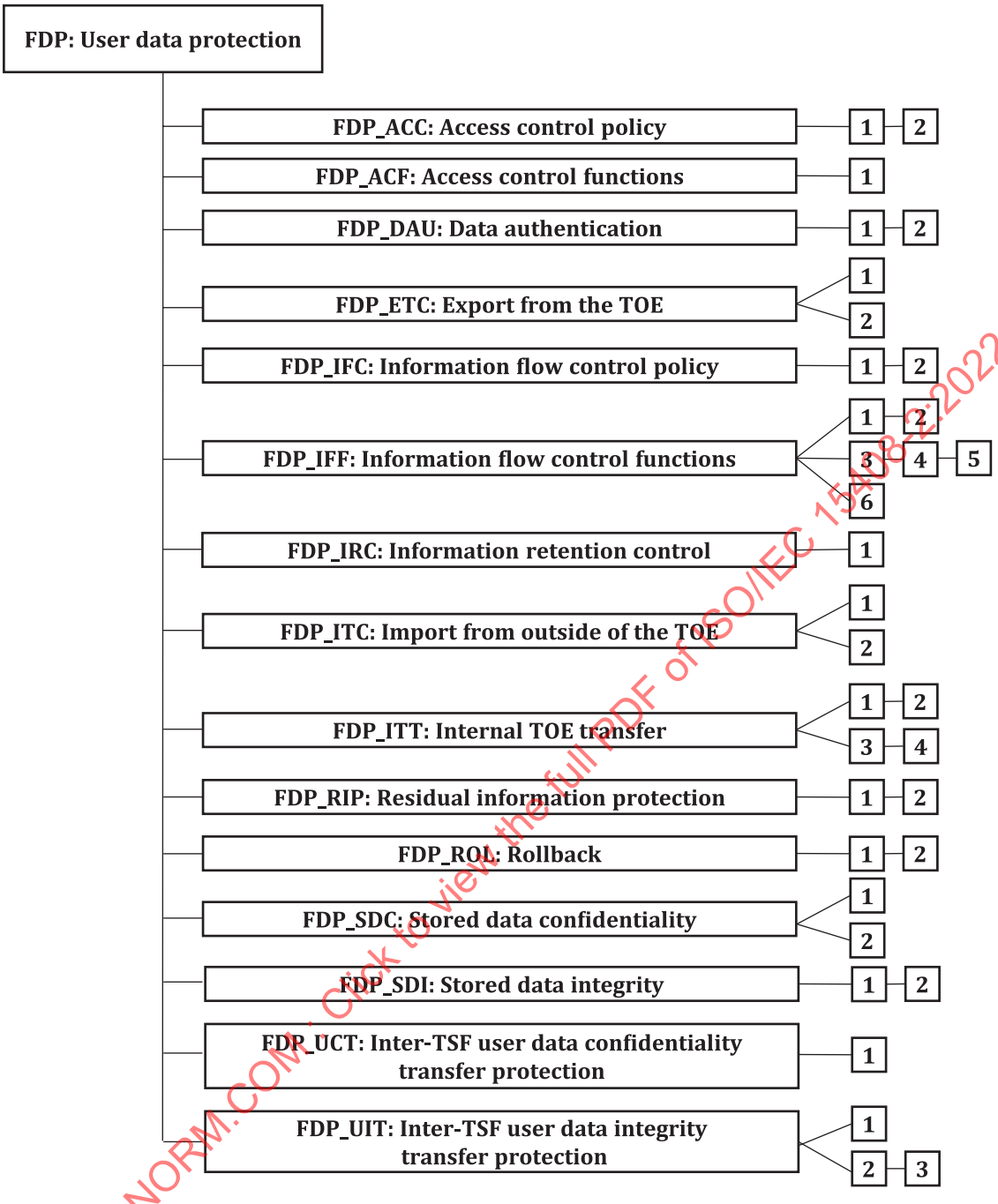


Figure 22 — FDP: User data protection class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

11.2 Access control policy (FDP_ACC)

11.2.1 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 characterized 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 allow 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

© ISO/IEC 2022 – All rights reserved

identified here in Access control 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."

11.2.2 Components leveling and description

Figure 23 shows the component leveling for this family.

Figure 23 — FDP_ACC: Component leveling

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.

11.2.3 Management of FDP_ACC.1, FDP_ACC.2

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

a) there are no management activities foreseen.

11.2.4 Audit of FDP_ACC.1, FDP_ACC.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

11.2.5 FDP_ACC.1 Subset access control

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute-based access control

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*].

11.2.6 FDP_ACC.2 Complete access control

Component relationships

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute-based access control

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.**

FDP_ACC.2.2

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

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.

11.3 Access control functions (FDP_ACF)

11.3.1 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.

11.3.2 Components leveling and description

Figure 24 shows the component leveling for this family.

Figure 24 — FDP_ACF: Component leveling

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 control policy (FDP_ACC). The author of a PP, PP-Module, functional package or ST may also iterate this component to address multiple policies in the TOE.

FDP_ACF.1 Security attribute-based access control allows the TSF to enforce access control based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorize or deny access to an object based upon security attributes.

11.3.3 Management of FDP_ACF.1

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

a) managing the attributes used to make explicit access or denial-based decisions.

11.3.4 Audit of FDP_ACF.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful requests to perform an operation on an object covered by the SFP;

b) basic: All requests to perform an operation on an object covered by the SFP;

c) detailed: The specific security attributes used in making an access check.

11.3.5 FDP_ACF.1 Security attribute-based access control

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute

FDP_ACF.1.1

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

11.4 Data authentication (FDP_DAU)

11.4.1 Family behaviour

Data authentication permits an entity to accept responsibility for the authenticity of information. This family provides a method of providing a guarantee of the validity of a specific unit of data that can be subsequently used to verify that the information content has not been forged or fraudulently modified. In contrast to FAU: Security audit, this family is intended to be applied to "static" data rather than data that is being transferred.

11.4.2 Components leveling and description

Figure 25 shows the component leveling for this family.

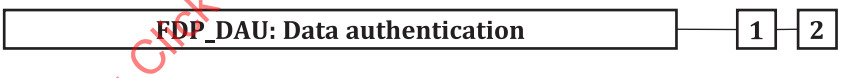


Figure 25 — FDP_DAU: Component leveling

FDP_DAU.1 Basic Data Authentication, requires that the TSF is capable of generating a guarantee of authenticity of the information content of objects.

FDP_DAU.2 Data Authentication with Identity of Guarantor additionally requires that the TSF is capable of establishing the identity of the subject who provided the guarantee of authenticity.

11.4.3 Management of FDP_DAU.1, FDP_DAU.2

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

a) the assignment or modification of the objects for which data authentication may apply can be configurable.

11.4.4 Audit of FDP_DAU.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful generation of validity evidence;

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

b) basic: Unsuccessful generation of validity evidence;

c) detailed: The identity of the subject that requested the evidence.

11.4.5 Audit of FDP_DAU.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful generation of validity evidence;

b) Bbasic: Unsuccessful generation of validity evidence;

c) detailed: The identity of the subject that requested the evidence;

d) detailed: The identity of the subject that generated the evidence.

11.4.6 FDP_DAU.1 Basic Data Authentication

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DAU.1.1

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *list of objects or information types*].

FDP_DAU.1.2

The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information.

11.4.7 FDP_DAU.2 Data Authentication with Identity of Guarantor

Component relationships

Hierarchical to: FDP_DAU.1 Basic Data Authentication

Dependencies: FIA_UID.1 Timing of identification

FDP_DAU.2.1

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *list of objects or information types*].

FDP_DAU.2.2

The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information **and the identity of the user that generated the evidence.**

11.5 Export from the TOE (FDP_ETC)

11.5.1 Family behaviour

This family defines functions for TSF-mediated exporting of user data from the TOE such that its security attributes and protection either can be explicitly preserved or can be ignored once it has been exported. It is concerned with limitations on export and with the association of security attributes with the exported user data.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

11.5.2 Components leveling and description

Figure 26 shows the component leveling for this family.

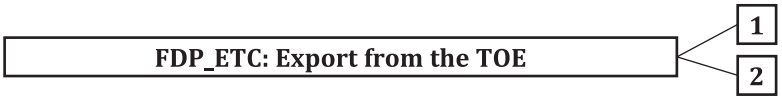


Figure 26 — FDP_ETC: Component leveling

FDP_ETC.1 Export of user data without security attributes, requires that the TSF enforces the appropriate SFPs when exporting user data outside the TSF. User data that is exported by this function is exported without its associated security attributes.

FDP_ETC.2 Export of user data with security attributes, requires that the TSF enforces the appropriate SFPs using a function that accurately and unambiguously associates security attributes with the user data that is exported.

11.5.3 Management of FDP_ETC.1

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

a) there are no management activities foreseen.

11.5.4 Management of FDP_ETC.2

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

a) the additional exportation control rules can be configurable by a user in a defined role.

11.5.5 Audit of FDP_ETC.1, FDP_ETC.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful export of information;

b) basic: All attempts to export information.

11.5.6 FDP_ETC.1 Export of user data without security attributes

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes.

11.5.7 FDP_ETC.2 Export of user data with security attributes

Component relationships

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2

The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3

The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4

The TSF shall ensure that interpretation of the security attributes of the exported user data is as intended by the owner of the user data.

FDP_ETC.2.5

The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: *additional exportation control rules*].

11.6 Information flow control policy (FDP_IFC)

11.6.1 Family behaviour

This family identifies the information flow control SFPs (by name) and defines the scope of control for each named information flow control SFP. This scope of control is characterized by three sets: the subjects under control of the policy, the information under control of the policy, and operations which cause controlled information to flow to and from controlled subjects covered by the policy. The criteria allow multiple policies to exist, each having a unique name. This is accomplished by iterating components from this family once for each named information flow control policy. The rules that define the functionality of an information flow control SFP will be defined by other families such as Information flow control functions (FDP_IFF) and Export from the TOE (FDP_ETC). The names of the information flow control SFPs identified here in Information flow control policy (FDP_IFC) 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 "information flow control SFP."

The TSF mechanism controls the flow of information in accordance with the information flow control SFP. Operations that would change the security attributes of information are not generally permitted as this would be in violation of an information flow control SFP. However, such operations may be permitted as exceptions to the information flow control SFP if explicitly specified.

11.6.2 Components leveling and description

Figure 27 shows the component leveling for this family.

Figure 27 — FDP_IFC: Component leveling

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FDP_IFC.1 Subset information flow control, requires that each identified information flow control SFPs be in place for a subset of the possible operations on a subset of information flows in the TOE.

FDP_IFC.2 Complete information flow control, requires that each identified information flow control SFP cover all operations on subjects and information covered by that SFP. It further requires that all information flows and operations controlled by the TSF are covered by at least one identified information flow control SFP.

11.6.3 Management of FDP_IFC.1, FDP_IFC.2

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

a) there are no management activities foreseen.

11.6.4 Audit of FDP_IFC.1, FDP_IFC.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

11.6.5 FDP_IFC.1 Subset information flow control

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1

The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].

11.6.6 FDP_IFC.2 Complete information flow control

Component relationships

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1

The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects and* ***information***] **and all** operations that cause **that** information to flow to and from subjects covered by the **SFP.**

FDP_IFC.2.2

The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

11.7 Information flow control functions (FDP_IFF)

11.7.1 Family behaviour

This family describes the rules for the specific functions that can implement the information flow control SFPs named in Information flow control policy (FDP_IFC), which also specifies the scope of

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

control of the policy. It consists of two kinds of requirements: one addressing the common information flow function issues, and a second addressing illicit information flows (i.e. covert channels). This division arises because the issues concerning illicit information flows are, in some sense, orthogonal to the rest of an information flow control SFP. By their nature, they circumvent the information flow control SFP resulting in a violation of the policy. As such, they require special functions to either limit or prevent their occurrence.

11.7.2 Components leveling and description

Figure 28 shows the component leveling for this family.

Figure 28 — FDP_IFF: Component leveling

FDP_IFF.1 Simple security attributes, requires security attributes on information, and on subjects that cause that information to flow and on subjects that act as recipients of that information. It specifies the rules that must be enforced by the function and describes how security attributes are derived by the function.

FDP_IFF.2 Hierarchical security attributes expands on the requirements of FDP_IFF.1 Simple security attributes by requiring that all information flow control SFPs in the set of SFRs use hierarchical security attributes that form a lattice (as defined in mathematics). FDP_IFF.2.6 is derived from the mathematical properties of a lattice. A lattice consists of a set of elements with an ordering relationship with the property defined in the first bullet, a least upper bound which is the unique element in the set that is greater than or equal to (in the ordering relationship) than any other element of the lattice, and a greatest lower bound, which is the unique element in the set that is smaller than or equal to than any other element of the lattice.

FDP_IFF.3 Limited illicit information flows, requires the SFP to cover illicit information flows, but does not necessarily eliminate them.

FDP_IFF.4 Partial elimination of illicit information flows, requires the SFP to cover the elimination of some (but does not necessarily all) illicit information flows.

FDP_IFF.5 No illicit information flows, requires SFP to cover the elimination of all illicit information flows.

FDP_IFF.6 Illicit information flow monitoring, requires the SFP to monitor illicit information flows for specified and maximum capacities.

11.7.3 Management of FDP_IFF.1, FDP_IFF.2

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

a) managing the attributes used to make explicit access-based decisions.

11.7.4 Management of FDP_IFF.3, FDP_IFF.4, FDP_IFF.5

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

a) there are no management activities foreseen.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

11.7.5 Management of FDP_IFF.6

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

a) the enabling or disabling of the monitoring function;

b) modification of the maximum capacity at which the monitoring occurs.

11.7.6 Audit of FDP_IFF.1, FDP_IFF.2, FDP_IFF.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Decisions to permit requested information flows;

b) basic: All decisions on requests for information flow;

c) detailed: The specific security attributes used in making an information flow enforcement decision;

d) detailed: Some specific subsets of the information that has flowed based upon policy goals.

11.7.7 Audit of FDP_IFF.3, FDP_IFF.4, FDP_IFF.6

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Decisions to permit requested information flows;

b) basic: All decisions on requests for information flow;

c) basic: The use of identified illicit information flow channels;

d) detailed: The specific security attributes used in making an information flow enforcement decision;

e) detailed: Some specific subsets of the information that has flowed based upon policy goals;

f) detailed: The use of identified illicit information flow channels with estimated maximum capacity exceeding a specified value.

11.7.8 FDP_IFF.1 Simple security attributes

Component relationships

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute

FDP_IFF.1.1

The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*].

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that hold between subject and information security attributes*].

FDP_IFF.1.3

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorize information flows*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

11.7.9 FDP_IFF.2 Hierarchical security attributes

Component relationships

Hierarchical to:	FDP_IFF.1 Simple security attributes
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute

FDP_IFF.2.1

The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*].

FDP_IFF.2.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, **based on the ordering relationships between security attributes** hold: [assignment: *for each operation, the security attribute-based relationship that shall hold between subject and information security attributes*].

FDP_IFF.2.3

The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.2.4

The TSF shall explicitly authorize an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorize information flows*].

FDP_IFF.2.5

The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

FDP_IFF.2.6

The TSF shall enforce the following relationships for any two valid information flow control security attributes:

a) there exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable;

b) there exists a “least upper bound” in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes;

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

c) there exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.

11.7.10 FDP_IFF.3 Limited illicit information flows

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FDP_IFF.3.1

The TSF shall enforce the [assignment: *information flow control SFP*] to limit the capacity of [assignment: *types of illicit information flows*] to a [assignment: *maximum capacity*].

11.7.11 FDP_IFF.4 Partial elimination of illicit information flows

Component relationships

Hierarchical to: FDP_IFF.3 Limited illicit information flows

Dependencies: FDP_IFC.1 Subset information flow control

FDP_IFF.4.1

The TSF shall enforce the [assignment: *information flow control SFP*] to limit the capacity of [assignment: *types of illicit information flows*] to a [assignment: *maximum capacity*].

FDP_IFF.4.2

The TSF shall prevent [assignment: *types of illicit information flows*].

11.7.12 FDP_IFF.5 No illicit information flows

Component relationships

Hierarchical to: FDP_IFF.4 Partial elimination of illicit information flows

Dependencies: FDP_IFC.1 Subset information flow control

FDP_IFF.5.1

The TSF shall ensure that **no illicit information flows exist to circumvent [assignment: *name of information flow control SFP*]**.

11.7.13 FDP_IFF.6 Illicit information flow monitoring

Component relationships

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control

FDP_IFF.6.1

The TSF shall enforce the [assignment: *information flow control SFP*] to monitor [assignment: *types of illicit information flows*] when it exceeds the [assignment: *maximum capacity*].

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

11.8 Information Retention Control (FDP_IRC)

11.8.1 Family behaviour

The “Information retention control” family addresses a basic need in secure information processing and storage applications for the secure management of data no longer needed by the TOE to perform its operations, but that is still stored in the TOE.

The historical view of IT systems as data storage systems suggested that once entered, data would seldom be deleted from the system, and if it was deleted, this would mainly be because of storage exhaustion problems.

However, in a multilateral or high security environment it is important to minimize the replication of data, as well as the time period during which data is stored in the system. It is also possible that users can want their IT products to avoid retaining sensitive data that they consider to be exploitable by third parties or that can threaten privacy. FDP_IRC may help users to gain confidence that the product is secure by deleting every copy of the data when it is no longer needed.

The FDP_RIP “Residual information protection” family addresses one side of this problem, but an explicit requirement on the management of data that is no longer needed is missing.

Of course, competing requirements can arise, since some data can be needed by the system for more operations over a longer time period. Possible solutions to this problem are:

— better protecting the information objects stored in the TOE from access;

— re-requesting the protected information from the user each time it is needed.

Information retention control ensures, that data no longer necessary for the operation of the TOE is deleted by the TOE. Components of this family require the author of a PP, PP-Module, functional package or ST to identify the TOE operations, including both simple and complex processing and the information objects, that are not to be kept in the TOE, that are the subject of those operations.

The TOE is also required to keep track of such stored information objects, and to delete both the on-line and the off-line information objects that are no longer required.

This family sets only requirements on information objects requested for specific activities in the TOE operation, and not on general data gathering. The policies which control the collection, storage, processing, disclosure, and elimination of general user data stored on the TOE are detailed elsewhere, and are in the domain of the environmental objectives and organizational policies, not of the PP, PP-Module, functional package or ST.

When more than one operation requires the presence of a protected object, all operations, which refer to the required object, shall end before deleting it.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

11.8.2 Components leveling and description

Figure 29 shows the component leveling for this family.

Figure 29 — FDP_IRC: Component leveling

FDP_IRC.1 Information retention control requires that the TSF ensure that any copy of a defined set of objects in the TOE is deleted when no longer strictly necessary for the operation of the TOE, and to identify and define the operations for which the object is required.

© ISO/IEC 2022 – All rights reserved

11.8.3 Management of FDP_IRC.1

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

a) there are no management actions foreseen.

11.8.4 Audit of FDP_IRC.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

11.8.5 FDP_IRC.1 Information retention control

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_IRC.1.1

The TSF shall enforce the [assignment: *information erasure policy*] on a [assignment*: list of objects*] required for [assignment: *list of operations*] so that the selected objects are deleted irreversibly and untraceably from the TOE promptly upon termination of the selected operations.

FDP_IRC.1.2

The TSF shall ensure that [assignment: *list of objects*] cannot be accessed after their release and prior to their irreversible and untraceable deletion.

11.9 Import from outside of the TOE (FDP_ITC)

11.9.1 Family behaviour

This family defines the mechanisms for TSF-mediated importing of user data into the TOE such that it has appropriate security attributes and is appropriately protected. It is concerned with limitations on importation, determination of desired security attributes, and interpretation of security attributes associated with the user data.

11.9.2 Components leveling and description

Figure 30 shows the component leveling for this family.

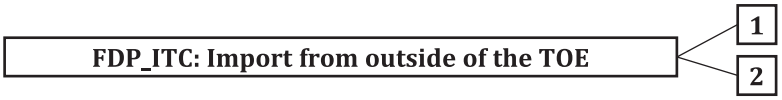


Figure 30 — FDP_ITC: Component leveling

FDP_ITC.1 Import of user data without security attributes, requires that the security attributes correctly represent the user data and are supplied separately from the object.

FDP_ITC.2 Import of user data with security attributes, requires that security attributes correctly represent the user data and are accurately and unambiguously associated with the user data imported from outside the TOE.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

11.9.3 Management of FDP_ITC.1, FDP_ITC.2

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

a) the modification of the additional control rules used for import.

11.9.4 Audit of FDP_ITC.1, FDP_ITC.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful import of user data, including any security attributes;

b) basic: All attempts to import user data, including any security attributes;

c) detailed: The specification of security attributes for imported user data supplied by an authorized user.

11.9.5 FDP_ITC.1 Import of user data without security attributes

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

11.9.6 FDP_ITC.2 Import of user data with security attributes

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3

The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4

The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*].

11.10 Internal TOE transfer (FDP_ITT)

11.10.1 Family behaviour

This family provides requirements that address protection of user data when it is transferred between separated parts of a TOE across an internal channel. This may be contrasted with the Inter-TSF user data confidentiality transfer protection (FDP_UCT) and Inter-TSF user data integrity transfer protection (FDP_UIT) families, which provide protection for user data when it is transferred between distinct TSFs across an external channel, and Export from the TOE (FDP_ETC) and Import from outside of the TOE (FDP_ITC), which address TSF-mediated transfer of data to or from outside the TOE.

11.10.2 Components leveling and description

Figure 31 shows the component leveling for this family.

Figure 31 — FDP_ITT: Component leveling

FDP_ITT.1 Basic internal transfer protection, requires that user data be protected when transmitted between parts of the TOE.

FDP_ITT.2 Transmission separation by attribute, requires separation of data based on the value of SFP-relevant attributes in addition to the first component.

FDP_ITT.3 Integrity monitoring, requires that the TSF monitor user data transmitted between parts of the TOE for identified integrity errors.

FDP_ITT.4 Attribute-based integrity monitoring expands on the third component by allowing the form of integrity monitoring to differ by SFP-relevant attributes.

11.10.3 Management of FDP_ITT.1, FDP_ITT.2

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

a) if the TSF provides multiple methods to protect user data during transmission between physically separated parts of the TOE, the TSF can provide a pre-defined role with the ability to select the method that will be used.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

11.10.4 Management of FDP_ITT.3, FDP_ITT.4

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

a) the specification of the actions to be taken upon detection of an integrity error can be configurable.

11.10.5 Audit of FDP_ITT.1, FDP_ITT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful transfers of user data, including identification of the protection method used;

b) basic: All attempts to transfer user data, including the protection method used and any errors that occurred.

11.10.6 Audit of FDP_ITT.3, FDP_ITT.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful transfers of user data, including identification of the integrity protection method used;

b) basic: All attempts to transfer user data, including the integrity protection method used and any errors that occurred;

c) basic: Unauthorized attempts to change the integrity protection method;

d) detailed: The action taken upon detection of an integrity error.

11.10.7 FDP_ITT.1 Basic internal transfer protection

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ITT.1.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to prevent the [selection: *disclosure, modification, loss of use*] of user data when it is transmitted between physically-separated parts of the TOE.

11.10.8 FDP_ITT.2 Transmission separation by attribute

Component relationships

Hierarchical to:	FDP_ITT.1 Basic internal transfer protection
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ITT.2.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to prevent the [selection: *disclosure, modification, loss of use*] of user data when it is transmitted between physically-separated parts of the TOE.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FDP_ITT.2.2

The TSF shall separate data controlled by the SFP(s) when transmitted between physically-separated parts of the TOE, based on the values of the following: [assignment: *security attributes that require separation*].

11.10.9 FDP_ITT.3 Integrity monitoring

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FDP_ITT.1 Basic internal transfer protection

FDP_ITT.3.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: *integrity errors*].

FDP_ITT.3.2

Upon detection of a data integrity error, the TSF shall [assignment: *specify the action to be taken upon integrity error*].

11.10.10 FDP_ITT.4 Attribute-based integrity monitoring

Component relationships

Hierarchical to:	FDP_ITT.3 Integrity monitoring
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FDP_ITT.2 Transmission separation by attribute

FDP_ITT.4.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [assignment: *integrity errors*], **based on the following attributes: [assignment: *security attributes that require separate transmission channels*].**

FDP_ITT.4.2

Upon detection of a data integrity error, the TSF shall [assignment: *specify the action to be taken upon integrity error*].

11.11 Residual information protection (FDP_RIP)

11.11.1 Family behaviour

This family addresses the need to ensure that any data contained in a resource is not available when the resource is de-allocated from one object and reallocated to a different object. This family requires protection for any data contained in a resource that has been logically deleted or released but may still be present within the TSF-controlled resource which in turn may be re-allocated to another object.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

11.11.2 Components leveling and description

Figure 32 shows the component leveling for this family.

Figure 32 — FDP_RIP: Component leveling

FDP_RIP.1 Subset residual information protection, requires that the TSF ensure that any residual information content of any resources is unavailable to a defined subset of the objects controlled by the TSF upon the resource's allocation or deallocation.

FDP_RIP.2 Full residual information protection, requires that the TSF ensure that any residual information content of any resources is unavailable to all objects upon the resource's allocation or deallocation.

11.11.3 Management of FDP_RIP.1, FDP_RIP.2

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

a) the choice of when to perform residual information protection (i.e. upon allocation or deallocation) can be made configurable within the TOE.

11.11.4 Audit of FDP_RIP.1, FDP_RIP.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

11.11.5 FDP_RIP.1 Subset residual information protection

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: [assignment: *list of objects*].

11.11.6 FDP_RIP.2 Full residual information protection

Component relationships

Hierarchical to: FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

FDP_RIP.2.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] **all** objects.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

11.12 Rollback (FDP_ROL)

11.12.1 Family behaviour

The rollback operation involves undoing the last operation or a series of operations, bounded by some limit, such as a period of time, and return to a previous known state. Rollback provides the ability to undo the effects of an operation or series of operations to preserve the integrity of the user data.

11.12.2 Components leveling and description

Figure 33 shows the component leveling for this family.

Figure 33 — FDP_ROL: Component leveling

FDP_ROL.1 Basic rollback addresses a need to roll back or undo a limited number of operations within the defined bounds.

FDP_ROL.2 Advanced rollback addresses the need to roll back or undo all operations within the defined bounds.

11.12.3 Management of FDP_ROL.1, FDP_ROL.2

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

a) the boundary limit to which rollback may be performed can be a configurable item within the TOE;

b) permission to perform a rollback operation can be restricted to a well-defined role.

11.12.4 Audit of FDP_ROL.1, FDP_ROL.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: All successful rollback operations;

b) basic: All attempts to perform rollback operations;

c) detailed: All attempts to perform rollback operations, including identification of the types of operations rolled back.

11.12.5 FDP_ROL.1 Basic rollback

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ROL.1.1

The TSF shall enforce [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to permit the rollback of the [assignment: *list of operations*] on the [assignment: *information and/or list of objects*].

FDP_ROL.1.2

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall permit operations to be rolled back within the [assignment: *boundary limit to which rollback may be performed*].

11.12.6 FDP_ROL.2 Advanced rollback

Component relationships

Hierarchical to:	FDP_ROL.1 Basic rollback
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ROL.2.1

The TSF shall enforce [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to permit the rollback of **all** the **operations** on the [assignment: ***list*** *of objects*].

FDP_ROL.2.2

The TSF shall permit operations to be rolled back within the [assignment: *boundary limit to which rollback may be performed*].

11.13 Stored data confidentiality (FDP_SDC)

11.13.1 Family behaviour

This family provides requirements that address protection of user data confidentiality while the data is stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromise of their information bypassing these interfaces. It complements the family Stored data integrity (FDP_SDI) which protects the user data from integrity errors while being stored in the memory.

11.13.2 Components leveling and description

Figure 34 shows the component leveling for this family.

Figure 34 — FDP_SDC: Component leveling

FDP_SDC.1 Stored data confidentiality, requires the TSF to protect the confidentiality of information of the user data in specified memory areas.

FDP_SDC.2 Stored data confidentiality with dedicated method, requires the TSF to protect the confidentiality of the user data according to data characteristics leading to specify a dedicated method of protection of confidentiality.

11.13.3 Management of FDP_SDC.1, FDP_SDC.2

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

a) there are no management activities foreseen.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

11.13.4 Audit of FDP_SDC.1, FDP_SDC.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

11.13.5 FDP_SDC.1 Stored data confidentiality

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDC.1.1

The TSF shall ensure the confidentiality of [selection: *all user data, the following user data [assignment: list of user data]*] while it is stored in the [selection: *temporary memory, persistent memory, any memory*].

11.13.6 FDP_SDC.2 Stored data confidentiality with dedicated method

Component relationships

Hierarchical to: No other components.

Dependencies: FCS_COP.1.

FDP_SDC.2.1

The TSF shall ensure the confidentiality of the [selection: *all user data, the following user data [assignment: list of user data]*] according to [assignment: *data characteristics*] while it is stored under the control of the TSF.

FDP_SDC.2.2

The TSF shall ensure the confidentiality of the user data specified in FDP_SDC.2.1 without user intervention.

11.14 Stored data integrity (FDP_SDI)

11.14.1 Family behaviour

This family provides requirements that address protection of user data while it is stored within containers controlled by the TSF. Integrity errors may affect user data stored in memory, or in a storage device. This family differs from Internal TOE transfer (FDP_ITT) which protects the user data from integrity errors while being transferred within the TOE.

11.14.2 Components leveling and description

Figure 35 shows the component leveling for this family.

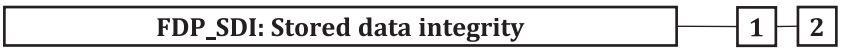


Figure 35 — FDP_SDI: Component leveling

FDP_SDI.1 Stored data integrity monitoring, requires that the TSF monitor user data stored within containers controlled by the TSF for identified integrity errors.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FDP_SDI.2 Stored data integrity monitoring and action adds the additional capability to the first component by allowing for actions to be taken as a result of an error detection.

11.14.3 Management of FDP_SDI.1

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

a) there are no management activities foreseen.

11.14.4 Management of FDP_SDI.2

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

a) the actions to be taken upon the detection of an integrity error can be configurable.

11.14.5 Audit of FDP_SDI.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful attempts to check the integrity of user data, including an indication of the results of the check;

b) basic: All attempts to check the integrity of user data, including an indication of the results of the check, if performed;

c) detailed: The type of integrity error that occurred.

11.14.6 Audit of FDP_SDI.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful attempts to check the integrity of user data, including an indication of the results of the check;

b) basic: All attempts to check the integrity of user data, including an indication of the results of the check, if performed;

c) detailed: The type of integrity error that occurred;

d) detailed: The action taken upon detection of an integrity error.

11.14.7 FDP_SDI.1 Stored data integrity monitoring

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDI.1.1

The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].

11.14.8 FDP_SDI.2 Stored data integrity monitoring and action

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1

The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*].

11.15 Inter-TSF user data confidentiality transfer protection (FDP_UCT)

11.15.1 Family behaviour

This family defines the requirements for ensuring the confidentiality of user data when it is transferred using an external channel between the TOE and another trusted IT product.

11.15.2 Components leveling and description

Figure 36 shows the component leveling for this family.

Figure 36 — FDP_UCT: Component leveling

In FDP_UCT.1 Basic data exchange confidentiality, the goal is to provide protection from disclosure of user data while in transit.

11.15.3 Management of FDP_UCT.1

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

a) there are no management activities foreseen.

11.15.4 Audit of FDP_UCT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The identity of any user or subject using the data exchange mechanisms;

b) basic: The identity of any unauthorized user or subject attempting to use the data exchange mechanisms;

c) basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This can include security attributes associated with the information.

11.15.5 FDP_UCT.1 Basic data exchange confidentiality

Component relationships

Hierarchical to: No other components.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to [selection: *transmit, receive*] user data in a manner protected from unauthorized disclosure.

11.16 Inter-TSF user data integrity transfer protection (FDP_UIT)

11.16.1 Family behaviour

This family defines the requirements for providing integrity for user data in transit between the TOE and another trusted IT product and recovering from detectable errors. At a minimum, this family monitors the integrity of user data for modifications. Furthermore, this family supports different ways of correcting detected integrity errors.

11.16.2 Components leveling and description

Figure 37 shows the component leveling for this family.

Figure 37 — FDP_UIT: Component leveling

FDP_UIT.1 Data exchange integrity addresses detection of modifications, deletions, insertions, and replay errors of the user data transmitted.

FDP_UIT.2 Source data exchange recovery addresses recovery of the original user data by the receiving TSF with help from the source trusted IT product.

FDP_UIT.3 Destination data exchange recovery addresses recovery of the original user data by the receiving TSF on its own without any help from the source trusted IT product.

11.16.3 Management of FDP_UIT.1, FDP_UIT.2, FDP_UIT.3

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

a) there are no management activities foreseen.

11.16.4 Audit of FDP_UIT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The identity of any user or subject using the data exchange mechanisms;

b) basic: The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorized to do so;

c) basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This can include security attributes associated with the user data;

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

d) basic: Any identified attempts to block transmission of user data;

e) detailed: The types and/or effects of any detected modifications of transmitted user data.

11.16.5 Audit of FDP_UIT.2, FDP_UIT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The identity of any user or subject using the data exchange mechanisms;

b) minimal: Successful recovery from errors including the type of error that was detected;

c) basic: The identity of any user or subject attempting to use the user data exchange mechanisms, but who is unauthorized to do so;

d) basic: A reference to the names or other indexing information useful in identifying the user data that was transmitted or received. This can include security attributes associated with the user data;

e) basic: Any identified attempts to block transmission of user data;

f) detailed: The types and/or effects of any detected modifications of transmitted user data.

11.16.6 FDP_UIT.1 Data exchange integrity

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

FDP_UIT.1.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to [selection*: transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.

FDP_UIT.1.2

The TSF shall be able to determine on receipt of user data, whether [selection: *modification, deletion, insertion, replay*] has occurred.

11.16.7 FDP_UIT.2 Source data exchange recovery

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FDP_UIT.1 Data exchange integrity, or FTP_ITC.1 Inter-TSF trusted channel]

FDP_UIT.2.1

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to recover from [assignment: *list of recoverable errors*] with the help of the source trusted IT product.

11.16.8 FDP_UIT.3 Destination data exchange recovery

Hierarchical to:	FDP_UIT.2 Source data exchange recovery
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FDP_UIT.1 Data exchange integrity, or FTP_ITC.1 Inter-TSF trusted channel]

FDP_UIT.3.1

The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to recover from [assignment: *list of recoverable errors*] **without any** help **from** the source trusted IT product.

12 Class FIA: Identification and authentication

12.1 Class description

Families in this class address the requirements for functions to establish and verify a claimed user identity.

Identification and authentication are required to ensure that users are associated with the proper security attributes

The unambiguous identification of authorized users and the correct association of security attributes with users and subjects is critical to the enforcement of the intended security policies. The families in this class deal with determining and verifying the identity of users, determining their authority to interact with the TOE, and with the correct association of security attributes for each authorized user. Other classes of requirements are dependent upon correct identification and authentication of users in order to be effective.

Figure 38 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex G provides explanatory information for this class and should be consulted when using the components identified in this class.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

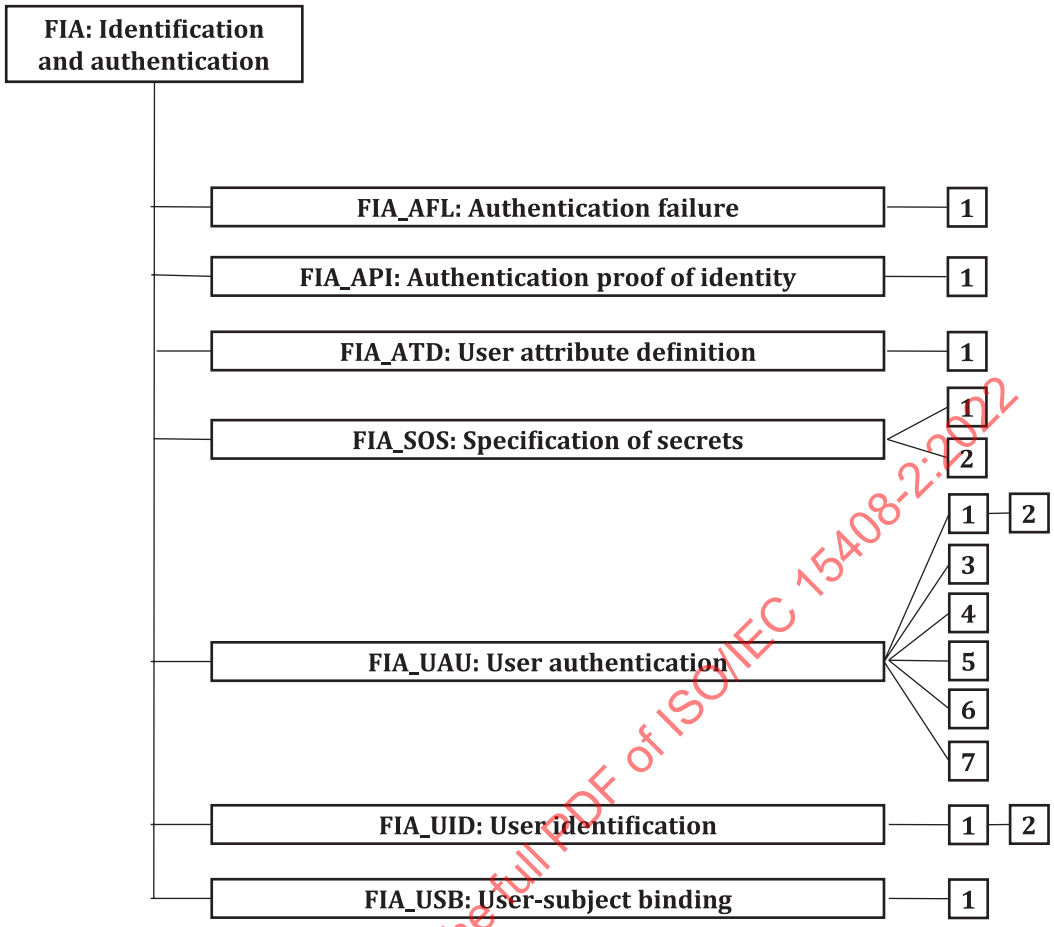


Figure 38 — FIA: Identification and authentication class decomposition

12.2 Authentication failures (FIA_AFL)

12.2.1 Family behaviour

This family contains requirements for defining values for some number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures. Parameters include, but are not limited to, the number of failed authentication attempts and time thresholds.

12.2.2 Components leveling and description

Figure 39 shows the component leveling for this family.

Figure 39 — FIA_AFL: Component leveling

FIA_AFL.1 Authentication failure handling, requires that the TSF be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the TSF be able to disable the user account or the point of entry from which the attempts were made until an administrator-defined condition occurs.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

12.2.3 Management of FIA_AFL.1

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

a) management of the threshold for unsuccessful authentication attempts;

b) management of actions to be taken in the event of an authentication failure.

12.2.4 Audit of FIA_AFL.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.

12.2.5 FIA_AFL.1 Authentication failure handling

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1

The TSF shall detect when [selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

12.3 Authentication proof of identity (FIA_API)

12.3.1 Family behaviour

This family defines functions provided by the TOE to prove its identity and so allow for verification of the TOE by an external entity in the TOE's IT environment.

12.3.2 Components leveling and description

Figure 40 shows the component leveling for this family.

Figure 40 — FIA_API: Component leveling

FIA_API.1 Authentication Proof of Identity, provides proof of the identity of the TOE to an external entity.

12.3.3 Management of FIA_API.1

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

a) management of authentication information used to prove the claimed identity.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

12.3.4 Audit of FIA_API.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

12.3.5 FIA_API.1 Authentication proof of identity

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_API.1.1

The TSF shall provide an [assignment: *authentication mechanism*] to prove the identity of [assignment: *entity*] by including the following properties [assignment: *list of properties*] to an external entity.

12.4 User attribute definition (FIA_ATD)

12.4.1 Family behaviour

All authorized users may have a set of security attributes, other than the user's identity, that is used to enforce the SFRs. This family defines the requirements for associating user security attributes with users as needed to support the TSF in making security decisions.

12.4.2 Components leveling and description

Figure 41 shows the component leveling for this family.

Figure 41 — FIA_ATD: Component leveling

FIA_ATD.1 User attribute definition, allows user security attributes for each user to be maintained individually.

12.4.3 Management of FIA_ATD.1

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

a) if indicated in the assignment, the authorized administrator can be able to define additional security attributes for users.

12.4.4 Audit of FIA_ATD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

12.4.5 FIA_ATD.1 User attribute definition

Component relationships

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

12.5 Specification of secrets (FIA_SOS)

12.5.1 Family behaviour

This family defines requirements for mechanisms that enforce defined quality metrics on provided secrets and generate secrets to satisfy the defined metric.

12.5.2 Components leveling and description

Figure 42 shows the component leveling for this family.

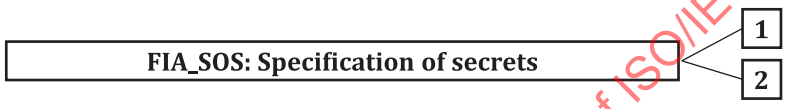


Figure 42 — FIA_SOS: Component leveling

FIA_SOS.1 Verification of secrets, requires the TSF to verify that secrets meet defined quality metrics.

FIA_SOS.2 TSF Generation of secrets, requires the TSF to be able to generate secrets that meet defined quality metrics.

12.5.3 Management of FIA_SOS.1

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

a) the management of the metric used to verify the secrets.

12.5.4 Management of FIA_SOS.2

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

a) the management of the metric used to generate the secrets.

12.5.5 Audit of FIA_SOS.1, FIA_SOS.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Rejection by the TSF of any tested secret;

b) basic: Rejection or acceptance by the TSF of any tested secret;

c) detailed: Identification of any changes to the defined quality metrics.

12.5.6 FIA_SOS.1 Verification of secrets

Component relationships

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

12.5.7 FIA_SOS.2 TSF Generation of secrets

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.2.1

The TSF shall provide a mechanism to **generate** secrets that meet [assignment: *a defined quality metric*].

FIA_SOS.2.2

The TSF shall be able to enforce the use of TSF generated secrets for [assignment: *list of TSF functions*].

12.6 User authentication (FIA_UAU)

12.6.1 Family behaviour

This family defines the types of user authentication mechanisms supported by the TSF. This family also defines the required attributes on which the user authentication mechanisms be based.

12.6.2 Components leveling and description

Figure 43 shows the component leveling for this family.

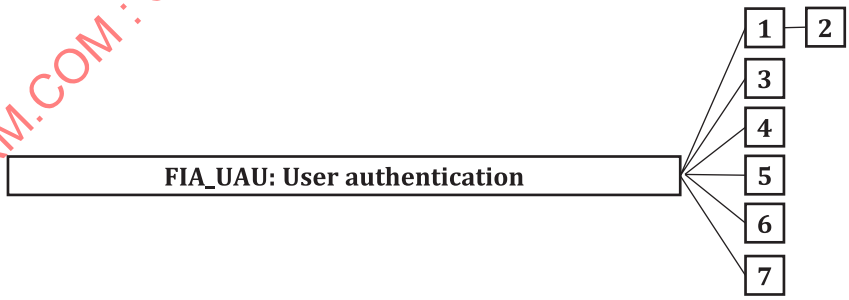


Figure 43 — FIA_UAU: Component leveling

FIA_UAU.1 Timing of authentication, allows a user to perform certain actions prior to the authentication of the user's identity.

FIA_UAU.2 User authentication before any action, requires that users are authenticated before any other action will be allowed by the TSF.

FIA_UAU.3 Unforgeable authentication, requires the authentication mechanism to be able to detect and prevent the use of authentication data that has been forged or copied.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FIA_UAU.4 Single-use authentication mechanisms, requires an authentication mechanism that operates with single-use authentication data.

FIA_UAU.5 Multiple authentication mechanisms, requires that different authentication mechanisms be provided and used to authenticate user identities for specific events.

FIA_UAU.6 Re-authenticating, requires the ability to specify events for which the user needs to be re-authenticated.

FIA_UAU.7 Protected authentication feedback, requires that only limited feedback information is provided to the user during the authentication.

12.6.3 Management of FIA_UAU.1

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

a) management of the authentication data by an administrator;

b) management of the authentication data by the associated user;

c) managing the list of actions that can be taken before the user is authenticated.

12.6.4 Management of FIA_UAU.2

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

a) management of the authentication data by an administrator;

b) management of the authentication data by the user associated with this data.

12.6.5 Management of FIA_UAU.3, FIA_UAU.4, FIA_UAU.7

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

a) there are no management activities foreseen.

12.6.6 Management of FIA_UAU.5

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

a) the management of authentication mechanisms.

12.6.7 Management of FIA_UAU.6

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

a) if an authorized administrator can request re-authentication, the management includes a re-authentication request.

12.6.8 Management of FIA_UAU.7

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

a) the management of the rules for authentication.

12.6.9 Audit of FIA_UAU.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Unsuccessful use of the authentication mechanism;

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

b) basic: All use of the authentication mechanism;

c) detailed: All TSF mediated actions performed before authentication of the user.

12.6.10 Audit of FIA_UAU.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Unsuccessful use of the authentication mechanism;

b) basic: All use of the authentication mechanism.

12.6.11 Audit of FIA_UAU.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Detection of fraudulent authentication data;

b) basic: All immediate measures taken and results of checks on the fraudulent data.

12.6.12 Audit of FIA_UAU.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Attempts to reuse authentication data.

12.6.13 Audit of FIA_UAU.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The final decision on authentication;

b) basic: The result of each activated mechanism together with the final decision.

12.6.14 Audit of FIA_UAU.6

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Failure of re-authentication;

b) basic: All re-authentication attempts.

12.6.15 Audit of FIA_UAU.7

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) well-formedness of rules regarding the semantics of rule-set;

b) basic: verification of enforceability of rules.

12.6.16 FIA_UAU.1 Timing of authentication

Component relationships

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1

The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

12.6.17 FIA_UAU.2 User authentication before any action

Component relationships

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

12.6.18 FIA_UAU.3 Unforgeable authentication

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.3.1

The TSF shall [selection: *detect, prevent*] use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2

The TSF shall [selection: *detect, prevent*] use of authentication data that has been copied from any other user of the TSF.

12.6.19 FIA_UAU.4 Single-use authentication mechanisms

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.4.1

The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanism(s)*].

12.6.20 FIA_UAU.5 Multiple authentication mechanisms

Component relationships

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1

The TSF shall provide [assignment: *list of multiple authentication mechanisms*] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication*].

12.6.21 FIA_UAU.6 Re-authenticating

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.6.1

The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].

12.6.22 FIA_UAU.7 Protected authentication feedback

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1

The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

12.7 User identification (FIA_UID)

12.7.1 Family behaviour

This family defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification.

12.7.2 Components leveling and description

Figure 44 shows the component leveling for this family.

Figure 44 — FIA_UID: Component leveling

FIA_UID.1 Timing of identification, allows users to perform certain actions before being identified by the TSF.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FIA_UID.2 User identification before any action, requires that users identify themselves before any action will be allowed by the TSF.

12.7.3 Management of FIA_UID.1

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

a) the management of the user identities;

b) if an authorized administrator can change the actions allowed before identification, the managing of the action lists.

12.7.4 Management of FIA_UID.2

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

a) the management of the user identities.

12.7.5 Audit of FIA_UID.1, FIA_UID.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Unsuccessful use of the user identification mechanism, including the user identity provided;

b) basic: All use of the user identification mechanism, including the user identity provided.

12.7.6 FIA_UID.1 Timing of identification

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1

The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

12.7.7 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1

The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

12.8 User-subject binding (FIA_USB)

12.8.1 Family behaviour

An authenticated user, in order to use the TOE, typically activates a subject. The user's security attributes are associated (totally or partially) with this subject. This family defines requirements to create and maintain the association of the user's security attributes to a subject acting on the user's behalf.

12.8.2 Components leveling and description

Figure 45 shows the component leveling for this family.

Figure 45 — FIA_USB: Component leveling

FIA_USB.1 User-subject binding, requires the specification of any rules governing the association between user attributes and the subject attributes into which they are mapped.

12.8.3 Management of FIA_USB.1

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

a) an authorized administrator can define default subject security attributes;

b) an authorized administrator can change subject security attributes.

12.8.4 Audit of FIA_USB.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Unsuccessful binding of user security attributes to a subject;

b) basic: Success and failure of binding of user security attributes to a subject.

12.8.5 FIA_USB.1 User-subject binding

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

FIA_USB.1.2

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

13 Class FMT: Security management

13.1 Class description

This class is intended to specify the management of several aspects of the TSF: security attributes, TSF data and functions. The different management roles and their interaction, such as separation of capability, can be specified.

This class has the following objectives:

a) management of TSF data;

b) management of security attributes;

c) management of functions of the TSF;

d) definition of security roles.

Figure 46 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex H provides explanatory information for this class and should be consulted when using the components identified in this class.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

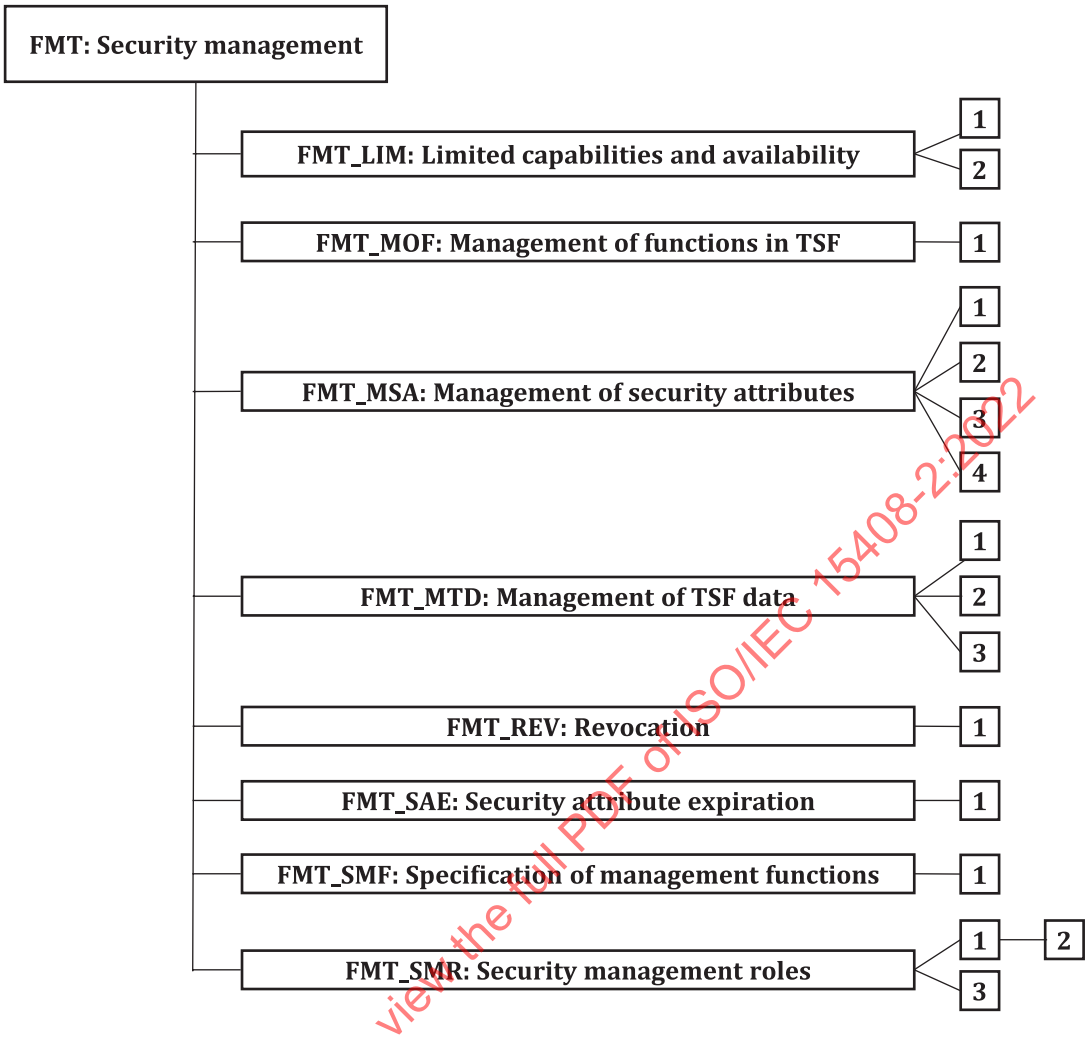


Figure 46 — FMT: Security management class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

13.2 Limited capabilities and availability (FMT_LIM)

13.2.1 Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner.

NOTE FDP_ACF restricts the access to functions whereas the component Limited Capability of this family requires the functions themselves to be designed in a specific manner.

13.2.2 Components leveling and description

Figure 47 shows the component leveling for this family.

Figure 47 — FMT_LIM: Component leveling

FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

© ISO/IEC 2022 – All rights reserved

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

13.2.3 Management of FMT_LIM.1, FMT_LIM.2

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

a) there are no management activities foreseen.

13.2.4 Audit of FMT_LIM.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

13.2.5 FMT_LIM.1 Limited capabilities

Component relationships

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability

FMT_LIM.1.1

The TSF shall limit its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: Limited capability and availability policy].

13.2.6 FMT_LIM.2 Limited availability

Component relationships

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities

FMT_LIM.2.1

The TSF shall be designed in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: *Limited capability and availability policy*].

13.3 Management of functions in TSF (FMT_MOF)

13.3.1 Family behaviour

This family allows authorized users to control over the management of functions in the TSF.

13.3.2 Components leveling and description

Figure 48 shows the component leveling for this family.

Figure 48 — FMT_MOF: Component leveling

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FMT_MOF.1 Management of security functions behaviour allows the authorized users (roles) to manage the behaviour of functions in the TSF that use rules or have specified conditions that may be manageable.

13.3.3 Management of FMT_MOF.1

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

a) managing the group of roles that can interact with the functions in the TSF.

13.3.4 Audit of FMT_MOF.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: All modifications in the behaviour of the functions in the TSF.

13.3.5 FMT_MOF.1 Management of security functions behaviour

Component relationships

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1

The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

13.4 Management of security attributes (FMT_MSA)

13.4.1 Family behaviour

This family allows authorized users control over the management of security attributes. This management can include capabilities for viewing and modifying of security attributes.

13.4.2 Components leveling and description

Figure 49 shows the component leveling for this family.

Figure 49 — FMT_MSA: Component leveling

FMT_MSA.1 Management of security attributes allows authorized users (roles) to manage the specified security attributes.

FMT_MSA.2 Secure security attributes ensures that values assigned to security attributes are valid with respect to the secure state.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FMT_MSA.3 Static attribute ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

FMT_MSA.4 Security attribute value inheritance allows the rules/policies to be specified that will dictate the value to be inherited by a security attribute.

13.4.3 Management of FMT_MSA.1

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

a) managing the group of roles that can interact with the security attributes;

b) management of rules by which security attributes inherit specified values.

13.4.4 Management of FMT_MSA.2

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

a) management of rules by which security attributes inherit specified values.

13.4.5 Management of FMT_MSA.3

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

a) managing the group of roles that can specify initial values;

b) managing the permissive or restrictive setting of default values for a given access control SFP;

c) management of rules by which security attributes inherit specified values.

13.4.6 Management of FMT_MSA.4

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

a) specification of the role permitted to establish or modify security attributes.

13.4.7 Audit of FMT_MSA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: All modifications of the values of security attributes.

13.4.8 Audit of FMT_MSA.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: All offered and rejected values for a security attribute;

b) detailed: All offered and accepted secure values for a security attribute.

13.4.9 Audit of FMT_MSA.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Modifications of the default setting of permissive or restrictive rules;

b) basic: All modifications of the initial values of security attributes.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

13.4.10 Audit of FMT_MSA.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Modifications of security attributes, possibly with the old and/or values of security attributes that were modified.

13.4.11 FMT_MSA.1 Management of security attributes

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1

The TSF shall enforce the [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].

13.4.12 FMT_MSA.2 Secure security attributes

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for [assignment: *list of security attributes*].

13.4.13 FMT_MSA.3 Static attribute initialization

Component relationships

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.3.1

The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

13.4.14 FMT_MSA.4 Security attribute value inheritance

Component relationships

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_MSA.4.1

The TSF shall use the following rules to set the value of security attributes: [assignment: *rules for setting the values of security attributes*].

13.5 Management of TSF data (FMT_MTD)

13.5.1 Family behaviour

This family allows authorized users (roles) control over the management of TSF data.

13.5.2 Components leveling and description

Figure 50 shows the component leveling for this family.

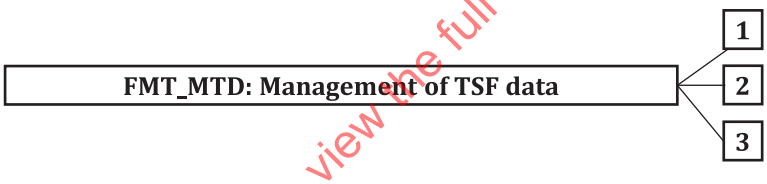


Figure 50 — FMT_MTD: Component leveling

FMT_MTD.1 Management of TSF data allows authorized users to manage TSF data.

FMT_MTD.2 Management of limits on TSF data specifies the action to be taken if limits on TSF data are reached or exceeded.

FMT_MTD.3 Secure TSF data ensures that values assigned to TSF data are valid with respect to the secure state.

13.5.3 Management of FMT_MTD.1

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

a) managing the group of roles that can interact with the TSF data.

13.5.4 Management of FMT_MTD.2

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

a) managing the group of roles that can interact with the limits on the TSF data.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

13.5.5 Management of FMT_MTD.3

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

a) there are no management activities foreseen.

13.5.6 Audit of FMT_MTD.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: All modifications to the values of TSF data.

13.5.7 Audit of FMT_MTD.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: All modifications to the limits on TSF data;

b) basic: All modifications in the actions to be taken in case of violation of the limits.

13.5.8 Audit of FMT_MTD.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: All rejected values of TSF data.

13.5.9 FMT_MTD.1 Management of TSF data

Component relationships

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1

The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].

13.5.10 FMT_MTD.2 Management of limits on TSF data

Component relationships

Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of TSF data FMT_SMR.1 Security roles

FMT_MTD.2.1

The TSF shall restrict the specification of the limits for [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].

FMT_MTD.2.2

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [assignment: *actions to be taken*].

13.5.11 FMT_MTD.3 Secure TSF data

Component relationships

Hierarchical to: No other components.

Dependencies: FMT_MTD.1 Management of TSF data

FMT_MTD.3.1

The TSF shall ensure that only secure values are accepted for [assignment: *list of TSF data*].

13.6 Revocation (FMT_REV)

13.6.1 Family behaviour

This family addresses revocation of security attributes for a variety of entities within a TOE.

13.6.2 Components leveling and description

Figure 51 shows the component leveling for this family.

Figure 51 — FMT_REV: Component leveling

FMT_REV.1 Revocation provides for revocation of security attributes to be enforced at some point in time.

13.6.3 Management of FMT_REV.1

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

a) managing the group of roles that can invoke revocation of security attributes;

b) managing the lists of users, subjects, objects, and other resources for which revocation is possible;

c) managing the revocation rules.

13.6.4 Audit of FMT_REV.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Unsuccessful revocation of security attributes;

b) basic: All attempts to revoke security attributes.

13.6.5 FMT_REV.1 Revocation

Component relationships

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FMT_REV.1.1

The TSF shall restrict the ability to revoke [assignment: *list of security attributes*] associated with the [selection: *users, subjects, objects, [assignment: other additional resources]*] under the control of the TSF to [assignment: *the authorized identified roles*].

FMT_REV.1.2

The TSF shall enforce the rules [assignment: *specification of revocation rules*].

13.7 Security attribute expiration (FMT_SAE)

13.7.1 Family behaviour

This family addresses the capability to enforce time limits for the validity of security attributes.

13.7.2 Components leveling and description

Figure 52 shows the component leveling for this family.

Figure 52 — FMT_SAE: Component leveling

FMT_SAE.1 Time-limited authorization provides the capability for an authorized user to specify an expiration time on specified security attributes.

13.7.3 Management of FMT_SAE.1

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

a) managing the list of security attributes for which expiration is to be supported;

b) the actions to be taken if the expiration time has passed.

13.7.4 Audit of FMT_SAE.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Specification of the expiration time for an attribute;

b) basic: Action taken due to attribute expiration.

13.7.5 FMT_SAE.1 Time-limited authorization

Component relationships

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FPT_STM.1 Reliable time stamps

FMT_SAE.1.1

The TSF shall restrict the capability to specify an expiration time for [assignment: *list of security attributes for which expiration is to be supported*] to [assignment: *the authorized identified roles*].

FMT_SAE.1.2

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed.

13.8 Specification of Management Functions (FMT_SMF)

13.8.1 Family behaviour

This family allows the specification of the management functions to be provided by the TOE. Management functions provide TSFI that allow administrators to define the parameters that control the operation of security-related aspects of the TOE, such as data protection attributes, TOE protection attributes, audit attributes, and identification and authentication attributes. Management functions also include those functions performed by an operator to ensure continued operation of the TOE, such as backup and recovery. This family works in conjunction with the other components in the FMT: Security management class: the component in this family calls out the management functions, and other families in FMT: Security management restricts the ability to use these management functions.

13.8.2 Components leveling and description

Figure 53 shows the component leveling for this family.

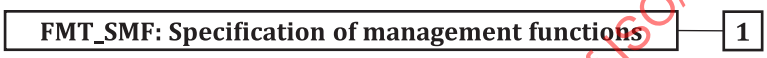


Figure 53 — FMT_SMF: Component leveling

FMT_SMF.1 Specification of Management Functions requires that the TSF provide specific management functions.

13.8.3 Management of FMT_SMF.1

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

a) there are no management activities foreseen.

13.8.4 Audit of FMT_SMF.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Use of the management functions.

13.8.5 FMT_SMF.1 Specification of Management Functions

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

13.9 Security management roles (FMT_SMR)

13.9.1 Family behaviour

This family is intended to control the assignment of different roles to users. The capabilities of these roles with respect to security management are described in the other families in this class.

13.9.2 Components leveling and description

Figure 54 shows the component leveling for this family.

Figure 54 — FMT_SMR: Component leveling

FMT_SMR.1 Security roles specifies the roles with respect to security that the TSF recognizes.

FMT_SMR.2 Restrictions on security roles specifies that in addition to the specification of the roles, there are rules that control the relationship between the roles.

FMT_SMR.3 Assuming roles, requires that an explicit request is given to the TSF to assume a role.

13.9.3 Management of FMT_SMR.1

The following actions can be considered for the management functions in FMT_SMR.1:

a) managing the group of users that are part of a role.

13.9.4 Management of FMT_SMR.2

The following actions can be considered for the management functions in FMT_SMR.2:

a) managing the group of users that are part of a role;

b) managing the conditions that the roles must satisfy.

13.9.5 Management of FMT_SMR.3

The following actions can be considered for the management functions in FMT_SMR.3:

a) there are no management activities foreseen.

13.9.6 Audit of FMT_SMR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: modifications to the group of users that are part of a role;

b) detailed: every use of the rights of a role.

13.9.7 Audit of FMT_SMR.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: modifications to the group of users that are part of a role;

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

b) minimal: unsuccessful attempts to use a role due to the given conditions on the roles;

c) detailed: every use of the rights of a role.

13.9.8 Audit of FMT_SMR.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Explicit request to assume a role.

13.9.9 FMT_SMR.1 Security roles

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [assignment: *the authorized identified roles*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

13.9.10 FMT_SMR.2 Restrictions on security roles

Component relationships

Hierarchical to: FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.2.1

The TSF shall maintain the roles: [assignment: ***authorized*** *identified roles*].

FMT_SMR.2.2

The TSF shall be able to associate users with roles.

FMT_SMR.2.3

The TSF shall ensure that the conditions [assignment: *conditions for the different roles*] are satisfied.

13.9.11 FMT_SMR.3 Assuming roles

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMR.3.1

The TSF shall require an explicit request to assume the following roles: [assignment: *the roles*].

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

14 Class FPR: Privacy

14.1 Class description

This class contains privacy requirements. These requirements provide a user protection against discovery and misuse of identity by other users.

Figure 55 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex I provides explanatory information for this class and should be consulted when using the components identified in this class.

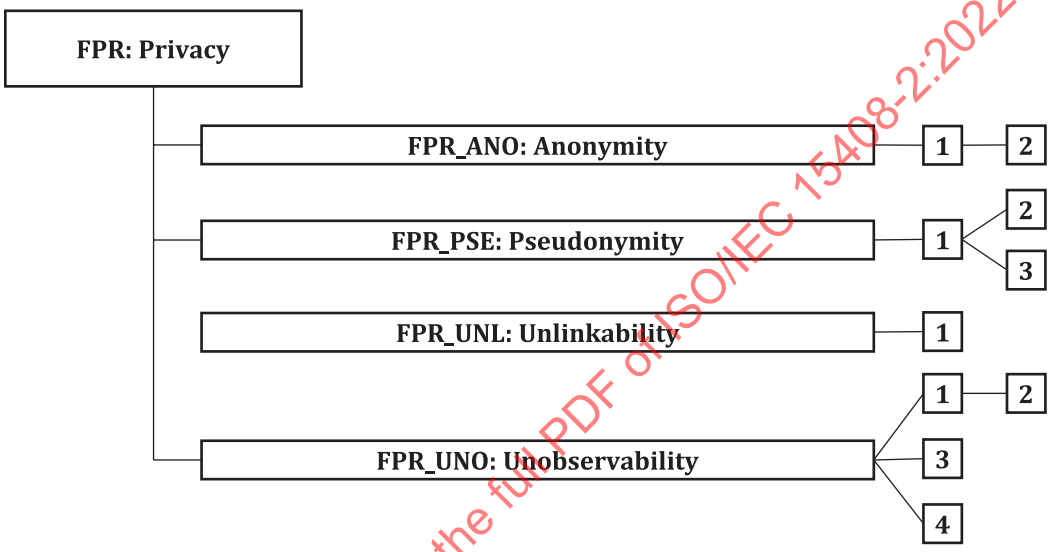


Figure 55 — FPR: Privacy class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

14.2 Anonymity (FPR_ANO)

14.2.1 Family behaviour

This family ensures that a user can use a resource or service without disclosing the user's identity. The requirements for anonymity provide protection of the user identity. Anonymity is not intended to protect the subject identity.

14.2.2 Components leveling and description

Figure 56 shows the component leveling for this family.

Figure 56 — FPR_ANO: Component leveling

FPR_ANO.1 Anonymity, requires that other users or subjects are unable to determine the identity of a user bound to a subject or operation.

FPR_ANO.2 Anonymity without soliciting information enhances the requirements of FPR_ANO.1 Anonymity by ensuring that the TSF does not ask for the user identity.

© ISO/IEC 2022 – All rights reserved

14.2.3 Management of FPR_ANO.1, FPR_ANO.2

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

a) there are no management activities foreseen.

14.2.4 Audit of FPR_ANO.1, FPR_ANO.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The invocation of the anonymity mechanism.

14.2.5 FPR_ANO.1 Anonymity

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPR_ANO.1.1

The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine the real user name bound to [assignment: *list of subjects and/or operations and/or objects*].

14.2.6 FPR_ANO.2 Anonymity without soliciting information

Component relationships

Hierarchical to: FPR_ANO.1 Anonymity

Dependencies: No dependencies.

FPR_ANO.2.1

The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine the real user name bound to [assignment: *list of subjects and/or operations and/or objects*].

FPR_ANO.2.2

The TSF shall provide [assignment: *list of services*] to [assignment: *list of subjects*] without soliciting any reference to the real user name.

14.3 Pseudonymity (FPR_PSE)

14.3.1 Family behaviour

This family ensures that a user may use a resource or service without disclosing its user identity but can still be accountable for that use.

14.3.2 Components leveling and description

Figure 57 shows the component leveling for this family.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Figure 57 — FPR_PSE: Component leveling

FPR_PSE.1 Pseudonymity requires that a set of users and/or subjects are unable to determine the identity of a user bound to a subject or operation, but that this user is still accountable for its actions.

FPR_PSE.2 Reversible pseudonymity, requires the TSF to provide a capability to determine the original user identity based on a provided alias.

FPR_PSE.3 Alias pseudonymity, requires the TSF to follow certain construction rules for the alias to the user identity.

14.3.3 Management of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3

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

a) there are no management activities foreseen.

14.3.4 Audit of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The subject/user that requested resolution of the user identity should be audited.

14.3.5 FPR_PSE.1 Pseudonymity

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPR_PSE.1.1

The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine the real user name bound to [assignment: *list of subjects and/or operations and/or objects*].

FPR_PSE.1.2

The TSF shall be able to provide [assignment: *number of aliases*] aliases of the real user name to [assignment: *list of subjects*].

FPR_PSE.1.3

The TSF shall [selection, choose one of: *determine an alias for a user, accept the alias from the user*] and verify that it conforms to the [assignment: *alias metric*].

14.3.6 FPR_PSE.2 Reversible pseudonymity

Component relationships

Hierarchical to: FPR_PSE.1 Pseudonymity

Dependencies: FIA_UID.1 Timing of identification

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FPR_PSE.2.1

The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine the real user name bound to [assignment: *list of subjects and/or operations and/or objects*].

FPR_PSE.2.2

The TSF shall be able to provide [assignment: *number of aliases*] aliases of the real user name to [assignment: *list of subjects*].

FPR_PSE.2.3

The TSF shall [selection, choose one of: *determine an alias for a user, accept the alias from the user*] and verify that it conforms to the [assignment: *alias metric*].

FPR_PSE.2.4

The TSF shall provide [selection: *an authorized user, [assignment: list of trusted subjects]*] a capability to determine the user identity based on the provided alias only under the following [assignment: *list of conditions*].

14.3.7 FPR_PSE.3 Alias pseudonymity

Component relationships

Hierarchical to: FPR_PSE.1 Pseudonymity

Dependencies: No dependencies.

FPR_PSE.3.1

The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine the real user name bound to [assignment: *list of subjects and/or operations and/or objects*].

FPR_PSE.3.2

The TSF shall be able to provide [assignment: *number of aliases*] aliases of the real user name to [assignment: *list of subjects*].

FPR_PSE.3.3

The TSF shall [selection, choose one of: *determine an alias for a user, accept the alias from the user*] and verify that it conforms to the [assignment: *alias metric*].

FPR_PSE.3.4

The TSF shall provide an alias to the real user name which shall be identical to an alias provided previously under the following [assignment: *list of conditions*] otherwise the alias provided shall be unrelated to previously provided aliases.

14.4 Unlinkability (FPR_UNL)

14.4.1 Family behaviour

This family ensures that selected entities can be linked together without external entities being able to back trace these links.

14.4.2 Components leveling and description

Figure 58 shows the component leveling for this family.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Figure 58 — FPR_UNL: Component leveling

FPR_UNL.1 Unlinkability of operations requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system, or whether operations are related in some other manner. This component ensures that users cannot link different operations in the system and thereby obtain information.

14.4.3 Management of FPR_UNL.1

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

a) the management of the unlinkability function.

14.4.4 Audit of FPR_UNL.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The invocation of the unlinkability mechanism.

14.4.5 FPR_UNL.1 Unlinkability of operations

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPR_UNL.1.1

The TSF shall ensure that [assignment: *set of entities and/or operations*] are unable to determine whether [assignment: *list of entities and/or operations*] [selection: *were caused by the same user, are related as follows [assignment: list of relations]*].

NOTE This SFR does not only stipulate at the individual set of operations performed by one entity. This SFR intends to look at a chain of interlinked operations by multiple entities. This chain can be subsumed as a transaction.

14.5 Unobservability (FPR_UNO)

14.5.1 Family behaviour

This family ensures that a user can use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

14.5.2 Components leveling and description

Figure 59 shows the component leveling for this family.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

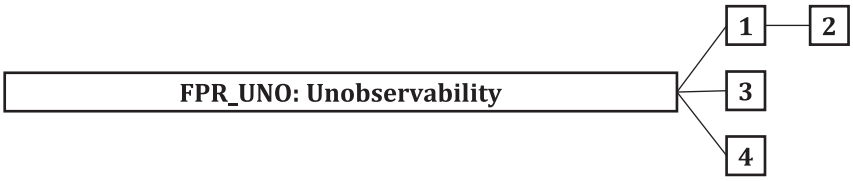


Figure 59 — FPR_UNO: Component leveling

FPR_UNO.1 Unobservability, requires that users and/or subjects cannot determine whether an operation is being performed.

FPR_UNO.2 Allocation of information impacting unobservability, requires that the TSF provide specific mechanisms to avoid the concentration of privacy related information within the TOE. Such concentrations can impact unobservability if a security compromise occurs.

FPR_UNO.3 Unobservability without soliciting information, requires that the TSF does not try to obtain privacy related information that can be used to compromise unobservability.

FPR_UNO.4 Authorized user observability, requires the TSF to provide one or more authorized users with a capability to observe the usage of resources and/or services.

14.5.3 Management of FPR_UNO.1, FPR_UNO.2

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

a) the management of the behaviour of the unobservability function.

14.5.4 Management of FPR_UNO.3

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

a) there are no management activities foreseen.

14.5.5 Management of FPR_UNO.4

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

a) the list of authorized users that are capable of determining the occurrence of operations.

14.5.6 Audit of FPR_UNO.1, FPR_UNO.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The invocation of the unobservability mechanism.

14.5.7 Audit of FPR_UNO.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

14.5.8 Audit of FPR_UNO.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The observation of the use of a resource or service by a user or subject.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

14.5.9 FPR_UNO.1 Unobservability

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPR_UNO.1.1

The TSF shall ensure that [assignment: *list of users and/or subjects*] are unable to observe the operation [assignment: *list of operations*] on [assignment: *list of objects*] by [assignment: *list of protected users and/or subjects*].

14.5.10 FPR_UNO.2 Allocation of information impacting unobservability

Component relationships

Hierarchical to: FPR_UNO.1 Unobservability

Dependencies: No dependencies.

FPR_UNO.2.1

The TSF shall ensure that [assignment: *list of users and/or subjects*] are unable to observe the operation [assignment: *list of operations*] on [assignment: *list of objects*] by [assignment: *list of protected users and/or subjects*].

FPR_UNO.2.2

The TSF shall allocate the [assignment: *unobservability related information*] among different parts of the TOE such that the following conditions hold during the lifetime of the information: [assignment: *list of conditions*].

14.5.11 FPR_UNO.3 Unobservability without soliciting information

Component relationships

Hierarchical to: No other components.

Dependencies: FPR_UNO.1 Unobservability

FPR_UNO.3.1

The TSF shall provide [assignment: *list of services*] to [assignment: *list of subjects*] without soliciting any reference to [assignment: *privacy related information*].

14.5.12 FPR_UNO.4 Authorized user observability

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPR_UNO.4.1

The TSF shall provide [assignment: *set of authorized users*] with the capability to observe the usage of [assignment: *list of resources and/or services*].

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15 Class FPT: Protection of the TSF

15.1 Class description

This class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data. Although families in this class appear to duplicate components in the FDP: User data protection class, and they can be implemented using the same mechanisms. However, FDP: User data protection focuses on user data protection, while FPT: Protection of the TSF focuses on TSF data protection. In fact, Components from the FPT: Protection of the TSF class are necessary to provide requirements that the SFPs in the TOE cannot be tampered with or bypassed.

From the point of view of this class, regarding to the TSF there are three significant elements:

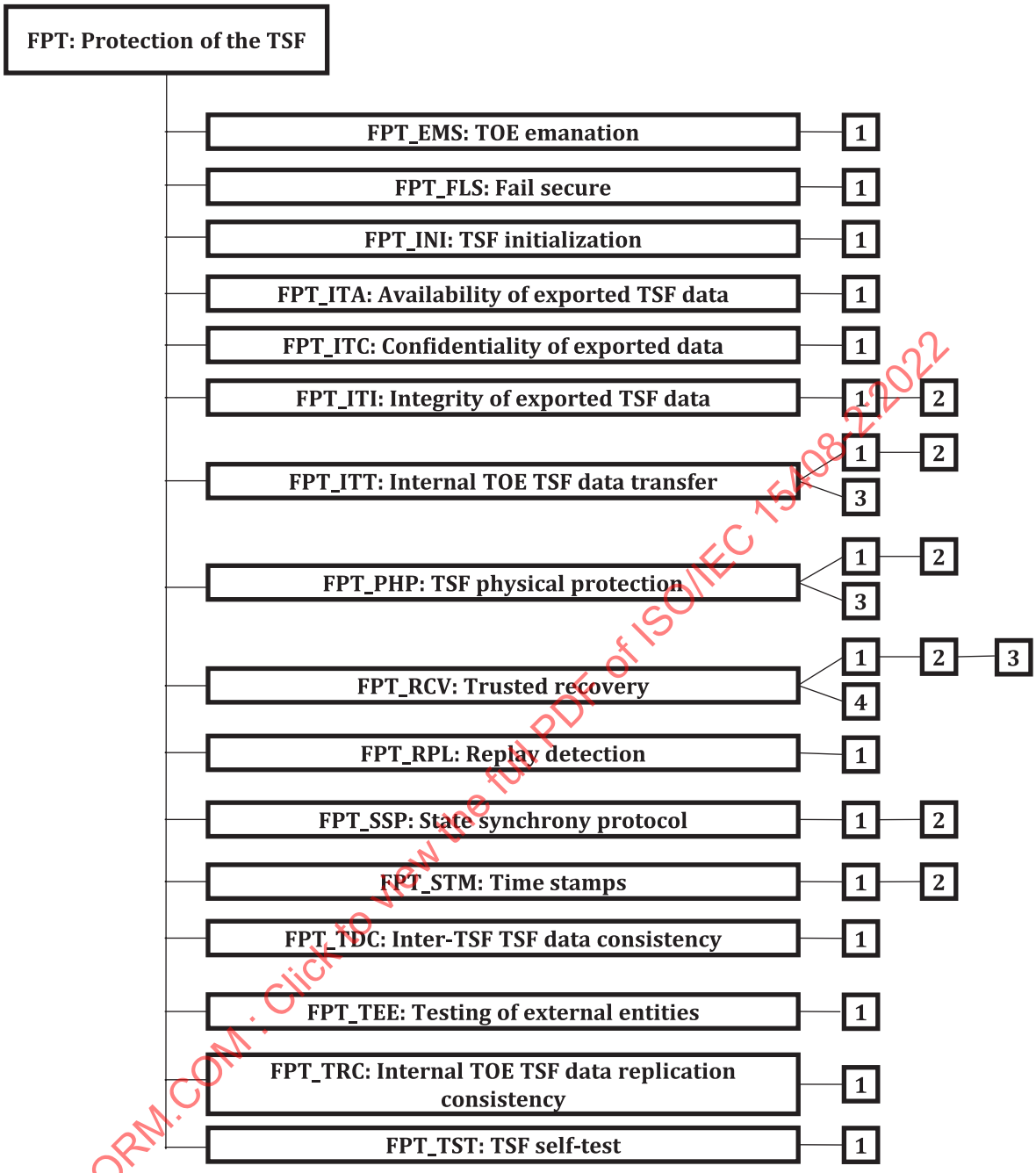
a) the TSF's implementation, which executes and implements the mechanisms that enforce the SFRs;

b) the TSF's data, which are the administrative databases that guide the enforcement of the SFRs;

c) the external entities that the TSF may interact with in order to enforce the SFRs.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved



IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

Figure 60 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex J provides explanatory information for this class and should be consulted when using the components identified in this class.

© ISO/IEC 2022 – All rights reserved

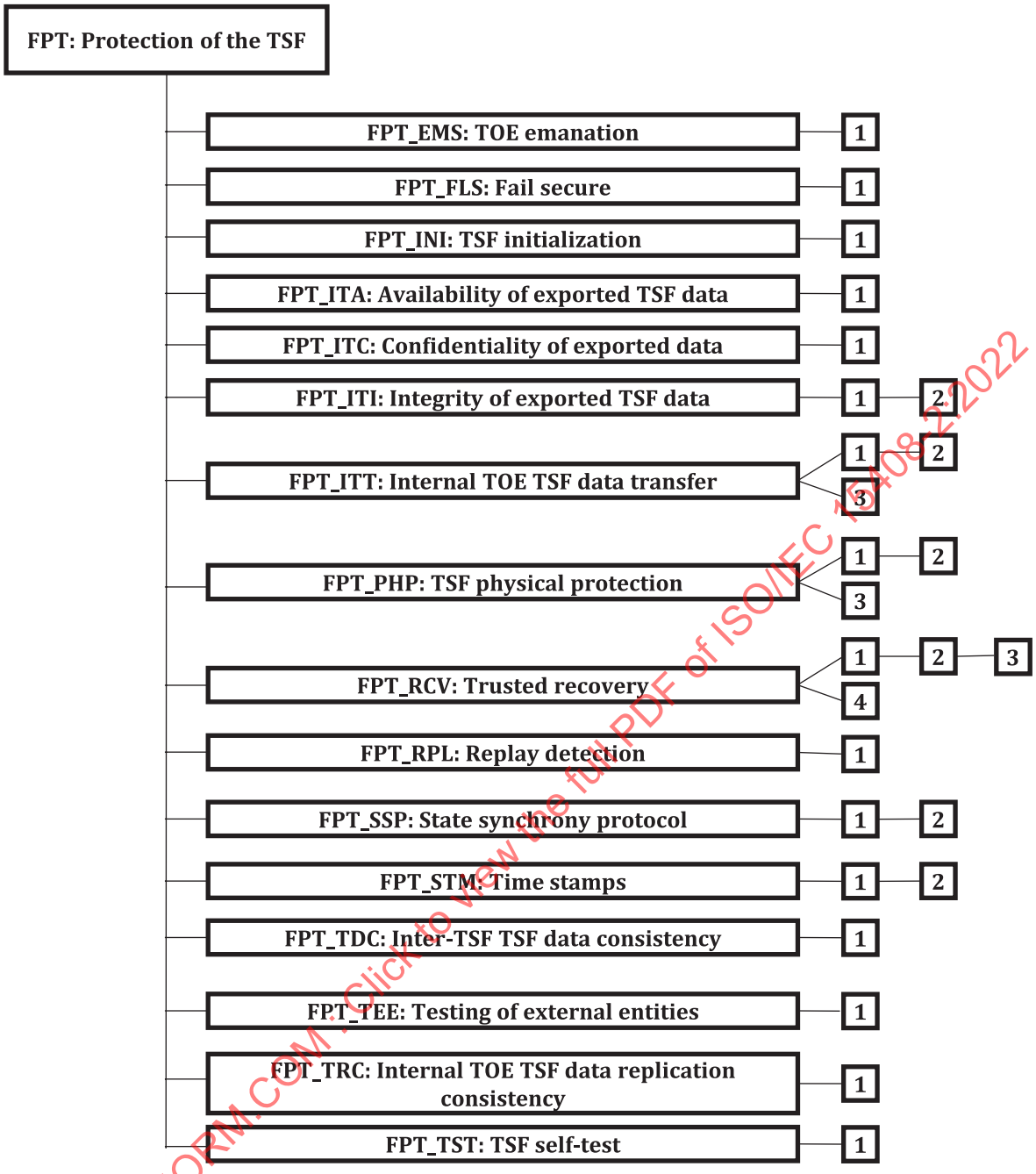


Figure 60 — FPT: Protection of the TSF class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

15.2 TOE emanation (FPT_EMS)

15.2.1 Family behaviour

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) describes the IT SFRs of the TOE related to leakage of information based on emanation.

If the TOE must prevent attacks against the TOE and secret data processed by the TOE where the attack is based on external observable phenomena of the TOE during its operation, different types of emissions and interfaces of the TOE as well as different types of TSF data and user data can be addressed.

EXAMPLE

© ISO/IEC 2022 – All rights reserved

Examples of such attacks against the TOE and its processed secret data are simple power analysis (SPA), differential power analysis (DPA), simple electromagnetic analysis (SEMA), differential electromagnetic analysis (DEMA), timing attacks, padding oracle attacks, cache miss attacks.

This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of this document.

15.2.2 Components leveling and description

Figure 61 shows the component leveling for this family.

Figure 61 — FPT_EMS: Component leveling

This family consists of one component, FPT_EMS.1 Emanation of TSF and User data, which defines requirements for the TOE to mitigate intelligible emanations.

15.2.3 Management of FPT_EMS.1

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

a) there are no management activities foreseen.

15.2.4 Audit of FPT_EMS.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

15.2.5 FPT_EMS.1 Emanation of TSF and User data

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1

The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in Table 1:

Table 1 — FPT_EMS.1.1 Table

ID	Emissions	attack surface	TSF data	User data
1	[assignment: *list of types of emissions*]	[assignment: *list of types of attack surface*]	[assignment: *list of types of TSF data*]	[assignment: *list of types of user data*]
...	...	...	...	...

15.3 Fail secure (FPT_FLS)

15.3.1 Family behaviour

The requirements of this family ensure that the TOE will always enforce its SFRs in the event of identified categories of failures in the TSF.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.3.2 Components leveling and description

Figure 62 shows the component leveling for this family.

Figure 62 — FPT_FLS: Component leveling

This family consists of only one component, FPT_FLS.1 Failure with preservation of secure state, which requires that the TSF preserve a secure state in the face of the identified failures.

15.3.3 Management of FPT_FLS.1

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

a) there are no management activities foreseen.

15.3.4 Audit of FPT_FLS.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or /ST:

a) basic: Failure of the TSF.

15.3.5 FPT_FLS.1 Failure with preservation of secure state

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*].

15.4 TSF initialization (FPT_INI)

15.4.1 Family behaviour

This family describes the functional requirements for the initialization of the TSF by a dedicated function of the TOE that ensures the initialization in a correct and secure operational state.

15.4.2 Components leveling and description

Figure 63 shows the component leveling for this family.

Figure 63 — FPT_INI: Component leveling

This family consists of only one component, Component FPT_INI.1. This component requires the TOE to provide a TSF initialization function that brings the TSF into a secure operational state at power-on.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.4.3 Management of FPT_INI.1

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

a) there are no management activities foreseen.

15.4.4 Audit of FPT_INI.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

15.4.5 FPT_INI.1 TSF initialization

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_INI.1.1

The TOE shall provide an initialization function which is self-protected for integrity and authenticity.

FPT_INI.1.2

The TOE initialization function shall ensure that certain properties hold on certain elements immediately before establishing the TSF in a secure initial state, as specified in Table 2:

Table 2 — FPT_INI.1.2 Table

ID	Properties	Elements
1	[assignment: *property, for instance authenticity, integrity, correct version*]	[assignment: *list of TSF/user firmware, software or data*]
...	...	...

FPT_INI.1.3

The TOE initialization function shall detect and respond to errors and failures during initialization such that the TOE [selection: *is halted, successfully completes initialization with [selection: reduced functionality, signaling error state, [assignment: list of actions]*].

FPT_INI.1.4

The TOE initialization function shall only interact with the TSF in [assignment: *defined methods*] during initialization.

15.5 Availability of exported TSF data (FPT_ITA)

15.5.1 Family behaviour

This family defines the rules for the prevention of loss of availability of TSF data moving between the TSF and another trusted IT product.

15.5.2 Components leveling and description

Figure 64 shows the component leveling for this family.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Figure 64 — FPT_ITA: Component leveling

This family consists of only one component, FPT_ITA.1 Inter-TSF availability within a defined availability metric. This component requires that the TSF ensure, to an identified degree of probability, the availability of TSF data provided to another trusted IT product.

15.5.3 Management of FPT_ITA.1

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

a) management of the list of types of TSF data that be available to another trusted IT product.

15.5.4 Audit of FPT_ITA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The absence of TSF data when required by a TOE.

15.5.5 FPT_ITA.1 Inter-TSF availability within a defined availability metric

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITA.1.1

The TSF shall ensure the availability of [assignment: *list of types of TSF data*] provided to another trusted IT product within [assignment: *a defined availability metric*] given the following conditions [assignment: *conditions to ensure availability*].

15.6 Confidentiality of exported TSF data (FPT_ITC)

15.6.1 Family behaviour

This family defines the rules for the protection from unauthorized disclosure of TSF data during transmission between the TSF and another trusted IT product.

15.6.2 Components leveling and description

Figure 65 shows the component leveling for this family.

Figure 65 — FPT_ITC: Component leveling

This family consists of only one component, FPT_ITC.1 Inter-TSF confidentiality during transmission, which requires that the TSF ensure that data transmitted between the TSF and another trusted IT product is protected from disclosure while in transit.

IECNORM.COM: Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.6.3 Management of FPT_ITC.1

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

a) there are no management activities foreseen.

15.6.4 Audit of FPT_ITC.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

15.6.5 FPT_ITC.1 Inter-TSF confidentiality during transmission

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITC.1.1

The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

15.7 Integrity of exported TSF data (FPT_ITI)

15.7.1 Family behaviour

This family defines the rules for the protection, from unauthorized modification, of TSF data during transmission between the TSF and another trusted IT product.

15.7.2 Components leveling and description

Figure 66 shows the component leveling for this family.

Figure 66 — FPT_ITI: Component leveling

FPT_ITI.1 Inter-TSF detection of modification, provides the ability to detect modification of TSF data during transmission between the TSF and another trusted IT product, under the assumption that another trusted IT product is cognizant of the mechanism used.

FPT_ITI.2 Inter-TSF detection and correction of modification, provides the ability for another trusted IT product not only to detect modification, but to correct modified TSF data under the assumption that another trusted IT product is cognizant of the mechanism used.

15.7.3 Management of FPT_ITI.1

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

a) there are no management activities foreseen.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.7.4 Management of FPT_ITI.2

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

a) management of the types of TSF data that the TSF tries to correct if modified in transit;

b) management of the types of action that the TSF takes if TSF data is modified in transit.

15.7.5 Audit of FPT_ITI.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: the detection of modification of transmitted TSF data;

b) basic: the action taken upon detection of modification of transmitted TSF data.

15.7.6 Audit of FPT_ITI.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: the detection of modification of transmitted TSF data;

b) basic: the action taken upon detection of modification of transmitted TSF data;

c) basic: the use of the correction mechanism.

15.7.7 FPT_ITI.1 Inter-TSF detection of modification

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITI.1.1

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [assignment: *a defined modification metric*].

FPT_ITI.1.2

The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [assignment: *action to be taken*] if modifications are detected.

15.7.8 FPT_ITI.2 Inter-TSF detection and correction of modification

Component relationships

Hierarchical to: FPT_ITI.1 Inter-TSF detection of modification

Dependencies: No dependencies.

FPT_ITI.2.1

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [assignment: *a defined modification metric*].

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FPT_ITI.2.2

The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [assignment: *action to be taken*] if modifications are detected.

FPT_ITI.2.3

The TSF shall provide the capability to correct [assignment: *type of modification*] of all TSF data transmitted between the TSF and another trusted IT product.

15.8 Internal TOE TSF data transfer (FPT_ITT)

15.8.1 Family behaviour

This family provides requirements that address protection of TSF data when it is transferred between separate parts of a TOE across an internal channel.

15.8.2 Components leveling and description

Figure 67 shows the component leveling for this family.

Figure 67 — FPT_ITT: Component leveling

FPT_ITT.1 Basic internal TSF data transfer protection, requires that TSF data be protected when transmitted between separate parts of the TOE.

FPT_ITT.2 TSF data transfer separation requires that the TSF separate user data from TSF data during transmission.

FPT_ITT.3 TSF data integrity monitoring, requires that the TSF data transmitted between separate parts of the TOE is monitored for identified integrity errors.

15.8.3 Management of FPT_ITT.1

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

a) management of the types of modification against which the TSF should protect;

b) management of the mechanism used to provide the protection of the data in transit between different parts of the TSF.

15.8.4 Management of FPT_ITT.2

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

a) management of the types of modification against which the TSF should protect;

b) management of the mechanism used to provide the protection of the data in transit between different parts of the TSF;

c) management of the separation mechanism.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.8.5 Management of FPT_ITT.3

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

a) management of the types of modification against which the TSF should protect;

b) management of the mechanism used to provide the protection of the data in transit between different parts of the TSF;

c) management of the types of modification of TSF data the TSF should try to detect;

d) management of the actions that will be taken.

15.8.6 Audit of FPT_ITT.1, FPT_ITT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

15.8.7 Audit of FPT_ITT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: the detection of modification of TSF data;

b) basic: the action taken following detection of an integrity error.

15.8.8 FPT_ITT.1 Basic internal TSF data transfer protection

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1

The TSF shall protect TSF data from [selection: *disclosure, modification*] when it is transmitted between separate parts of the TOE.

15.8.9 FPT_ITT.2 TSF data transfer separation

Component relationships

Hierarchical to: FPT_ITT.1 Basic internal TSF data transfer protection

Dependencies: No dependencies.

FPT_ITT.2.1

The TSF shall protect TSF data from [selection: *disclosure, modification*] when it is transmitted between separate parts of the TOE.

FPT_ITT.2.2

The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.8.10 FPT_ITT.3 TSF data integrity monitoring

Component relationships

Hierarchical to: No other components.

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.3.1

The TSF shall be able to detect [selection: modification of data, substitution of data, re-ordering of data, deletion of data, [assignment: other integrity errors]] for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2

Upon detection of a data integrity error, the TSF shall take the following actions: [assignment: *specify the action to be taken*].

15.9 TSF physical protection (FPT_PHP)

15.9.1 Family behaviour

TSF physical protection components refer to restrictions on unauthorized physical access to the TSF, and to the deterrence of, and resistance to, unauthorized physical modification, or substitution of the TSF.

The requirements of components in this family ensure that the TSF is protected from physical tampering and interference. Satisfying the requirements of these components results in the TSF being packaged and used in such a manner that physical tampering is detectable, or resistance to physical tampering is enforced. Without these components, the protection functions of a TSF lose their effectiveness in environments where physical damage cannot be prevented. This family also provides requirements regarding how the TSF shall respond to physical tampering attempts.

15.9.2 Components leveling and description

Figure 68 shows the component leveling for this family.

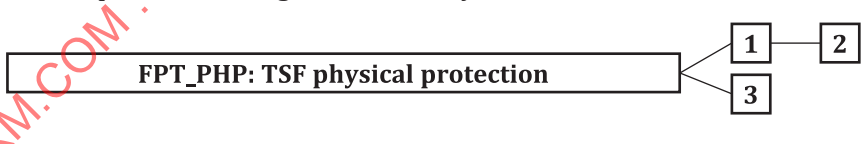


Figure 68 — FPT_PHP: Component leveling

FPT_PHP.1 Passive detection of physical attack, provides for features that indicate when a TSF device or TSF element is subject to tampering. However, notification of tampering is not automatic; an authorized user invokes a security administrative function or perform manual inspection to determine if tampering has occurred.

FPT_PHP.2 Notification of physical attack, provides for automatic notification of tampering for an identified subset of physical penetrations.

FPT_PHP.3 Resistance to physical attack, provides for features that prevent or resist physical tampering with TSF devices and TSF elements.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.9.3 Management of FPT_PHP.1

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

a) management of the user or role that determines whether physical tampering has occurred.

15.9.4 Management of FPT_PHP.2

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

a) management of the user or role that gets informed about intrusions;

b) management of the list of devices that should inform the indicated user or role about the intrusion.

15.9.5 Management of FPT_PHP.3

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

a) management of the automatic responses to physical tampering.

15.9.6 Audit of FPT_PHP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: If detection by IT means, detection of intrusion.

15.9.7 Audit of FPT_PHP.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Detection of intrusion.

15.9.8 Audit of FPT_PHP.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

15.9.9 FPT_PHP.1 Passive detection of physical attack

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1

The TSF shall provide unambiguous detection of physical tampering that can compromise the TSF.

FPT_PHP.1.2

The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.9.10 FPT_PHP.2 Notification of physical attack

Component relationships

Hierarchical to: FPT_PHP.1 Passive detection of physical attack

Dependencies: FMT_LIM.1 Limited capabilities

FPT_PHP.2.1

The TSF shall provide unambiguous detection of physical tampering that can compromise the TSF.

FPT_PHP.2.2

The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3

For [assignment: *list of TSF devices/elements for which active detection is required*], the TSF shall monitor the devices and elements and notify [assignment: *a designated user or role*] when physical tampering with the TSF's devices or TSF's elements has occurred.

15.9.11 FPT_PHP.3 Resistance to physical attack

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1

The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices/elements*] by responding automatically such that the SFRs are always enforced.

15.10 Trusted recovery (FPT_RCV)

15.10.1 Family behaviour

The requirements of this family ensure that the TSF can determine that the TOE is started up without protection compromise and can recover without protection compromise after discontinuity of operations. This family is important because the start-up state of the TSF determines the protection of subsequent states.

15.10.2 Components leveling and description

Figure 69 shows the component leveling for this family.

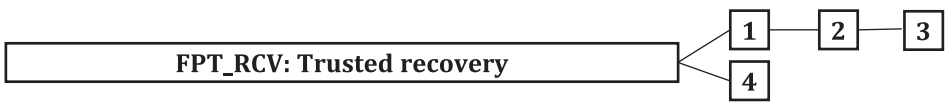


Figure 69 — FPT_RCV: Component leveling

FPT_RCV.1 Manual recovery, allows a TOE to only provide mechanisms that involve human intervention to return to a secure state.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FPT_RCV.2 Automated recovery, provides, for at least one type of service discontinuity, recovery to a secure state without human intervention; recovery for other discontinuities that can require human intervention.

FPT_RCV.3 Automated recovery without undue loss, also provides for automated recovery, but strengthens the requirements by disallowing undue loss of protected objects.

FPT_RCV.4 Function recovery, provides for recovery at the level of particular functions, ensuring either successful completion or rollback of TSF data to a secure state.

15.10.3 Management of FPT_RCV.1

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

a) management of who can access the restore capability within the maintenance mode.

15.10.4 Management of FPT_RCV.2, FPT_RCV.3

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

a) management of who can access the restore capability within the maintenance mode;

b) management of the list of failures/service discontinuities that will be handled through the automatic procedures.

15.10.5 Management of FPT_RCV.4

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

a) there are no management activities foreseen.

15.10.6 Audit of FPT_RCV.1, FPT_RCV.2, FPT_RCV.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) Minimal: the fact that a failure or service discontinuity occurred;

b) Minimal: resumption of the regular operation;

c) Basic: type of failure or service discontinuity.

15.10.7 Audit of FPT_RCV.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: If possible, the impossibility to return to a secure state after a failure of the TSF;

b) basic: If possible, the detection of a failure of a function.

15.10.8 FPT_RCV.1 Manual recovery

Component relationships

Hierarchical to: No other components.

Dependencies: AGD_OPE.1 Operational user guidance

FPT_RCV.1.1

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

After [assignment: *list of failures/service discontinuities*] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

15.10.9 FPT_RCV.2 Automated recovery

Component relationships

Hierarchical to: FPT_RCV.1 Manual recovery

Dependencies: AGD_OPE.1 Operational user guidance

FPT_RCV.2.1

When automated recovery from [assignment: *list of failures/service discontinuities*] **is not possible,** the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.2.2

For [assignment: *list of failures/service discontinuities*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

15.10.10 FPT_RCV.3 Automated recovery without undue loss

Component relationships

Hierarchical to: FPT_RCV.2 Automated recovery

Dependencies: AGD_OPE.1 Operational user guidance

FPT_RCV.3.1

When automated recovery from [assignment: *list of failures/service discontinuities*] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.3.2

For [assignment: *list of failures/service discontinuities*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3

The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: *quantification*] for loss of TSF data or objects under the control of the TSF.

FPT_RCV.3.4

The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

15.10.11 FPT_RCV.4 Function recovery

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_RCV.4.1

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall ensure that [assignment: *list of functions and failure scenarios*] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

15.11 Replay detection (FPT_RPL)

15.11.1 Family behaviour

This family addresses detection of replay for various types of entities and subsequent actions to correct. In the case where replay may be detected, this effectively prevents it.

15.11.2 Components leveling and description

Figure 70 shows the component leveling for this family.

Figure 70 — FPT_RPL: Component leveling

The family consists of only one component, FPT_RPL.1 Replay detection, which requires that the TSF shall be able to detect the replay of identified entities.

15.11.3 Management of FPT_RPL.1

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

a) management of the list of identified entities for which replay is detected;

b) management of the list of actions that need to be taken in case of replay.

15.11.4 Audit of FPT_RPL.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Detected replay attacks;

b) detailed: Action to be taken based on the specific actions.

15.11.5 FPT_RPL.1 Replay detection

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_RPL.1.1

The TSF shall detect replay for the following entities: [assignment: *list of identified entities*].

FPT_RPL.1.2

The TSF shall perform [assignment: *list of specific actions*] when replay is detected.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.12 State synchrony protocol (FPT_SSP)

15.12.1 Family behaviour

Distributed TOEs can give rise to greater complexity than monolithic TOEs through the potential for differences in state between parts of the TOE, and through delays in communication. In most cases synchronization of state between distributed functions involves an exchange protocol, not a simple action. When malice exists in the distributed environment of these protocols, more complex defensive protocols are required.

State synchrony protocol (FPT_SSP) establishes the requirement for certain critical functions of the TSF to use this trusted protocol. State synchrony protocol (FPT_SSP) ensures that two distributed parts of the TOE have synchronized their states after a security-relevant action.

15.12.2 Components leveling and description

Figure 71 shows the component leveling for this family.

Figure 71 — FPT_SSP: Component leveling

FPT_SSP.1 Simple trusted acknowledgement, requires only a simple acknowledgment by the data recipient.

FPT_SSP.2 Mutual trusted acknowledgement, requires mutual acknowledgment of the data exchange.

15.12.3 Management of FPT_SSP.1, FPT_SSP.2

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

a) there are no management activities foreseen.

15.12.4 Audit of FPT_SSP.1, FPT_SSP.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Failure to receive an acknowledgement when expected.

15.12.5 FPT_SSP.1 Simple trusted acknowledgement

Component relationships

Hierarchical to: No other components.

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_SSP.1.1

The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission.

15.12.6 FPT_SSP.2 Mutual trusted acknowledgement

Component relationships

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Hierarchical to: FPT_SSP.1 Simple trusted acknowledgement

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_SSP.2.1

The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission.

FPT_SSP.2.2

The TSF shall ensure that the relevant parts of the TSF know the correct status of transmitted data among its different parts, using acknowledgements.

15.13 Time stamps (FPT_STM)

15.13.1 Family behaviour

This family addresses requirements for a reliable time stamp function within a TOE.

15.13.2 Components leveling and description

Figure 72 shows the component leveling for this family.

Figure 72 — FPR_STM: Component leveling

FPT_STM.1 Reliable time stamps, requires that the TSF provide reliable time stamps for TSF functions.

FPT_STM.2 Time source, requires the description of the time source used in timestamps

15.13.3 Management of FPT_STM.1

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

a) management of the time.

15.13.4 Management of FPT_STM.2

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

a) setting of time by user authorized according to security policy.

15.13.5 Audit of FPT_STM.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Changes to the time;

b) detailed: Providing a timestamp.

15.13.6 Audit of FPT_STM.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Discontinuous changes to the time;

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

b) detailed: Changes to the time source.

15.13.7 FPT_STM.1 Reliable time stamps

Component relationships

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

15.13.8 FPT_STM.2 Time source

Component relationships

Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps FMT_SMR.1 Security roles

FPT_STM.2.1

The TSF shall allow the [assignment: *user authorized by security policy*] to [assignment: *set the time, configure another time source*]].

15.14 Inter-TSF TSF data consistency (FPT_TDC)

15.14.1 Family behaviour

In a distributed environment, a TOE may need to exchange TSF data with another trusted IT product. This family defines the requirements for sharing and consistent interpretation of these attributes between the TSF of the TOE and a different trusted IT product.

15.14.2 Components leveling and description

Figure 73 shows the component leveling for this family.

Figure 73 — FPT_TDC: Component leveling

FPT_TDC.1 Inter-TSF basic TSF data consistency, requires that the TSF provide the capability to ensure consistency of attributes between TSFs.

15.14.3 Management of FPT_TDC.1

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

a) there are no management activities foreseen.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.14.4 Audit of FPT_TDC.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful use of TSF data consistency mechanisms;

b) basic: Use of the TSF data consistency mechanisms;

c) basic: Identification of which TSF data have been interpreted;

d) basic: Detection of modified TSF data.

15.14.5 FPT_TDC.1 Inter-TSF basic TSF data consistency

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1

The TSF shall provide the capability to consistently interpret [assignment: *list of TSF data types*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2

The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

15.15 Testing of external entities (FPT_TEE)

15.15.1 Family behaviour

This family defines requirements for the TSF to perform tests on one or more external entities.

This component is not intended to be applied to human users.

External entities can include applications running on the TOE, hardware or software running "underneath" the TOE (e.g. platforms, operating systems) or applications/boxes connected to the TOE (e.g. intrusion detection systems, firewalls, login servers, time servers).

15.15.2 Components leveling and description

Figure 74 shows the component leveling for this family.

Figure 74 — FPT_TEE: Component leveling

FPT_TEE.1 Testing of external entities, provides for testing of the external entities by the TSF.

15.15.3 Management of FPT_TEE.1

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

a) management of the conditions under which the testing of external entities occurs, such as during initial start-up, regular interval, or under specified conditions;

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

b) management of the time interval if appropriate.

15.15.4 Audit of FPT_TEE.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Execution of the tests of the external entities and the results of the tests.

15.15.5 FPT_TEE.1 Testing of external entities

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TEE.1.1

The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorized user, [assignment: other conditions]*] to check the fulfillment of [assignment: *list of properties of the external entities*].

FPT_TEE.1.2

If the test fails, the TSF shall [assignment: *action(s)*].

15.16 Internal TOE TSF data replication consistency (FPT_TRC)

15.16.1 Family behaviour

The requirements of this family are needed to ensure the consistency of TSF data when such data is replicated internal to the TOE. Such data can become inconsistent if the internal channel between parts of the TOE becomes inoperative. If the TOE is internally structured as a network and parts of the TOE network connections are broken, this can occur when parts become disabled.

15.16.2 Components leveling and description

Figure 75 shows the component leveling for this family.

Figure 75 — FPT_TRC: Component leveling

This family consists of only one component, FPT_TRC.1 Internal TSF consistency, which requires that the TSF ensure the consistency of TSF data that is replicated in multiple locations.

15.16.3 Management of FPT_TRC.1

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

a) there are no management activities foreseen.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.16.4 Audit of FPT_TRC.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Restoring consistency upon reconnection;

b) basic: Detected inconsistency between TSF data.

15.16.5 FPT_TRC.1 Internal TSF consistency

Component relationships

Hierarchical to: No other components.

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_TRC.1.1

The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2

When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [assignment: *list of functions dependent on TSF data replication consistency*].

15.17 TSF self-test (FPT_TST)

15.17.1 Family behaviour

The family defines the requirements for the self-testing of the TSF with respect to some expected correct operation. Examples are interfaces to enforcement functions, and sample arithmetical operations on critical parts of the TOE. These tests can be carried out at start-up, periodically, at the request of the authorized user, or when other conditions are met. The actions to be taken by the TOE as the result of self-testing are defined in other families.

The requirements of this family are also needed to detect the corruption of TSF data and TSF itself (i.e. TSF executable code or TSF hardware component) by various failures that do not necessarily stop the TOE's operation (which would be handled by other families). These checks need to be performed because these failures cannot necessarily be prevented. Such failures can occur either because of unforeseen failure modes or associated oversights in the design of hardware, firmware, or software, or because of malicious corruption of the TSF due to inadequate logical and/or physical protection.

15.17.2 Components leveling and description

Figure 76 shows the component leveling for this family.

Figure 76 — FPT_TST: Component leveling

FPT_TST.1 TSF self-testing, provides the ability to test the TSF's correct operation. These tests can be performed at start-up, periodically, at the request of the authorized user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and TSF itself.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

15.17.3 Management of FPT_TST.1

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

a) management of the conditions under which TSF self-testing occurs, such as during initial start-up, regular interval, or under specified conditions;

b) management of the time interval if appropriate.

15.17.4 Audit of FPT_TST.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Indication that the TSF self-tests were completed and any failures of the tests.

b) basic: Execution of the TSF self-tests and the results of the tests.

15.17.5 FPT_TST.1 TSF self-testing

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1

The TSF shall run a suite of the following self-tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test should occur]*] to demonstrate the correct operation of [selection: *[assignment: parts of TSF], the TSF*]: [assignment: *list of self-tests run by the TSF*].

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of [selection: *[assignment: parts of TSF data], TSF data*].

FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of [selection: *[assignment: parts of TSF], TSF*].

16 Class FRU: Resource utilization

16.1 Class description

This class provides three families that support the availability of required resources such as processing capability and/or storage capacity. The family Fault Tolerance provides protection against unavailability of capabilities caused by failure of the TOE. The family Priority of Service ensures that the resources will be allocated to the more important or time-critical tasks and cannot be monopolized by lower priority tasks. The family Resource Allocation provides limits on the use of available resources, therefore preventing users from monopolizing the resources.

Figure 77 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex K provides explanatory information for this class and should be consulted when using the components identified in this class.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

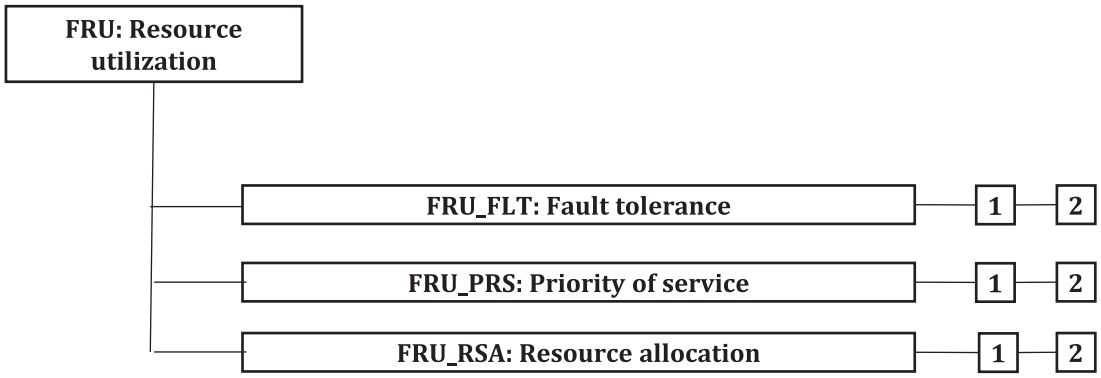


Figure 77 — FRU: Resource utilization class decomposition

16.2 Fault tolerance (FRU_FLT)

16.2.1 Family behaviour

The requirements of this family ensure that the TOE will maintain correct operation even in the event of failures.

16.2.2 Components leveling and description

Figure 78 shows the component leveling for this family.

Figure 78 — FRU_FLT: Component leveling

FRU_FLT.1 Degraded fault tolerance, requires the TOE to continue correct operation of identified capabilities in the event of identified failures.

FRU_FLT.2 Limited fault tolerance, requires the TOE to continue correct operation of all capabilities in the event of identified failures.

16.2.3 Management of FRU_FLT.1, FRU_FLT.2

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

a) there are no management activities foreseen.

16.2.4 Audit of FRU_FLT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Any failure detected by the TSF;

b) basic: All TOE capabilities being discontinued due to a failure.

16.2.5 Audit of FRU_FLT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Any failure detected by the TSF.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

16.2.6 FRU_FLT.1 Degraded fault tolerance

Component relationships

Hierarchical to: No other components.

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1.1

The TSF shall ensure the operation of [assignment: *list of TOE capabilities*] when the following failures occur: [assignment: *list of type of failures*].

16.2.7 FRU_FLT.2 Limited fault tolerance

Component relationships

Hierarchical to: FRU_FLT.1 Degraded fault tolerance

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.2.1

The TSF shall ensure the operation of **all the TOE's capabilities** when the following failures occur: [assignment: *list of type of failures*].

16.3 Priority of service (FRU_PRS)

16.3.1 Family behaviour

The requirements of this family allow the TSF to control the use of resources under the control of the TSF by users and subjects such that high priority activities under the control of the TSF will always be accomplished without undue interference or delay caused by low priority activities.

16.3.2 Components leveling and description

Figure 79 shows the component leveling for this family.

Figure 79 — FRU_PRS: Component leveling

FRU_PRS.1 Limited priority of service, provides priorities for a subject's use of a subset of the resources under the control of the TSF.

FRU_PRS.2 Full priority of service, provides priorities for a subject's use of all of the resources under the control of the TSF.

16.3.3 Management of FRU_PRS.1, FRU_PRS.2

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

a) assignment of priorities to each subject in the TSF.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

16.3.4 Audit of FRU_PRS.1, FRU_PRS.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Rejection of operation based on the use of priority within an allocation;

b) basic: All attempted uses of the allocation function which involves the priority of the service functions.

16.3.5 FRU_PRS.1 Limited priority of service

Hierarchical to: No other components.

Dependencies: No dependencies.

FRU_PRS.1.1

The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2

The TSF shall ensure that each access to [assignment: *controlled resources*] shall be mediated on the basis of the subjects assigned priority.

16.3.6 FRU_PRS.2 Full priority of service

Component relationships

Hierarchical to: FRU_PRS.1 Limited priority of service

Dependencies: No dependencies.

FRU_PRS.2.1

The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.2.2

The TSF shall ensure that each access to **all shareable resources** shall be mediated on the basis of the subjects assigned priority.

16.4 Resource allocation (FRU_RSA)

16.4.1 Family behaviour

The requirements of this family allow the TSF to control the use of resources by users and subjects such that denial of service will not occur because of unauthorized monopolization of resources.

16.4.2 Components leveling and description

Figure 80 shows the component leveling for this family.

Figure 80 — FRU_RSA: Component leveling

FRU_RSA.1 Maximum quotas, provides requirements for quota mechanisms that ensure that users and subjects will not monopolize a controlled resource.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FRU_RSA.2 Minimum and maximum quotas, provides requirements for quota mechanisms that ensure that users and subjects will always have at least a minimum of a specified resource and that they will not be able to monopolize a controlled resource.

16.4.3 Management of FRU_RSA.1

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

a) specifying maximum limits for a resource for groups and/or individual users and/or subjects by an administrator.

16.4.4 Management of FRU_RSA.2

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

a) specifying minimum and maximum limits for a resource for groups and/or individual users and/or subjects by an administrator.

16.4.5 Audit of FRU_RSA.1, FRU_RSA.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Rejection of allocation operation due to resource limits.

b) basic: All attempted uses of the resource allocation functions for resources that are under control of the TSF.

16.4.6 FRU_RSA.1 Maximum quotas

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FRU_RSA.1.1

The TSF shall enforce maximum quotas of the following resources: [assignment: *controlled resources*] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*].

16.4.7 FRU_RSA.2 Minimum and maximum quotas

Component relationships

Hierarchical to: FRU_RSA.1 Maximum quotas

Dependencies: No dependencies.

FRU_RSA.2.1

The TSF shall enforce maximum quotas of the following resources [assignment: *controlled resources*] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*].

FRU_RSA.2.2

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall ensure the provision of minimum quantity of each [assignment: *controlled resource*] that is available for [selection: *an individual user, defined group of users, subjects*] to use [selection: *simultaneously, over a specified period of time*].

17 Class FTA: TOE access

17.1 Class description

This family specifies functional requirements for controlling the establishment of a user's session.

Figure 81 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex L provides explanatory information for this class and should be consulted when using the components identified in this class.

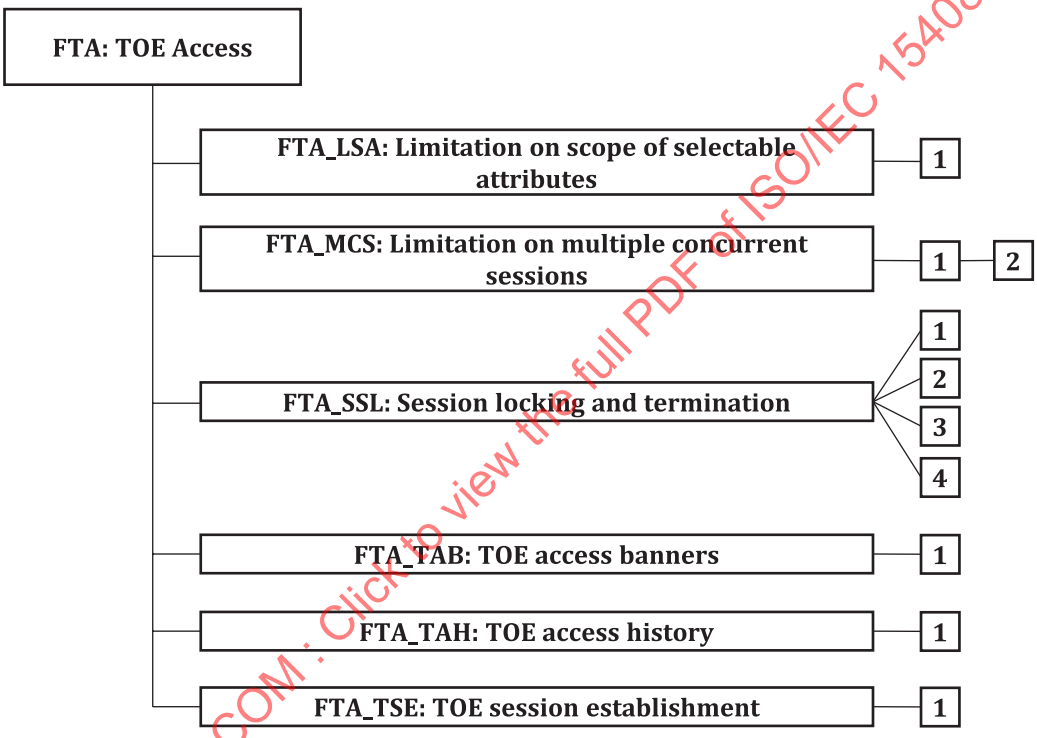


Figure 81 — FTA: TOE access class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

17.2 Limitation on scope of selectable attributes (FTA_LSA)

17.2.1 Family behaviour

This family defines requirements to limit the scope of session security attributes that a user can select for a session.

17.2.2 Components leveling and description

Figure 82 shows the component leveling for this family.

Figure 82 — FTA_LSA: Component leveling

© ISO/IEC 2022 – All rights reserved

FTA_LSA.1 Limitation on scope of selectable attributes, provides the requirement for a TOE to limit the scope of the session security attributes during session establishment.

17.2.3 Management of FTA_LSA.1

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

a) management of the scope of the session security attributes by an administrator.

17.2.4 Audit of FTA_LSA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: All failed attempts at selecting session security attributes;

b) basic: All attempts at selecting session security attributes;

c) detailed: Capture of the values of each of the session security attributes.

17.2.5 FTA_LSA.1 Limitation on scope of selectable attributes

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_LSA.1.1

The TSF shall restrict the scope of the session security attributes [assignment: *session security attributes*], based on [assignment: *attributes*].

17.3 Limitation on multiple concurrent sessions (FTA_MCS)

17.3.1 Family behaviour

This family defines requirements to place limits on the number of concurrent sessions that belong to the same user.

17.3.2 Components leveling and description

Figure 83 shows the component leveling for this family.

Figure 83 — FTA_MCS: Component leveling

FTA_MCS.1 Basic limitation on multiple concurrent sessions, provides limitations that apply to all users of the TSF.

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions extends FTA_MCS.1 Basic limitation on multiple concurrent sessions by requiring the ability to specify limitations on the number of concurrent sessions based on the related security attributes.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

17.3.3 Management of FTA_MCS.1

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

a) management of the maximum allowed number of concurrent user sessions by an administrator.

17.3.4 Management of FTA_MCS.2

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

a) management of the rules that govern the maximum allowed number of concurrent user sessions by an administrator.

17.3.5 Audit of FTA_MCS.1, FTA_MCS.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Rejection of a new session based on the limitation of multiple concurrent sessions;

b) detailed: Capture of the number of currently concurrent user sessions and the user security attribute(s).

17.3.6 FTA_MCS.1 Basic limitation on multiple concurrent sessions

Component relationships

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

FTA_MCS.1.1

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2

The TSF shall enforce, by default, a limit of [assignment: *default number*] sessions per user.

17.3.7 FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Component relationships

Hierarchical to:	FTA_MCS.1 Basic limitation on multiple concurrent sessions
Dependencies:	FIA_UID.1 Timing of identification

FTA_MCS.2.1

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user **according to the rules [assignment: *rules for the number of maximum concurrent sessions*].**

FTA_MCS.2.2

The TSF shall enforce, by default, a limit of [assignment: *default number*] sessions per user.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

17.4 Session locking and termination (FTA_SSL)

17.4.1 Family behaviour

This family defines requirements for the TSF to provide the capability for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions.

17.4.2 Components leveling and description

Figure 84 shows the component leveling for this family.

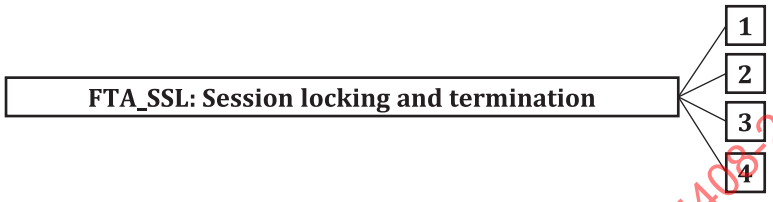


Figure 84 — FTA_SSL: Component leveling

FTA_SSL.1 TSF-initiated session locking includes system-initiated locking of an interactive session after a specified period of user inactivity.

FTA_SSL.2 User-initiated locking, provides capabilities for the user to lock and unlock the user's own interactive sessions.

FTA_SSL.3 TSF-initiated termination, provides requirements for the TSF to terminate the session after a specified period of user inactivity.

FTA_SSL.4 User-initiated termination, provides capabilities for the user to terminate the user's own interactive sessions.

17.4.3 Management of FTA_SSL.1

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

a) specification of the time of user inactivity after which lock-out occurs for an individual user;

b) specification of the default time of user inactivity after which lock-out occurs;

c) management of the events that occur prior to unlocking the session.

17.4.4 Management of FTA_SSL.2

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

a) management of the events that occur prior to unlocking the session.

17.4.5 Management of FTA_SSL.3

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

a) specification of the time of user inactivity after which termination of the interactive session occurs for an individual user;

b) specification of the default time of user inactivity after which termination of the interactive session occurs.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

17.4.6 Management of FTA_SSL.4

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

a) there are no management activities foreseen.

17.4.7 Audit of FTA_SSL.1, FTA_SSL.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Locking of an interactive session by the session locking mechanism;

b) minimal: Successful unlocking of an interactive session;

c) basic: Any attempts at unlocking an interactive session.

17.4.8 Audit of FTA_SSL.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Termination of an interactive session by the session locking mechanism.

17.4.9 Audit of FTA_SSL.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Termination of an interactive session by the user.

17.4.10 FTA_SSL.1 TSF-initiated session locking

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL.1.1

The TSF shall lock an interactive session after [assignment: *time interval of user inactivity*] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2

The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].

17.4.11 FTA_SSL.2 User-initiated locking

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FTA_SSL.2.1

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall allow user-initiated locking of the user's own interactive session, by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2

The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].

17.4.12 FTA_SSL.3 TSF-initiated termination

Component relationships

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [assignment: time interval of user inactivity].

17.4.13 FTA_SSL.4 User-initiated termination

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user's own interactive session.

17.5 TOE access banners (FTA_TAB)

17.5.1 Family behaviour

This family defines requirements to display a configurable advisory warning message to users regarding the appropriate use of the TOE.

17.5.2 Components leveling and description

Figure 85 shows the component leveling for this family.

Figure 85 — FTA_TAB: Component leveling

FTA_TAB.1 Default TOE access banners, provides the requirement for a TOE Access Banner. This banner is displayed prior to the establishment dialogue for a session.

17.5.3 Management of FTA_TAB.1

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

a) maintenance of the banner by the authorized administrator.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

17.5.4 Audit of FTA_TAB.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

17.5.5 FTA_TAB.1 Default TOE access banners

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1

Before establishing a user session, the [selection: *TSF, TOE platform*] shall display an [assignment: *description of the message*] message.

17.6 TOE access history (FTA_TAH)

17.6.1 Family behaviour

This family defines requirements for the TSF to display to a user, upon successful session establishment, a history of successful and unsuccessful attempts to access the user's account.

17.6.2 Components leveling and description

Figure 86 shows the component leveling for this family.

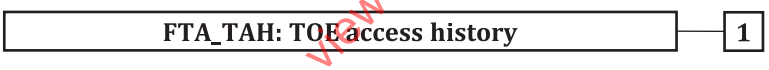


Figure 86 – FTA_TAH: Component leveling

FTA_TAH.1 TOE access history, provides the requirement for a TOE to display information related to previous attempts to establish a session.

17.6.3 Management of FTA_TAH.1

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

a) there are no management activities foreseen.

17.6.4 Audit of FTA_TAH.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

17.6.5 FTA_TAH.1 TOE access history

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FTA_TAH.1.1

Upon successful session establishment, the TSF shall display the [selection: *date, time, method, location*] of the last successful session establishment to the user.

FTA_TAH.1.2

Upon successful session establishment, the TSF shall display the [selection: *date, time, method, location*] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3

The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

17.7 TOE session establishment (FTA_TSE)

17.7.1 Family behaviour

This family defines requirements to deny a user permission to establish a session with the TOE.

17.7.2 Components leveling and description

Figure 87 shows the component leveling for this family.

Figure 87 — FTA_TSE: Component leveling

FTA_TSE.1 TOE session establishment, provides requirements for denying users access to the TOE based on attributes.

17.7.3 Management of FTA_TSE.1

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

a) management of the session establishment conditions by the authorized administrator.

17.7.4 Audit of FTA_TSE.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Denial of a session establishment due to the session establishment mechanism;

b) basic: All attempts at establishment of a user session;

c) detailed: Capture of the value of the selected access parameters.

17.7.5 FTA_TSE.1 TOE session establishment

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall be able to deny session establishment based on [assignment: *attributes*].

18 Class FTP: Trusted path/channels

18.1 Class description

Families in this class provide requirements for a trusted communication path between users and the TSF, and for a trusted communication channel between the TSF and other trusted IT products. Trusted paths and channels have the following general characteristics:

— the communications path is constructed using internal and external communications channels (as appropriate for the component) that isolate an identified subset of TSF data and commands from the remainder of the TSF and user data;

— use of the communications path can be initiated by the user and/or the TSF (as appropriate for the component);

— the communications path is capable of providing assurance that the user is communicating with the correct TSF, and that the TSF is communicating with the correct user (as appropriate for the component).

In this paradigm, a trusted channel is a communication channel that can be initiated by either side of the channel and provides non-repudiation characteristics with respect to the identity of the sides of the channel.

A trusted path provides a means for users to perform functions through an assured direct interaction with the TSF. Trusted path is usually desired for user actions such as initial identification and/or authentication but can also be desired at other times during a user's session. Trusted path exchanges can be initiated by a user or the TSF. User responses via the trusted path are guaranteed to be protected from modification by or disclosure to untrusted applications.

Families describing the use of commonly used communication protocols used in the provision of trusted channels and paths are also given.

Figure 88 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex M provides explanatory information for this class and should be consulted when using the components identified in this class.

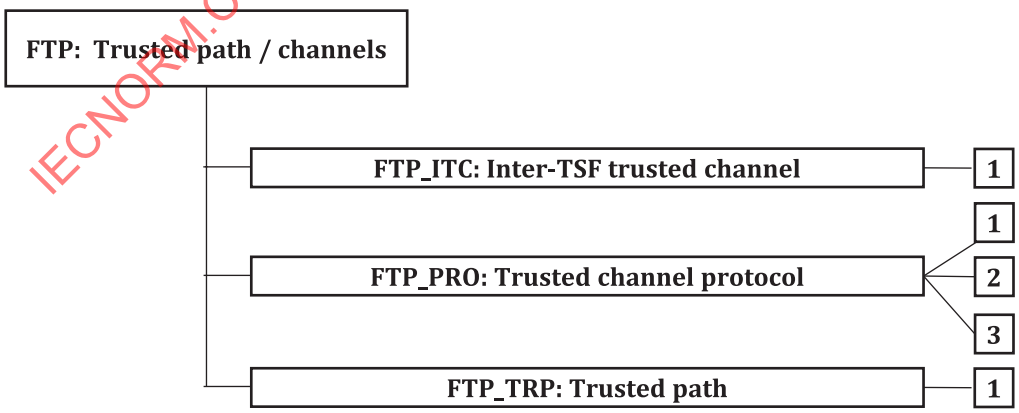


Figure 88 — FTP: Trusted path/channels class decomposition

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

18.2 Inter-TSF trusted channel (FTP_ITC)

18.2.1 Family behaviour

This family defines requirements for the creation of a trusted channel between the TSF and other trusted IT products for the performance of security critical operations. The components of this family may be included whenever there are requirements for the secure communication of user or TSF data between the TOE and other trusted IT products.

18.2.2 Components leveling and description

Figure 89 shows the component leveling for this family.

Figure 89 — FTP_ITC: Component leveling

FTP_ITC.1 Inter-TSF trusted channel, requires that the TSF provide a trusted communication channel between itself and another trusted IT product.

18.2.3 Management of FTP_ITC.1

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

a) configuring the actions that require trusted channel, if supported.

18.2.4 Audit of FTP_ITC.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Failure of the trusted channel functions;

b) minimal: Identification of the initiator and target of failed trusted channel functions;

c) basic: All attempted uses of the trusted channel functions;

d) basic: Identification of the initiator and target of all trusted channel functions.

18.2.5 FTP_ITC.1 Inter-TSF trusted channel

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

18.3 Trusted channel protocol (FTP_PRO)

18.3.1 Family behavior

This family defines requirements for establishing a trusted channel and using the trusted channel to transfer the TSF data or user data securely.

18.3.2 Components leveling and description

Figure 90 shows the component leveling for this family.

Figure 90 — FTP_PRO: Component leveling

FTP_PRO.1 Trusted channel protocol requires that communication be established in accordance with a defined protocol.

FTP_PRO.2 Trusted channel establishment requires that keys be securely established between the peers.

FTP_PRO.3 Trusted channel data protection requires that data in transit be protected.

18.3.3 Management of FTP_PRO.1

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

a) configuring the protocols needed for the trusted channel;

b) configuring the credentials for using the trusted channel;

c) configuring the conditions for initializing and terminating the trusted channel.

18.3.4 Management of FTP_PRO.2

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

a) configuring the parameters for shared secrets;

b) configuring the parameters for cryptographic key derivation.

18.3.5 Management of FTP_PRO.3

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

a) configuring the encryption and integrity mechanisms used by the trusted channel.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

18.3.6 Audit of FTP_PRO.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Failure of the trusted channel establishment;

b) minimal: Identification of the initiator and target of failed trusted channel establishment;

c) basic: All attempted uses of the trusted channel;

d) basic: Identification of the initiator and target of all trusted channel attempts.

Other events should be considered according to the specific protocols used.

18.3.7 Audit of FTP_PRO.2

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

a) minimal: Authentication failures during channel establishment;

b) basic: All authentication attempts.

18.3.8 Audit of FTP_PRO.3

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

a) minimal: Failures when attempting to verify channel properties in FTP_PRO.3.2.

18.3.9 FTP_PRO.1 Trusted channel protocol

Component relationships

Hierarchical to: No other components.

Dependencies: FTP_PRO.2 Trusted channel establishment
FTP_PRO.3 Trusted channel data protection.

FTP_PRO.1.1

The TSF shall implement [assignment: *trusted channel protocol*] acting as [assignment: *defined protocol role(s)*] in accordance with: [assignment: *list of standards*].

FTP_PRO.1.2

The TSF shall enforce usage of the trusted channel for [assignment: *purpose(s) of the trusted channel*] in accordance with: [assignment: *list of standards*].

FTP_PRO.1.3

The TSF shall permit [selection: *itself, its peer*] to initiate communication via the trusted channel.

FTP_PRO.1.4

The TSF shall enforce the following rules for the trusted channel: [assignment: *rules governing operation and use of the trusted channel and/or its protocol*].

FTP_PRO.1.5

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The TSF shall enforce the following static protocol options: [assignment: *list of options and references to standards in which each is defined*].

FTP_PRO.1.6

The TSF shall negotiate one of the following protocol configurations with its peer: [assignment: *list of configurations and reference to standards in which each is defined*].

18.3.10 FTP_PRO.2 Trusted channel establishment

Component relationships

Hierarchical to:	No other components.
Dependencies:	FTP_PRO.1 Trusted channel protocol [FCS_CKM.1 Cryptographic key generation, or FCS_CKM.2 Cryptographic key distribution] FCS_CKM.5 Cryptographic key derivation FCS_COP.1 Cryptographic operation.

FTP_PRO.2.1

The TSF shall establish a shared secret with its peer using one of the following mechanisms: [assignment: *list of key establishment mechanisms*].

FTP_PRO.2.2

The TSF shall authenticate [selection: *its peer, itself to its peer*] using one of the following mechanisms: [assignment: *list of authentication mechanisms*] and according to the following rules: [assignment: *list of rules for carrying out the authentication*].

FTP_PRO.2.3

The TSF shall use [assignment: *key derivation function*] to derive the following cryptographic keys from a shared secret: [assignment: *list of cryptographic keys*].

18.3.11 FTP_PRO.3 Trusted channel data protection

Component relationships

Hierarchical to:	No other components.
Dependencies:	FTP_PRO.1 Trusted channel protocol FTP_PRO.2 Trusted channel establishment FCS_COP.1 Cryptographic operation.

FTP_PRO.3.1

The TSF shall protect data in transit from unauthorised disclosure using one of the following mechanisms: [assignment: *list of encryption mechanisms*].

FTP_PRO.3.2

The TSF shall protect data in transit from [selection: *modification, deletion, insertion, replay, [assignment: other]*] using one of the following mechanisms: [assignment: *list of integrity protection mechanisms*].

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

18.4 Trusted path (FTP_TRP)

18.4.1 Family behaviour

This family defines the requirements to establish and maintain trusted communication to or from users and the TSF. A trusted path can be required for any security-relevant interaction. Trusted path exchanges can be initiated by a user during an interaction with the TSF, or the TSF can establish communication with the user via a trusted path.

18.4.2 Components leveling and description

Figure 91 shows the component leveling for this family.

Figure 91 — FTP_TRP: Component leveling

FTP_TRP.1 Trusted path, requires that a trusted path between the TSF and a user be provided for a set of events defined by a PP, PP-Module, functional package or ST author. The user and/or the TSF can have the ability to initiate the trusted path.

18.4.3 Management of FTP_TRP.1

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

a) configuring the actions that require trusted path, if supported.

18.4.4 Audit of FTP_TRP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Failures of the trusted path functions;

b) mMinimal: Identification of the user associated with all trusted path failures, if available;

c) basic: All attempted uses of the trusted path functions;

d) basic: Identification of the user associated with all trusted path invocations, if available.

18.4.5 FTP_TRP.1 Trusted path

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*].

FTP_TRP.1.2

The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [selection: *initial user authentication*, [assignment: *other services for which trusted path is required*]].

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Annex A
(informative)

Security functional requirements (SFRs) structure of the application notes

A.1 General

This annex contains additional guidance for the families and components defined in this document, which may be required by users, developers, or evaluators to use the components. To facilitate finding the appropriate information, the presentation of the classes, families and components in this annex is repeated from the presentation within the main clauses of this document.

A.2 Structure of the notes

A.2.1 General

The content and presentation of the notes related to functional requirements in this document is defined below.

A.2.2 Class structure

A.2.2.1 General

Figure A.1 illustrates the functional class structure in this annex.

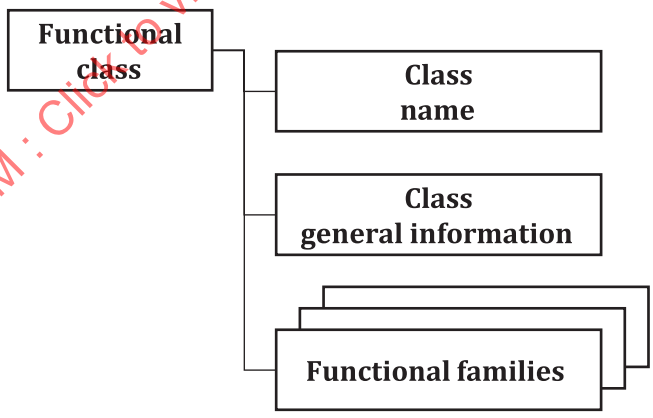


Figure A.1 — Functional class structure

NOTE Some functional classes contain multiple functional families.

A.2.2.2 Class name

This is the unique name of the class defined within the normative elements of this document.

A.2.2.3 Class introduction

The class introduction provides information about the use of the families and components of the class. This information is completed with the informative diagram that describes the organization of each

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

class with the families in each class and the hierarchical relationship between components in each family.

A.2.3 Family structure

A.2.3.1 General

Figure A.2 illustrates the functional family structure for application notes in diagrammatic form.

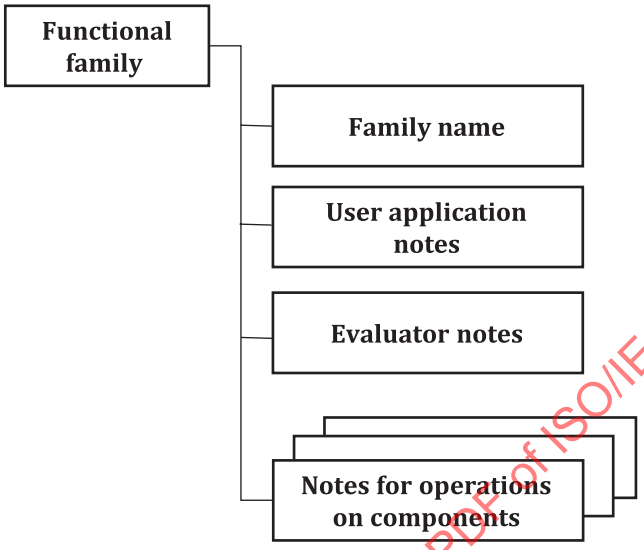


Figure A.2 — Functional family structure for application notes

A.2.3.2 Family name

This is the unique name of the family defined within the normative elements of this document.

A.2.3.3 User application notes

The user notes contain additional information that is of interest to potential users of the family, that is PP, PP-Module, ST and functional package authors, and developers of TOEs incorporating the functional components. The presentation is informative and can cover warnings about limitations of use and areas where specific attention can be required when using the components.

NOTE In the annexes the term PP, PP-Module, functional package or ST author includes authors of documents used to formulate a PP or ST, this includes PP-Modules and functional packages.

A.2.3.4 Evaluator notes

The evaluator notes contain any information that is of interest to developers and evaluators of TOEs that claim conformance with a component of the family. The presentation provides information and can cover a variety of areas where specific attention can be needed when evaluating the TOE. This can include clarifications of meaning and specification of the way to interpret requirements, as well as caveats and warnings of specific interest to evaluators.

The user application notes and evaluator notes are not mandatory and appear only if appropriate.

A.2.4 Component structure

A.2.4.1 General

Figure A.3 illustrates the functional component structure for the application notes.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

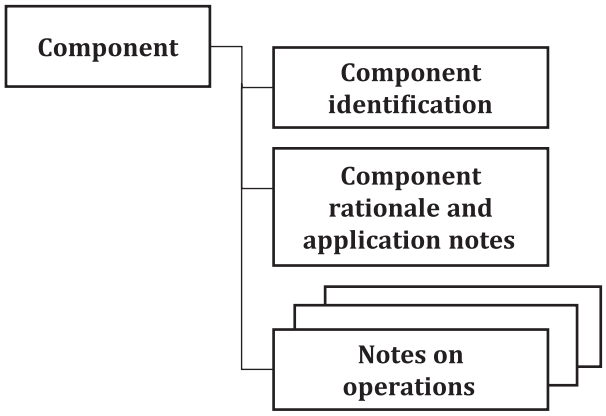


Figure A.3 — Functional component structure

A.2.4.2 Component identification

This is the unique name of the component defined within the normative elements of this document.

A.2.4.3 Component rationale and application notes

Any specific information related to the component is found in the component rationale and application notes subclause.

The component rationale contains information that refines the general statements on rationale for the specific component level and is used if level-specific amplification is needed.

The application notes contain additional refinement in the form of narrative qualifications for a specific component. This refinement may pertain to user notes, and/or evaluator notes as described in A.2.3. The application notes may be used to explain the nature of the dependencies.

The component rationale and application notes subclause appear only if appropriate.

A.2.4.4 Notes on operations

This portion of each component contains guidance relating to the permitted operations of the component.

The permitted operations subclause appears only if appropriate.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Annex B
(informative)

Dependency tables for security functional components

B.1 Dependency tables

Tables B.1 to Table B.11 show the hierarchical, direct, indirect, and optional dependencies among functional components.

Each of the components that is a dependency of some other functional component is allocated a column. Each functional component is allocated a row. The value in the table cell indicates whether the column label component is a hierarchical requirement (indicated by an "H"). directly required (indicated by a cross "X"), indirectly required (indicated by a dash "-"), or optionally required (indicated by a "O") by the row label component. Sets of optional requirements are indicated by using a subscript group, e.g. O^1 and O^2.

Where a dependency is given for security assurance requirements, ISO/IEC 15408-3 shall be referred to.

NOTE Depending upon the optional requirements chosen, some indirect dependencies are not applicable.

If no character is presented, the component is not dependent upon another component.

EXAMPLE

An example of a component with optional dependencies is FDP_ETC.1 Export of user data without security attributes, which requires either FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control to be present. So, if FDP_ACC.1 Subset access control is present, FDP_IFC.1 Subset information flow control is not necessary and vice versa.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Table B.1 — Dependency table for Class FAU: Security audit

	FAU_GEN.1	FAU_SAA.1	FAU_SAA.3	FAU_SAR.1	FAU_STG.1	FAU_STG.2	FAU_STG.4	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1	FTP_ITC.1
FAU_ARP.1	-	X										-	
FAU_GEN.1												X	
FAU_GEN.2	X							X				-	
FAU_SAA.1	X											-	
FAU_SAA.2								X					
FAU_SAA.3													
FAU_SAA.4			H										
FAU_SAR.1	X											-	
FAU_SAR.2	-			X								-	
FAU_SAR.3	-			X								-	
FAU_SEL.1	X							-	X	-	-	-	
FAU_STG.1	X											-	X
FAU_STG.2	X											-	
FAU_STG.3	X					H						-	
FAU_STG.4	-					X						-	
FAU_STG.5	X					X	H					-	

Table B.2 — Dependency table for Class FCO: Communication

	FIA_UID.1	FCO_NRR.1	FCO_NRO.1
FCO_NRO.1	X		
FCO_NRO.2	X		H
FCO_NRR.1	X		
FCO_NRR.2	X	H	

Table B.3 — Dependency table for Class FCS: Cryptographic support

	FCS_CKM.1	FCS_CKM.2	FCS_CKM.3	FCS_CKM.5	FCS_CGM.6	FCS_COP.1	FCS_RBG.1	FCS_RBG.2	FCS_RBG.3	FCS_RBG.4	FCS_RBG.5	FCS_RNG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITC.2	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FPT_TST.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FCS_CKM.1	-	O[1]	X	O[1]	X	O[1]	O[2]	-	-		-	O[2]	-	-	-	-	-	-	-	-	-	-	-	-	-	-		-
FCS_CKM.2	O[1]	-	X	O[1]	-	-	-	-	-		-	-	-	-	-	-	O[1]	O[1]	-	-	-	-	-	-	-	-	-	-
FCS_CKM.3	O[1]	-	-	O[1]	-	-	-	-	-		-	-	-	-	-	-	O[1]	O[1]	-	-	-	-	-	-	-	-	-	-
FCS_CKM.5	-	O[1]	-	-	X	O[1]	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
FCS_CKM.6	O[1]	-	-	-	-	-	-	-	-		-	-	-	-	-	-	O[1]	O[1]	-	-	-	-	-	-	-	-	-	-
FCS_COP.1	O[2]	-	X	O[2]	-	-	-	-	-			-	-	-	-	-	O[1]	O[1]	-	-	-	-	-	-	-	-	-	-
FCS_RBG.1							-	O[1]	O[1]		-													X	X			
FCS_RBG.2							X	-	-	-	-													-	-			

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Table B.3 *(continued)*

	FCS_CKM.1	FCS_CKM.2	FCS_CKM.3	FCS_CKM.5	FCS_CGM.6	FCS_COP.1	FCS_RBG.1	FCS_RBG.2	FCS_RBG.3	FCS_RBG.4	FCS_RBG.5	FCS_RNG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITC.2	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FPT_TST.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FCS_RBG.3							X	-	-	-	-													-	-			
FCS_RBG.4							X	-	-	-	X													-	-			
FCS_RBG.5							X	O[1]	O[1]	O[1]	-													-	-			
FCS_RBG.6							X	-	-	-	-													-	-			
FCS_RNG.1																												

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Table B.4 — Dependency table for Class FDP: User data protection

	FCS_CKM.1	FCS_CKM.3	FCS_CKM.5	FCS_CKM.6	FCS_COP.1	FCS_RBG.1	FCS_RBG.2	FCS_RBG.3	FCS_RNG.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_IFF.3	FDP_IFF.4	FDP_ITC.1	FDP_ITC.2	FDP_ROL.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FPT_TST.1	FPT_TDC.1	FTP_ITC.1	FTP_TRP.1
FDP_ACC.1																												
FDP_ACC.2																												
FDP_ACF.1										X											X							
FDP_DAU.1																												
FDP_DAU.2										H									X									
FDP_ETC.1										O^1	-	O^1	-			O^1			-	-	-	-	-					
FDP_ETC.2										O^1	-	O^1	-						-	-	-	-	-					
FDP_IFC.1										-	-	-	X						-	-	-	-	-					
FDP_IFC.2										-	-	H	X						-	-	-	-	-					
FDP_IFF.1										-	-	X	-						-	-	X	-	-					
FDP_IFF.2										-	-	X	H						-	-	X	-	-					
FDP_IFF.3										-	-	X	-						-	-	-	-	-					
FDP_IFF.4										-	-	X	-	H					-	-	-	-	-					
FDP_IFF.5										-	-	X	-		H				-	-	-	-	-					
FDP_IFF.6										-	-	X	-						-	-	-	-	-					
FDP_IRC.1																												
FDP_ITC.1										O^1	-	O^1	-						-	-	X	-	-					
FDP_ITC.2										O^1	-	O^1	-						-	-	-	-	-		X	O^2	O^2	-
FDP_ITT.1										O^1	-	O^1	-						-	-	-	-	-					
FDP_ITT.2										O^1	-	O^1	-						-	-	-	-	-					
FDP_ITT.3										O^1	-	O^1	-						-	-	-	-	-					
FDP_ITT.4										O^1	-	O^1	-						-	-	-	-	-					
FDP_RIP.1																												
FDP_RIP.2																		H										
FDP_ROL.1										O^1	-	O^1	-						-	-	-	-	-					
FDP_ROL.2										O^1	-	O^1	-					H	-	-	-	-	-					
FDP_SDC.1																												
FDP_SDC.2	-	-	-	-	X	-	-	-	-	-	-	-	-						-	-	-	-	-					-
FDP_SDI.1																												
FDP_SDI.2																												
FDP_UIT.1																												
FDP_UIT.2																												
FIA_UID.1	-	-	-	-		-	-	-	-		-	-	-	-	-	-	-	-		-		-	-	-				
FMT_MSA.1	-	-	-	-		-	-	-	-		-	-	-	-	-	-	-	-				-	-	-				
FMT_MSA.3	-	-	-	-		-	-	-	-		-	-	-	-	-	-	-	-				-	-	-				
FMT_SMF.1	-	-	-	-		-	-	-	-		-	-	-	-	-	-	-	-		-			-	-				
FMT_SMR.1	-	-	-	-		-	-	-	-		-	-	-	-	-	-	-	-		-				-				
FPT_FLS.1																												
FPT_TST.1																												
FPT_TDC.1																												
FTP_ITC.1																												
FTP_TRP.1																												

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Table B.4 *(continued)*

	FDP_SDI.2	FDP_UCT.1	FDP_UIT.1	FDP_UIT.2	FDP_UIT.3
FTP_TRP.1		O[1]	O[1]	-	-
FTP_ITC.1		O[1]	O[1]	O[2]	O[2]
FPT_TDC.1					
FPT_TST.1					
FPT_FLS.1					
FMT_SMR.1		-	-	-	-
FMT_SMF.1		-	-	-	-
FMT_MSA.3		-	-	-	-
FMT_MSA.1		-	-	-	-
FIA_UID.1		-	-	-	-
FDP_UIT.2					H
FDP_UIT.1				O[2]	O[2]
FDP_SDI.1	H				
FDP_ROL.1					
FDP_RIP.1					
FDP_ITT.3					
FDP_ITT.2					
FDP_ITT.1					
FDP_ITC.2					
FDP_ITC.1					
FDP_IFF.4					
FDP_IFF.3					
FDP_IFF.1		-	-	-	-
FDP_IFC.1		O[2]	O[2]	O[1]	O[1]
FDP_ACF.1		-	-	-	-
FDP_ACC.1		O[2]	O[2]	O[1]	O[1]
FCS_RNG.1					
FCS_RBG.3					
FCS_RBG.2					
FCS_RBG.1					
FCS_COP.1					
FCS_CKM.6					
FCS_CKM.5					
FCS_CKM.3					
FCS_CKM.1					

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Table B.5 — Dependency table for Class FIA: Identification and authentication

	FIA_ATD.1	FIA_UAU.1	FIA_UID.1
FIA_AFL.1		X	-
FIA_API.1			
FIA_ATD.1			
FIA_SOS.1			
FIA_SOS.2			
FIA_UAU.1			X
FIA_UAU.2		H	X
FIA_UAU.3			
FIA_UAU.4			
FIA_UAU.5			
FIA_UAU.6			
FIA_UAU.7		X	-
FIA_UID.1			
FIA_UID.2			H
FIA_USB.1	X		

Table B.6 — Dependency table for Class FMT: Security management

	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FIA_UID.1	FMT_LIM.1	FMT_LIM.2	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FMT_LIM.1						-	X						
FMT_LIM.2						X	-						
FMT_MOF.1					-						X	X	
FMT_MSA.1	O[1]	-	O[1]	-	-			-	-		X	X	
FMT_MSA.2	O[1]	-	O[1]	-	-			X	-		-	X	
FMT_MSA.3	-	-	-	-	-			X	-		-	X	
FMT_MSA.4	O[1]	-	O[1]	-	-			-	-		-	-	
FMT_MTD.1					-						X	X	
FMT_MTD.2					-					X	-	X	
FMT_MTD.3					-					X	-	-	
FMT_REV.1					-							X	
FMT_SAE.1					-							X	X
FMT_SMF.1													
FMT_SMR.1					X								
FMT_SMR.2					X							H	
FMT_SMR.3					-							X	

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Table B.7 — Dependency table for Class FPR: Privacy

	FIA_UID.1	FPR_ANO.1	FPR_PSE.1	FPR_UNO.1
FPR_ANO.1				
FPR_ANO.2		H		
FPR_PSE.1				
FPR_PSE.2	X		H	
FPR_PSE.3			H	
FPR_UNL.1				
FPR_UNO.1				
FPR_UNO.2				H
FPR_UNO.3				X
FPR_UNO.4				

Table B.8 — Dependency table for Class FPT: Protection of the TSF

	AGD_OPE.1	ADV_FSP.1	FIA_UID.1	FMT_LIM.1	FMT_LIM.2	FMT_SMF.1	FMT_SMR.1	FPT_ITI.1	FPT_ITT.1	FTP_PHP.1	FPT_RCV.1	FPT_RCV.2	FPT_SSP.1	FPT_STM.1
FPT_EMS.1														
FPT_FLS.1														
FPT_INI.1														
FPT_ITA.1														
FPT_ITC.1														
FPT_ITI.1														
FPT_ITI.2								H						
FPT_ITT.1														
FPT_ITT.2									H					
FPT_ITT.3									X					
FPT_PHP.1														
FPT_PHP.2				X	-					H				
FPT_PHP.3														
FPT_RCV.1	X	-												
FPT_RCV.2	X	-									H			
FPT_RCV.3	X	-										H		
FPT_RCV.4														
FPT_RPL.1														
FPT_SSP.1									X					
FPT_SSP.2									X				H	
FPT_STM.1														
FPT_STM.2			-				X							X
FPT_TDC.1														
FPT_TEE.1														

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Table B.8 *(continued)*

	AGD_OPE.1	ADV_FSP.1	FIA_UID.1	FMT_LIM.1	FMT_LIM.2	FMT_SMF.1	FMT_SMR.1	FPT_ITI.1	FPT_ITT.1	FTP_PHP.1	FPT_RCV.1	FPT_RCV.2	FPT_SSP.1	FPT_STM.1
FPT_TRC.1									X					
FPT_TST.1														

NOTE The AGD and ADV classes and their dependencies are described in ISO/IEC 15408-3.

Table B.9 — Dependency table for Class FRU: Resource utilization

	FPT_FLS.1	FRU_FLT.1	FRU_PRS.1	FRU_RSA.1
FRU_FLT.1	X			
FRU_FLT.2	X	H		
FRU_PRS.1				
FRU_PRS.2			H	
FRU_RSA.1				
FRU_RSA.2				H

Table B.10 — Dependency table for Class FTA: TOE access

	FIA_UAU.1	FIA_UID.1	FMT_SMR.1	FTA_MCS.1
FTA_LSA.1				
FTA_MCS.1		X		
FTA_MCS.2		X		H
FTA_SSL.1	X	-		
FTA_SSL.2	X	-		
FTA_SSL.3			X	
FTA_SSL.4				
FTA_TAB.1				
FTA_TAH.1				
FTA_TSE.1				

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Table B.11 — Dependency table for Class FTP: Trusted Path/channels

	FTP_ITC.1	FTP_PRO.1	FTP_PRO.2	FTP_PRO.3	FTP_TRP.1
FTP_PRO.3		X			
FTP_PRO.2		X		X	
FTP_PRO.1			X	X	
FTP_TRP.1		-	-	-	
FTP_ITC.1		-	-	-	
FPT_TDC.1		-	-	-	
FPT_TST.1		-	-	-	
FPT_FLS.1		-	-	-	
FMT_SMR.1		-	-	-	
FMT_SMF.1		-	-	-	
FMT_MSA.3		-	-	-	
FMT_MSA.1		-	-	-	
FIA_UID.1		-	-	-	
FDP_ITC.2		-	-	-	
FDP_ITC.1		-	-	-	
FDP_IFF.1		-	-	-	
FDP_IFC.1		-	-	-	
FDP_ACF.1		-	-	-	
FDP_ACC.1		-	-	-	
FCS_RNG.1		-	-	-	
FCS_RBG.3		-	-	-	
FCS_RBG.2		-	-	-	
FCS_RBG.1		-	-	-	
FCS_COP.1		-	X	X	
FCS_CKM.6		-	-	-	
FCS_CKM.5		-	X	-	
FCS_CKM.3		-	-	-	
FCS_CKM.2		-	O[1]	-	
FCS_CKM.1		-	O[1]	-	

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Annex C
(normative)

Class FAU: Security audit — Application notes

C.1 General

C.1.1 General information about audit requirements

The audit families allow PP, PP-Module, functional package or /ST authors the ability to define requirements for monitoring user activities and, in some cases, detecting real, possible, or imminent violations of the enforcement of the SFRs. The TOE's security audit functions are defined to help monitor security-relevant events, and act as a deterrent against security violations. The requirements of the audit families refer to functions that include audit data protection, record format, and event selection, as well as analysis tools, violation alarms, and real-time analysis. The audit records may be presented in human-readable format either directly or indirectly or both.

EXAMPLE 1

An example of direct presentation is storing the audit records in human-readable format.

An example of indirect presentation is by using audit reduction tools.

While developing the security audit requirements, the author of a PP, PP-Module, functional package or ST should take note of the inter-relationships among the audit families and components. The potential exists to specify a set of audit requirements that conform with the family/component dependencies lists, while at the same time resulting in a deficient audit function.

EXAMPLE 2

An audit function that requires all security relevant events to be audited but without the selectivity to control them on any reasonable basis such as individual user or object.

C.1.2 Audit requirements in a distributed environment

The implementation of audit requirements for networks and other large systems can differ significantly from those needed for stand-alone systems. Larger, more complex, and active systems require more thought concerning which audit data to collect and how this can be managed, due to the lowered feasibility of interpreting (or even storing) what gets collected. The traditional notion of a time-ordered list, set of records or "trail" of audited events is not always applicable in a global asynchronous network with many arbitrary events occurring at once.

Also, different hosts and servers on a distributed TOE can have differing naming policies and values. Further, the use of symbolic names for audit review requires a net-wide convention to avoid redundancies and "name clashes."

A multi-object audit repository, portions of which are accessible by a potentially wide variety of authorized users, are usually required if audit repositories are to serve a useful function in distributed systems.

Finally, misuse of authority by authorized users can be addressed by systematically avoiding local storage of audit data pertaining to administrator actions.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

C.2 Security audit automatic response (FAU_ARP)

C.2.1 User application notes

The security audit automatic response family describes requirements for the handling of audit events. The requirement can include requirements for alarms or TSF action (automatic response).

EXAMPLE

The TSF can include the generation of real time alarms, termination of the offending process, disabling of a service, or disconnection or invalidation of a user account.

An audit event is defined to be an "potential security violation" when indicated by the Security audit analysis (FAU_SAA) components.

C.2.2 FAU_ARP.1 Security alarms

C.2.2.1 Component rationale and application notes

One or more actions should be taken for follow up action in the event of an alarm.

These actions can include informing the authorized user of the alarm, presenting the authorized user with a set of possible containment actions, or options for the authorized user to take corrective actions.

The timing of the actions should be carefully considered by the PP, PP-Module, functional package or / ST author.

C.2.2.2 Operations

In FAU_ARP.1.1, the author of a PP, PP-Module, functional package or ST specifies the actions to be taken in case of a potential security violation.

EXAMPLE

An example of such a list is: "inform the authorized user, disable the subject that created the potential security violation."

The list may also specify that the action to be taken can be specified by an authorized user.

C.3 Security audit data generation (FAU_GEN)

C.3.1 General

C.3.1.1 User application notes

The security audit data generation family includes requirements to specify the audit events that shall be generated by the TSF for security-relevant events.

This family is presented in a manner that avoids a dependency on all components requiring audit support. Each component has an audit subclause developed in which the events to be audited for that functional area are listed. When the PP, PP-Module, functional package or /ST is written, the items in the audit area are used to complete the variable in these components. Thus, the specification of what can be audited for a functional area is localized in that functional area.

The list of auditable events is entirely dependent on the other functional families within the PP, PP-Module, functional package or ST./ST. Each family definition should therefore include a list of its family-specific auditable events. Each auditable event in the list of auditable events specified in the functional family should correspond to one of the levels of audit event generation specified in this family (i.e. minimal, basic, detailed). This provides the author of a PP, PP-Module, functional package or ST with the information necessary to ensure that all appropriate auditable events are specified in the PP, PP-

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Module, functional package or ST./ST. The following example shows how auditable events are to be specified in appropriate functional families:

EXAMPLE 1

The following actions should be auditable if Security audit data generation (FAU_GEN) is included in the PP, PP-Module, functional package or ST:

a) minimal: Successful use of the user security attribute administration functions;

b) basic: All attempted uses of the user security attribute administration functions;

c) basic: Identification of which user security attributes have been modified;

d) detailed: With the exception of specific sensitive attribute data items, the new values of the attributes should be captured."

NOTE Sensitive attribute data items include passwords and cryptographic keys.

For each functional component that is chosen, the auditable events that are indicated in that component, at and below the level indicated in Security audit data generation (FAU_GEN) should be auditable. So, in the previous example "Basic" would be selected in Security audit data generation (FAU_GEN), the auditable events mentioned in a), b) and c) should be auditable.

Observe that the categorization of auditable events (minimal, basic, detailed) is hierarchical in that order.

This means that:

— when minimal audit generation is desired, all auditable events identified as being minimal should be included in the PP, PP-Module, functional package or ST through the use of the appropriate assignment operation;

— when basic audit generation is desired, all auditable events identified as being either minimal or basic, should also be included in the PP, PP-Module, functional package or 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, PP-Module, functional package or ST.

A PP, PP-Module, functional package or ST author may decide to include other auditable events beyond those required for a given audit level.

EXAMPLE 2

The PP, PP-Module, functional package or ST may claim only minimal audit capabilities while including most of the basic capabilities because the few excluded capabilities conflict with other PP, PP-Module, functional package or ST constraints (perhaps because they require the collection of unavailable data).

The functionality that creates the auditable event should be specified in the PP, PP-Module, functional package or ST as a functional requirement.

EXAMPLE 3

The following are examples of the types of the events that can be defined as auditable within each PP, PP-Module, functional package or ST functional component:

a) introduction of objects within the control of the TSF into a subject's address space;

b) deletion of objects;

c) distribution or revocation of access rights or capabilities;

d) changes to subject or object security attributes;

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

e) policy checks performed by the TSF as a result of a request by a subject;

f) the use of access rights to bypass a policy check;

g) use of Identification and Authentication functions;

h) actions taken by an operator, and/or authorized user (such as. suppression of a TSF protection mechanism as human-readable labels);

i) import/export of data from/to removable media (such as printed output, tapes, USB sticks).

C.3.1.2 Evaluator notes

FAU_GEN.1.1 has a dependency on FPT_STM.1 Reliable time stamps. If correctness of time is not an issue for this TOE, elimination of this dependency can be justified by the author of a PP, PP-Module, functional package or ST.

C.3.2 FAU_GEN.1 Audit data generation

C.3.2.1 Component rationale and application notes

This component defines requirements to identify the auditable events for which audit records should be generated, and the information to be provided in the audit records.

FAU_GEN.1 Audit data generation by itself can be used when the SFRs do not require that individual user identities be associated with audit events. This can be appropriate when the PP, PP-Module, functional package or ST also contains privacy requirements. If the user identity needs to be incorporated FAU_GEN.2 User identity association can be used in addition to FAU_GEN.1.

If the subject is a user, the user identity may be recorded as the subject identity. The identity of the user may not yet have been verified if User authentication (FIA_UAU) has not been applied. Therefore, in the instance of an invalid login the claimed user identity should be recorded. It should also be considered whether to indicate when a recorded identity has not been authenticated.

C.3.2.2 Operations

In FAU_GEN.1.1, the author of a PP, PP-Module, functional package or ST should select the level of auditable events called out in the audit subclause of other functional components included in the PP, PP-Module, functional package or ST. This level is one of the following: “minimum”, “basic”, “detailed” or “not specified”.

In FAU_GEN.1.1, the author of a PP, PP-Module, functional package or ST should assign a list of other specifically defined auditable events to be included in the list of auditable events. The assignment may comprise none, or events that can be auditable events of a functional requirement that are of a higher audit level than requested in b), as well as the events generated through the use of a specified API.

In FAU_GEN.1.2, the author of a PP, PP-Module, functional package or ST should assign, for each of the auditable events included in the PP, PP-Module, functional package or ST, either a list of other audit relevant information to be included in audit events records or none.

C.3.3 FAU_GEN.2 User identity association

C.3.3.1 Component rationale and application notes

This component addresses the requirement of accountability of auditable events at the level of individual user identity. This component should be used in addition to FAU_GEN.1 Audit data generation.

There is a potential conflict between the audit and privacy requirements. For audit purposes, it can be desirable to know who performed an action. It is possible that a user wants to keep his/her actions to himself/herself and not be identified by other persons such as a site with job offers. Alternatively, it

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

can be required in the Organizational Security Policy that the identity of the users must be protected. In those cases, the objectives for audit and privacy can contradict each other. Therefore, if this requirement is selected and privacy is important, inclusion of the component user pseudonymity should be considered. Requirements on determining the real user name based on its pseudonym are specified in the privacy class.

If the identity of the user has not yet been verified through authentication, in the instance of an invalid login the claimed user identity should be recorded. It should be considered to indicate when a recorded identity has not been authenticated.

C.3.3.2 Operations

There are no operations specified for this component.

C.4 Security audit analysis (FAU_SAA)

C.4.1 User application notes

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

The action to be performed by the TSF on detection of a potential violation is defined in Security audit automatic response (FAU_ARP) components.

For real-time analysis, audit data can be transformed into a useful format for automated treatment, but into a different useful format for delivery to authorized users for review.

C.4.2 FAU_SAA.1 Potential violation analysis

C.4.2.1 Component rationale and application notes

This component is used to specify the set of auditable events whose occurrence or accumulated occurrence held to indicate a potential violation of the enforcement of the SFRs, and any rules to be used to perform the violation analysis.

C.4.2.2 Operations

In FAU_SAA.1.2, the author of a PP, PP-Module, functional package or ST should identify the subset of defined auditable events whose occurrence or accumulated occurrence need to be detected as an indication of a potential violation of the enforcement of the SFRs.

In FAU_SAA.1.2, the author of a PP, PP-Module, functional package or ST should specify any other rules that the TSF should use in its analysis of the audit trail. Those rules can include specific requirements to express the needs for the events to occur in a certain period of time. If there are no additional rules that the TSF should use in the analysis of the audit trail, this assignment can be completed with “none”.

EXAMPLE

Period of time: period of the day, duration.

C.4.3 FAU_SAA.2 Profile based anomaly detection

C.4.3.1 Component rationale and application notes

A *profile* is a structure that characterizes the behaviour of users and/or subjects; it represents how the users/subjects interact with the TSF in a variety of ways. Patterns of usage are established with respect

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

to the various types of activity the users/subjects engage in. The ways in which the various types of activity are recorded in the profile are referred to as *profile metrics*.

EXAMPLE 1

Patterns of usage: patterns in exceptions raised, patterns in resource utilization (when, which, how), patterns in actions performed.

Profile metrics: resource measures, event counters, timers.

Each profile represents the expected patterns of usage performed by members of the *profile target group*. This pattern may be based on past use (historical patterns) or on normal use for users of similar target groups (expected behaviour). A profile target group refers to one or more users who interact with the TSF. The activity of each member of the profile group is used by the analysis tool in establishing the usage patterns represented in the profile. The following are some examples of profile target groups:

a) **single user account**: one profile per user;

b) **group ID or group account**: one profile for all users who possess the same group ID or operate using the same group account;

c) **operating role**: one profile for all users sharing a given operating role;

d) **system**: one profile for all users of a system.

Each member of a profile target group is assigned an individual *suspicion rating* that represents how closely that member's new activity corresponds to the established patterns of usage represented in the group profile.

The sophistication of the anomaly detection tool will largely be determined by the number of target profile groups required by the PP, PP-Module, functional package or ST and the complexity of the required profile metrics.

The author of a PP, PP-Module, functional package or ST should enumerate specifically what activity should be monitored and/or analysed by the TSF. The author of a PP, PP-Module, functional package or ST should also identify specifically what information pertaining to the activity is necessary to construct the usage profiles.

FAU_SAA.2 Profile based anomaly detection requires that the TSF maintain profiles of system usage. The word maintain implies that the anomaly detector is actively updating the usage profile based on new activity performed by the profile target members. It is important here that the metrics for representing user activity are defined by the author of a PP, PP-Module, functional package or ST.

EXAMPLE 2

There can be a thousand different actions an individual can be capable of performing, but the anomaly detector can choose to monitor a subset of that activity.

Anomalous activity gets integrated into the profile just like non-anomalous activity (assuming the tool is monitoring those actions). Things that may have appeared anomalous four months ago, can over time become the norm (and vice-versa) as the user's work duties change. The TSF wouldn't be able to capture this notion if it filtered out anomalous activity from the profile updating algorithms.

Administrative notification should be provided such that the authorized user understands the significance of the suspicion rating.

The author of a PP, PP-Module, functional package or ST should define how to interpret suspicion ratings and the conditions under which anomalous activity is indicated to the Security audit automatic response (FAU_ARP) mechanism.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

C.4.3.2 Operations

In FAU_SAA.2.1, the author of a PP, PP-Module, functional package or ST should specify the profile target group. A single PP, PP-Module, functional package or ST may include multiple profile target groups.

In FAU_SAA.2.3, the author of a PP, PP-Module, functional package or ST should specify conditions under which anomalous activity is reported by the TSF. Conditions may include the suspicion rating reaching a certain value or be based on the type of anomalous activity observed.

C.4.4 FAU_SAA.3 Simple attack heuristics

C.4.4.1 Component rationale and application notes

In practice, it is at best rare when an analysis tool can detect with certainty when a security violation is imminent. However, there do exist some system events that are so significant that they are always worthy of independent review.

EXAMPLE 1

Example of such events include the deletion of a key TSF security data file (such as the password file) or activity such as a remote user attempting to gain administrative privilege.

These events are referred to as signature events in that their occurrence in isolation from the rest of the system activity are indicative of intrusive activity.

The complexity of a given tool will depend greatly on the assignments defined by the author of a PP, PP-Module, functional package or ST in identifying the base set of *signature events*.

The author of a PP, PP-Module, functional package or ST should enumerate specifically what events should be monitored by the TSF in order to perform the analysis. The author of a PP, PP-Module, functional package or ST should identify specifically what information pertaining to the event is necessary to determine if the event maps to a signature event.

Administrative notification should be provided such that the authorized user understands the significance of the event and the appropriate possible responses.

An effort was made in the specification of these requirements to avoid a dependency on audit data as the sole input for monitoring system activity. This was done in recognition of the existence of previously developed intrusion detection tools that do not perform their analyses of system activity solely through the use of audit data.

EXAMPLE 2

Examples of other input data include network datagrams, resource/accounting data, or combinations of various system data.

The elements of FAU_SAA.3 Simple attack heuristics do not require that the TSF implementing the immediate attack heuristics be the same TSF whose activity is being monitored. Thus, one can develop an intrusion detection component that operates independently of the system whose system activity is being analyzed.

C.4.4.2 Operations

In FAU_SAA.3.1, the author of a PP, PP-Module, functional package or ST should identify a base subset of system events whose occurrence, in isolation from all other system activity, can indicate a violation of the enforcement of the SFRs. These include events that by themselves indicate a clear violation to the enforcement of the SFRs, or whose occurrence is so significant that they warrant actions.

In FAU_SAA.3.2, the author of a PP, PP-Module, functional package or ST should specify the information used to determine system activity. This information is the input data used by the analysis tool to determine the system activity that has occurred on the TOE. This data may include audit data,

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

combinations of audit data with other system data, or may consist of data other than the audit data. The author of a PP, PP-Module, functional package or ST should define precisely what system events and event attributes are being monitored within the input data.

C.4.5 FAU_SAA.4 Complex attack heuristics

C.4.5.1 Component rationale and application notes

In practice, it is at best rare when an analysis tool can detect with certainty when a security violation is imminent. However, there do exist some system events that are so significant they are always worthy of independent review.

EXAMPLE 1

Example of such events include the deletion of a key TSF security data file (such as the password file) or activity such as a remote user attempting to gain administrative privilege.

These events are referred to as signature events in that their occurrence in isolation from the rest of the system activity are indicative of intrusive activity. Event sequences are an ordered set of signature events that can indicate intrusive activity.

The complexity of a given tool will depend greatly on the assignments defined by the author of a PP, PP-Module, functional package or ST in identifying the base set of signature events and event sequences.

The author of a PP, PP-Module, functional package or ST should enumerate specifically what events should be monitored by the TSF in order to perform the analysis. The author of a PP, PP-Module, functional package or ST should identify specifically what information pertaining to the event is necessary to determine if the event maps to a signature event.

Administrative notification should be provided such that the authorized user understands the significance of the event and the appropriate possible responses.

An effort was made in the specification of these requirements to avoid a dependency on audit data as the sole input for monitoring system activity. This was done in recognition of the existence of previously developed intrusion detection tools that do not perform their analyses of system activity solely through the use of audit data.

EXAMPLE 2

Examples of other input data include network datagrams, resource/accounting data, or combinations of various system data.

Levelling, therefore, requires the author of a PP, PP-Module, functional package or ST to specify the type of input data used to monitor system activity.

The elements of FAU_SAA.4 Complex attack heuristics do not require that the TSF implementing the complex attack heuristics be the same TSF whose activity is being monitored. Thus, one can develop an intrusion detection component that operates independently of the system whose system activity is being analyzed.

C.4.5.2 Operations

In FAU_SAA.4.1, the author of a PP, PP-Module, functional package or ST should identify a base set of lists of sequences of system events whose occurrence are representative of known penetration scenarios. These event sequences represent known penetration scenarios. Each event represented in the sequence should map to a monitored system event, such that as the system events are performed, they are bound (mapped) to the known penetration event sequences.

In FAU_SAA.4.1, the author of a PP, PP-Module, functional package or ST should identify a base subset of system events whose occurrence, in isolation from all other system activity, may indicate a violation of

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

the enforcement of the SFRs. These include events that by themselves indicate a clear violation to the SFRs, or whose occurrence is so significant they warrant action.

In FAU_SAA.4.2, the author of a PP, PP-Module, functional package or ST should specify the information used to determine system activity. This information is the input data used by the analysis tool to determine the system activity that has occurred on the TOE. This data may include audit data, combinations of audit data with other system data, or may consist of data other than the audit data. The author of a PP, PP-Module, functional package or ST should define precisely what system events and event attributes are being monitored within the input data.

C.5 Security audit review (FAU_SAR)

C.5.1 User application notes

The Security audit review family defines requirements related to review of the audit information.

These functions should allow pre-storage or post-storage audit selection.

EXAMPLE

An example of requirement related to review of the audit information is the ability to selectively review:

— the actions of one or more users (such as. identification, authentication, TOE entry, and access control actions);

— the actions performed on a specific object or TOE resource;

— all of a specified set of audited exceptions; or

— actions associated with a specific SFR attribute.

The distinction between audit reviews is based on functionality. Audit review (only) encompasses the ability to view audit data. Selectable review is more sophisticated and requires the ability to select subsets of audit data based on a single criterion or multiple criteria with logical (i.e. and/or) relations and order the audit data before it is reviewed.

C.5.2 FAU_SAR.1 Audit review

C.5.2.1 Component rationale and application notes

This component provides authorized users the capability to obtain and interpret the information. In the case of human users this information needs to be in a human understandable presentation. In the case of external IT entities, the information needs to be unambiguously represented in an electronic fashion.

This component is also used to specify that users and/or authorized users can read the audit records. These audit records will be provided in a manner appropriate to the user. There are different types of users (human users, machine users) that can have different needs.

The content of the audit records that can be viewed can be specified.

C.5.2.2 Operations

In FAU_SAR.1.1, the author of a PP, PP-Module, functional package or ST should specify the authorized users that can use this capability. If appropriate the author of a PP, PP-Module, functional package or ST may include security roles (see FMT_SMR.1 Security roles).

In FAU_SAR.1.1, the author of a PP, PP-Module, functional package or ST should specify the type of information the specified user is permitted to obtain from the audit records.

EXAMPLE

Examples are “all”, “subject identity”, “all information belonging to audit records referencing this user”.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

When employing the SFR, FAU_SAR.1, it is not necessary to repeat, in full detail, the list of audit information first specified in FAU_GEN.1. Use of terms such as "all" or "all audit information" assist in eliminating ambiguity and the further need for comparative analysis between the two security requirements.

C.5.3 FAU_SAR.2 Restricted audit review

C.5.3.1 Component rationale and application notes

This component specifies that any users not identified in FAU_SAR.1 Audit review will not be able to read the audit records.

C.5.3.2 Operations

There are no operations specified for this component.

C.5.4 FAU_SAR.3 Selectable audit review

C.5.4.1 Component rationale and application notes

This component is used to specify that it should be possible to perform selection of the audit data to be reviewed. If based on multiple criteria, those criteria should be related together with logical (i.e. "and" or "or") relations, and the tools should provide the ability to manipulate audit data

EXAMPLE

Means of manipulating audit data include sorting and filtering.

C.5.4.2 Operations

In FAU_SAR.3.1, the author of a PP, PP-Module, functional package or ST should specify whether capabilities to select and/or order audit data is required from the TSF.

In FAU_SAR.3.1, the author of a PP, PP-Module, functional package or ST should assign the criteria, possibly with logical relations, to be used to select the audit data for review. The logical relations are intended to specify whether the operation can be on an individual attribute or a collection of attributes.

EXAMPLE An example of this assignment can be: "application, user account and/or location".

In this case, the operation can be specified using any combination of the three attributes: application, user account and location.

C.6 Security audit event selection (FAU_SEL)

C.6.1 User application notes

The security audit event selection family provides requirements related to the capabilities of identifying which of the possible auditable events are to be audited. The auditable events are defined in the Security audit data generation (FAU_GEN) family, but those events should be defined as being selectable in this component to be audited.

This family ensures that it is possible to keep the audit trail from becoming so large that it becomes useless, by defining the appropriate granularity of the selected security audit events.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

C.6.2 FAU_SEL.1 Selective audit

C.6.2.1 Component rationale and application notes

This component defines the selection criteria used, and the resulting audited subsets of the set of all auditable events, based on user attributes, subject attributes, object attributes, or event types.

The existence of individual user identities is not assumed for this component. This allows for TOEs such as routers that may not support the notion of users.

For a distributed environment, the host identity can be used as a selection criterion for events to be audited.

The management function FMT_MTD.1 Management of TSF data will handle the rights of authorized users to query or modify the selections.

C.6.2.2 Operations

In FAU_SEL.1.1, the author of a PP, PP-Module, functional package or ST should select whether the security attributes upon which audit selectivity is based, is related to object identity, user identity, subject identity, host identity, or event type.

In FAU_SEL.1.1, the author of a PP, PP-Module, functional package or ST should specify any additional attributes upon which audit selectivity is based. If there are no additional rules upon which audit selectivity is based, this assignment can be completed with "none".

C.7 Security audit data storage (FAU_STG)

C.7.1 User application notes

The security audit data storage family describes requirements for storing audit data for later use, including requirements controlling the loss of audit information due to TOE failure, attack and/or exhaustion of storage space.

C.7.2 FAU_STG.1 Audit data storage location

C.7.2.1 Component rationale and application notes

In a distributed environment, as the location of the audit trail is in the TSF, but not necessarily co-located with the function generating the audit data, the author of a PP, PP-Module, functional package or ST can request authentication of the originator of the audit record, or non-repudiation of the origin of the record prior to storing this record in the audit trail.

The TSF will protect the stored audit records in the audit trail from unauthorised deletion and modification. It is noted that in some TOEs the auditor (role) can not be authorized to delete the audit records for a certain period of time.

FAU_STG.1.1 is dependent upon FTP_ITC.1 Inter-TSF trusted channel, if "transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC" is not selected then the author of a PP, PP-Module, functional package or ST can satisfy the dependency by providing the rationale explaining why it was not selected.

C.7.2.2 Operations

In FAU_STG.1.1the author of a PP, PP-Module, functional package or ST should select where the audit data is stored. Audit data may be stored on the TOE itself, be transmitted to an external entity using a trusted channel, or other storage options can be specified in the assignment.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

If additional or alternative storage locations for audit data need to be specified by the author of a PP, PP-Module, functional package or ST then this requirement can be specified in FAU_STG.1.1 using the assignment found within the selection.

C.7.3 FAU_STG.2 Protected audit data storage

C.7.3.1 Component rationale and application notes

In a distributed environment, as the location of the audit trail is in the TSF, but not necessarily co-located with the function generating the audit data, the author of a PP, PP-Module, functional package or ST can request authentication of the originator of the audit record, or non-repudiation of the origin of the record prior storing this record in the audit trail.

The TSF will protect the stored audit data in the audit trail from unauthorized deletion and modification. It is noted that in some TOEs the auditor (role) can not be authorized to delete the audit records for a certain period of time.

C.7.3.2 Operations

In FAU_STG.2.2, the author of a PP, PP-Module, functional package or ST should specify whether the TSF shall prevent or only be able to detect modifications of the stored audit data in the audit trail. Only one of these options may be chosen.

C.7.4 FAU_STG.3 Guarantees of audit data availability

C.7.4.1 Component rationale and application notes

This component allows the author of a PP, PP-Module, functional package or ST to specify to which metrics the audit trail should conform.

In a distributed environment, as the location of the audit trail is in the TSF, but not necessarily co-located with the function generating the audit data, the author of a PP, PP-Module, functional package or ST can request authentication of the originator of the audit record, or non-repudiation of the origin of the record prior storing this record in the audit trail.

C.7.4.2 Operations

In FAU_STG.3.3, PP, PP-Module, functional package or ST author should specify the metric that the TSF must ensure with respect to the stored audit records. This metric limits the data loss by enumerating the number of records that must be kept, or the time that records are guaranteed to be maintained.

EXAMPLE

An example of the metric can be “100,000” indicating that 100,000 audit records can be stored.

In FAU_STG.3.3 the author of a PP, PP-Module, functional package or ST should specify the condition under which the TSF shall still be able to maintain a defined amount of audit data. This condition can be any of the following: audit storage exhaustion, failure, attack.

C.7.5 FAU_STG.4 Prevention of audit data loss

C.7.5.1 Component rationale and application notes

This component specifies the behaviour of the TOE if the audit trail is full: either audit records are ignored, or the TOE is frozen such that no audited events can take place. The requirement also states that no matter how the requirement is instantiated, the authorized user with specific rights to this effect, can continue to generate audited events (actions). The reason is that otherwise the authorized user can not even reset the TOE. Consideration should be given to the choice of the action to be taken by the TSF in the case of audit storage exhaustion, as ignoring events, which provides better availability of

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

the TOE, will also permit actions to be performed without being recorded and without the user being accountable.

C.7.5.2 Operations

In FAU_STG.5.1, the author of a PP, PP-Module, functional package or ST should select whether the TSF shall ignore audited actions, or whether it should prevent audited actions from happening, or whether the oldest audit records should be overwritten when the TSF can no longer store audit records. Only one of these options may be chosen.

In FAU_STG.5.1, the author of a PP, PP-Module, functional package or ST should specify other actions that should be taken in case of audit storage failure, such as informing the authorized user. If there is no other action to be taken in case of audit storage failure, this assignment can be completed with "none".

C.7.6 FAU_STG.5 Action in case of possible audit data loss

C.7.6.1 Component rationale and application notes

This component requires that actions will be taken when the audit trail exceeds certain pre-defined limits.

C.7.6.2 Operations

In FAU_STG.5 Prevention of audit data loss, the author of a PP, PP-Module, functional package or ST should indicate the pre-defined limit. If the management functions indicate that this number can be changed by the authorized user, this value is the default value. The author of a PP, PP-Module, functional package or ST can choose to let the authorized user define this limit.

EXAMPLE

In the case that an authorized user defines the limit, an example of the assignment can be "an authorized user set limit".

In FAU_STG.5 Prevention of audit data loss, the author of a PP, PP-Module, functional package or ST should specify actions that should be taken in case of imminent audit storage failure indicated by exceeding the threshold. Actions can include informing an authorized user.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Annex D
(normative)

Class FCO: Communication — Application notes

D.1 General

This class describes requirements specifically of interest for TOEs that are used for the transport of information. Families within this class deal with non-repudiation.

In this class, the concept of "information" is used. This information should be interpreted as the object being communicated, and can contain an electronic mail message, a file, or a set of predefined attribute types.

In the literature, the terms "proof of receipt" and "proof of origin" are commonly used terms. However, it is recognized that the term "proof" can be interpreted in a legal sense to imply a form of mathematical rationale. The components in this class interpret the de-facto use of the word "proof" in the context of "evidence" that the TSF demonstrates the non-repudiated transport of types of information.

D.2 Non-repudiation of origin (FCO_NRO)

D.2.1 User application notes

Non-repudiation of origin defines requirements to provide evidence to users/subjects about the identity of the originator of some information. The originator cannot successfully deny having sent the information because evidence of origin provides evidence of the binding between the originator and the information sent. The recipient or a third party can verify the evidence of origin. This evidence should not be forgeable.

EXAMPLE 1

Evidence of origin can be a digital signature.

If the information or the associated attributes are altered in any way, validation of the evidence of origin can fail. Therefore, a PP, PP-Module, functional package or ST author should consider including integrity requirements such as FDP_UIT.1 Data exchange integrity in the PP, PP-Module, functional package or ST.

In non-repudiation, there are several different roles involved, each of which can be combined in one or more subjects. The first role is a subject that requests evidence of origin (only in FCO_NRO.1 Selective proof of origin). The second role is the recipient and/or other subjects to which the evidence is provided. The third role is a subject that requests verification of the evidence of origin.

EXAMPLE 2

Subject that requests evidence of origin: a recipient or a third party such as an arbiter.

Subject to which the evidence is provided: A notary.

The author of a PP, PP-Module, functional package or ST specifies the conditions that must be met to be able to verify the validity of the evidence.

EXAMPLE 3

An example of a condition which can be specified is where the verification of evidence must occur within 24 h.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

These conditions, therefore, allow the tailoring of the non-repudiation to legal requirements, such as being able to provide evidence for several years.

In most cases, the identity of the recipient will be the identity of the user who received the transmission. In some instances, the author of a PP, PP-Module, functional package or ST does not want the user identity to be exported. In that case, the author of a PP, PP-Module, functional package or ST considers whether it is appropriate to include this class, or whether the identity of the transport service provider or the identity of the host should be used.

In addition to (or instead of) the user identity, a PP, PP-Module, functional package or ST author can be more concerned about the time the information was transmitted.

EXAMPLE 4

For example, requests for proposals must be transmitted before a certain date in order to be considered.

In such instances, these requirements can be customized to provide a timestamp indication (time of origin).

D.2.2 FCO_NRO.1 Selective proof of origin

D.2.2.1 User application notes

There are no user application notes specified for this component.

D.2.2.2 Operations

In FCO_NRO.1.1, the author of a PP, PP-Module, functional package or ST should fill in the types of information subject to the evidence of origin function.

EXAMPLE 1

An example of the type of information is “electronic mail messages”.

In FCO_NRO.1.1, the author of a PP, PP-Module, functional package or ST should specify the user/subject who can request evidence of origin.

In FCO_NRO.1.1, the author of a PP, PP-Module, functional package or ST, dependent on the selection, should specify the third parties that can request evidence of origin.

EXAMPLE 2

A third party can be an arbiter, judge, or legal body.

In FCO_NRO.1.2, the author of a PP, PP-Module, functional package or ST should fill in the list of the attributes that shall be linked to the information.

EXAMPLE 3

Attributes include originator identity, time of origin, and location of origin.

In FCO_NRO.1.2, the author of a PP, PP-Module, functional package or ST should fill in the list of information fields within the information over which the attributes provide evidence of origin, such as the body of a message.

In FCO_NRO.1.3, the author of a PP, PP-Module, functional package or ST should specify the user/subject who can verify the evidence of origin.

In FCO_NRO.1.3, the author of a PP, PP-Module, functional package or ST should fill in the list of limitations under which the evidence can be verified.

EXAMPLE 4

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

An example of a limitation is "the evidence can only be verified within a 24-h time interval."

An assignment of "immediate" or "indefinite" is acceptable.

In FCO_NRO.1.3, the author of a PP, PP-Module, functional package or ST, dependent on the selection, should specify the third parties that can verify the evidence of origin.

D.2.3 FCO_NRO.2 Enforced proof of origin

D.2.3.1 User application notes

There are no user application notes specified for this component.

D.2.3.2 Operations

In FCO_NRO.2.1, the author of a PP, PP-Module, functional package or ST should fill in the types of information subject to the evidence of origin function.

EXAMPLE 1 Electronic mail messages.

In FCO_NRO.2.2, the author of a PP, PP-Module, functional package or ST should fill in the list of the attributes that shall be linked to the information; for example, originator identity, time of origin, and location of origin.

In FCO_NRO.2.2, the author of a PP, PP-Module, functional package or ST should fill in the list of information fields within the information over which the attributes provide evidence of origin, such as the body of a message.

In FCO_NRO.2.3, the author of a PP, PP-Module, functional package or ST should specify the user/subject who can verify the evidence of origin.

In FCO_NRO.2.3, the author of a PP, PP-Module, functional package or ST should fill in the list of limitations under which the evidence can be verified.

EXAMPLE 2 The evidence can only be verified within a 24-h time interval.

An assignment of "immediate" or "indefinite" is acceptable.

In FCO_NRO.2.3, the author of a PP, PP-Module, functional package or ST, dependent on the selection, should specify the third parties that can verify the evidence of origin.

EXAMPLE 3 A third party can be an arbiter, judge, or legal body.

D.3 Non-repudiation of receipt (FCO_NRR)

D.3.1 User application notes

Non-repudiation of receipt defines requirements to provide evidence to other users/subjects that the information was received by the recipient. The recipient cannot successfully deny having received the information because evidence of receipt provides evidence of the binding between the recipient attributes and the information. The originator or a third party can verify the evidence of receipt. This evidence should not be forgeable.

EXAMPLE 1 An example of a receipt is a digital signature.

It should be noted that the provision of evidence that the information was received does not necessarily imply that the information was read or comprehended, but only delivered.

If the information or the associated attributes are altered in any way, validation of the evidence of receipt with respect to the original information can fail. Therefore, a PP, PP-Module, functional package

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

or ST author should consider including integrity requirements such as FDP_UIT.1 Data exchange integrity in the PP, PP-Module, functional package or ST.

In non-repudiation, there are several different roles involved, each of which can be combined in one or more subjects. The first role is a subject that requests evidence of receipt (only in FCO_NRR.1 Selective proof of receipt). The second role is the recipient and/or other subjects to which the evidence is provided). The third role is a subject that requests verification of the evidence of receipt, for example, an originator or a third party such as an arbiter.

EXAMPLE 2 A recipient or subject can be a notary.

The author of a PP, PP-Module, functional package or ST specifies the conditions that must be met to be able to verify the validity of the evidence.

EXAMPLE 3

An example of a condition which can be specified is where the verification of evidence must occur within 24 h.

These conditions, therefore, allow the tailoring of the non-repudiation to legal requirements, such as being able to provide evidence for several years.

In most cases, the identity of the recipient will be the identity of the user who received the transmission. In some instances, the author of a PP, PP-Module, functional package or ST does not want the user identity to be exported. In that case, the author of a PP, PP-Module, functional package or ST considers whether it is appropriate to include this class, or whether the identity of the transport service provider or the identity of the host should be used.

In addition to (or instead of) the user identity, a PP, PP-Module, functional package or ST author can be more concerned about the time the information was received.

EXAMPLE 4 When an offer expires at a certain date, orders must be received before a certain date in order to be considered.

In such instances, these requirements can be customized to provide a timestamp indication (time of receipt).

D.3.2 FCO_NRR.1 Selective proof of receipt

D.3.2.1 User application notes

There are no user application notes specified for this component.

D.3.2.2 Operations

In FCO_NRR.1.1, the author of a PP, PP-Module, functional package or ST should fill in the types of information subject to the evidence of receipt function, for example, electronic mail messages.

In FCO_NRR.1.1, the author of a PP, PP-Module, functional package or ST should specify the user/subject who can request evidence of receipt.

In FCO_NRR.1.1, the author of a PP, PP-Module, functional package or ST, dependent on the selection, should specify the third parties that can request evidence of receipt.

EXAMPLE A third party can be an arbiter, judge, or legal body.

In FCO_NRR.1.2, the author of a PP, PP-Module, functional package or ST should fill in the list of the attributes that shall be linked to the information; for example, recipient identity, time of receipt, and location of receipt.

In FCO_NRR.1.2, the author of a PP, PP-Module, functional package or ST should fill in the list of information fields with the fields within the information over which the attributes provide evidence of receipt, such as the body a message.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

In FCO_NRR.1.3, the author of a PP, PP-Module, functional package or ST should specify the user/subjects who can verify the evidence of receipt.

In FCO_NRR.1.3, the author of a PP, PP-Module, functional package or ST should fill in the list of limitations under which the evidence can be verified. For example, the evidence can only be verified within a 24-hour time interval. An assignment of "immediate" or "indefinite" is acceptable.

In FCO_NRR.1.3, the author of a PP, PP-Module, functional package or ST, dependent on the selection, should specify the third parties that can verify the evidence of receipt.

D.3.3 FCO_NRR.2 Enforced proof of receipt

D.3.3.1 User application notes

There are no user application notes specified for this component.

D.3.3.2 Operations

In FCO_NRR.2.1, the author of a PP, PP-Module, functional package or ST should fill in the types of information subject to the evidence of receipt function.

EXAMPLE 1 Electronic mail messages.

In FCO_NRR.2.2, the author of a PP, PP-Module, functional package or ST should fill in the list of the attributes that shall be linked to the information.

EXAMPLE 2 Recipient identity, time of receipt, and location of receipt.

In FCO_NRR.2.2, the author of a PP, PP-Module, functional package or ST should fill in the list of information fields with the fields within the information over which the attributes provide evidence of receipt, such as the body of a message.

In FCO_NRR.2.3, the author of a PP, PP-Module, functional package or ST should specify the user/subjects who can verify the evidence of receipt.

In FCO_NRR.2.3, the author of a PP, PP-Module, functional package or ST should fill in the list of limitations under which the evidence can be verified. An assignment of "immediate" or "indefinite" is acceptable.

EXAMPLE 3 When the evidence can only be verified within a 24-h time interval.

In FCO_NRR.2.3, the author of a PP, PP-Module, functional package or ST, dependent on the selection, should specify the third parties that can verify the evidence of receipt. A third party can be an arbiter, judge or legal body.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Annex E
(normative)

Class FCS: Cryptographic support — Application notes

E.1 General

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;

— data separation.

This class is used when the TOE implements cryptographic functions, the implementation of which can be in hardware, firmware and/or software.

The FCS: Cryptographic support class is composed of four families: Cryptographic key management (FCS_CKM), Cryptographic operation (FCS_COP), Random bit generation (FCS_RBG), and Generation of random numbers (FCS_RNG).

The Cryptographic key management (FCS_CKM) family addresses the management aspects of cryptographic keys; the Cryptographic operation (FCS_COP) family is concerned with the operational use of those cryptographic keys; the Random bit generation (FCS_RBG) family provides requirements for generating random bits; and the Generation of random numbers (FCS_RNG) is concerned with ensuring that random numbers meet defined quality metrics.

For each cryptographic key generation method implemented by the TOE, if any, the author of a PP, PP-Module, functional package or ST should select the FCS_CKM.1 Cryptographic key generation component.

For each cryptographic key distribution method implemented by the TOE, if any, the author of a PP, PP-Module, functional package or ST should select the FCS_CKM.2 Cryptographic key distribution.

For each cryptographic key access method implemented by the TOE, if any, the author of a PP, PP-Module, functional package or ST should select the FCS_CKM.3 Cryptographic key access.

For each cryptographic key derivation method implemented by the TOE, if any, the author of a PP, PP-Module, functional package or ST should select the FCS_CKM.5 Cryptographic key derivation.

For each cryptographic key destruction method implemented by the TOE, if any, the author of a PP, PP-Module, functional package or ST should select the FCS_CKM.6 Timing and event of cryptographic key destruction component.

For each cryptographic operation (such as digital signature, data encryption, key agreement, secure hash, etc.) performed by the TOE, if any, the author of a PP, PP-Module, functional package or ST should select the FCS_COP.1 Cryptographic operation component.

For each deterministic random bit generation service implemented by the TOE, if any, the author of a PP, PP-Module, functional package or ST should select the FCS_RBG.1 Random bit generation (RBG) component.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

For each external seeding source used by the TOE, if any, the author of a PP, PP-Module, functional package or ST should select the FCS_RBG.2 Random bit generation (external seeding) component.

For each internal seeding source (single) used by the TOE, if any, the author of a PP, PP-Module, functional package or ST should select the FCS_RBG.3 Random bit generation (internal seeding – single source) component.

Where internal seeding source (multiple) is to be specified, the author of a PP, PP-Module, functional package or ST should select the FCS_RBG.4 Random bit generation (internal seeding – multiple sources) component.

For cases where the TOE combines entropy sources, the FCS_RBG.5 Random bit generation (combining noise sources) component should be specified by PP, PP-Module, functional package or ST author.

For each random bit generation service implemented by the TOE, the author of a PP, PP-Module, functional package or ST should specify the FCS_RBG.6 Random bit generation service component.

For each random number generation service implemented by the TOE, the author of a PP, PP-Module, functional package or ST should specify the FCS_RNG.1 Random number generation component.

Cryptographic functionality may be used to meet objectives specified in class FCO: Communication, and in families Data authentication (FDP_DAU), Stored data integrity (FDP_SDI), Inter-TSF user data confidentiality transfer protection (FDP_UCT), Inter-TSF user data integrity transfer protection (FDP_UIT), Specification of secrets (FIA_SOS), User authentication (FIA_UAU), to meet a variety of objectives. In the cases where cryptographic functionality is used to meet objectives for other classes, the individual functional components specify the objectives that cryptographic functionality must satisfy. The objectives in class FCS: Cryptographic support should be used when assurance for the cryptographic functionality of the TOE is sought by consumers.

E.2 Cryptographic key management (FCS_CKM)

E.2.1 User application notes

Cryptographic keys need to be managed throughout their lifetime. The typical events in the lifecycle of a cryptographic key include but are not limited to key generation or derivation, distribution, entry, storage, access, and destruction.

EXAMPLE 1

— backup;

— escrow;

— archive;

— recovery.

The inclusion of other stages is dependent on the key management strategy being implemented, as the TOE is not always involved in all of the key life-cycle phases.

EXAMPLE 2 The TOE may only generate and distribute cryptographic keys.

This family is intended to support the cryptographic key lifecycle and consequently defines requirements for the following activities:

— cryptographic key generation;

— cryptographic key derivation;

— cryptographic key distribution;

— cryptographic key access;

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

— cryptographic key destruction.

This family should be included whenever there are functional requirements for the management of cryptographic keys.

If Security audit data generation (FAU_GEN) is included in the PP, PP-Module, functional package or ST then, in the context of the events being audited:

a) the object attributes may include the assigned user for the cryptographic key, the user role, the cryptographic operation that the cryptographic key is to be used for, the cryptographic key identifier and the cryptographic key validity period;

b) the object value may include the values of cryptographic key(s) and parameters excluding any sensitive information (such as secret or private cryptographic keys).

Typically, random numbers are used to generate cryptographic keys. If this is the case, then FCS_CKM.1 Cryptographic key generation should be used instead of the component FIA_SOS.2 TSF Generation of secrets. In cases where random number generation is required for purposes other than for the generation of cryptographic keys, the component FIA_SOS.2 TSF Generation of secrets should be used.

E.2.2 Evaluator notes

Evaluators should refer to ISO/IEC 15408-1:2022, B.4 for information in regard to the use of standards specified in FCS_CKM.5.

FCS_CKM.5 has a dependency on FCS_CKM.6, The dependency should be understood as the dependency of two directions, 1) destruction of key derivation key and 2) destruction of derived keys. Evaluators should keep in mind that the dependency of two directions shall be fulfilled, and should also consider any intermediate values (such as those from key establishment) that should be destroyed in order to preserve the confidentiality of the key.

E.2.3 FCS_CKM.1 Cryptographic key generation

E.2.3.1 Component rationale and application notes

This component requires the cryptographic key sizes and method used to generate cryptographic keys to be specified, this may be in accordance with an assigned standard. It should be used to specify the cryptographic key sizes and the method used to generate the cryptographic keys. Only one instance of the component is needed for the same method and multiple key sizes. The key size may be common or different for the various entities and may be either the input to or the output from the method.

EXAMPLE An example of a method is an algorithm.

E.2.3.2 Operations

In FCS_CKM.1.1, the author of a PP, PP-Module, functional package or ST should specify the cryptographic key generation algorithm to be used.

In FCS_CKM.1.1, the author of a PP, PP-Module, functional package or ST should specify the cryptographic key sizes to be used. The key sizes specified should be appropriate for the algorithm and its intended use.

In FCS_CKM.1.1, the author of a PP, PP-Module, functional package or ST should specify the assigned standard that documents the method used to generate cryptographic keys. The assigned standard may comprise none, one or more actual standards publications, for example, from international, national, industry or organizational standards.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

E.2.4 FCS_CKM.2 Cryptographic key distribution

E.2.4.1 Component rationale and application notes

This component requires the method used to distribute cryptographic keys to be specified, this may be in accordance with an assigned standard. See ISO/IEC 15408-1 for information on using standards in PPs, PP-Modules, functional packages and STs.

E.2.4.2 Operations

In FCS_CKM.2.1 the author of a PP, PP-Module, functional package or ST should specify the cryptographic key distribution method to be used.

In FCS_CKM.2.1 the author of a PP, PP-Module, functional package or ST should specify the assigned standard that documents the method used to distribute cryptographic keys. The assigned standard may comprise none, one or more actual standards publications, for example, from international, national, industry or organizational standards.

E.2.5 FCS_CKM.3 Cryptographic key access

E.2.5.1 Component rationale and application notes

This component is intended to allow the specification of requirements on the usage of keys outside the TOE (e.g. backup, archival, escrow, recovery) and requires the methods used to access cryptographic keys be specified, this may be in accordance with an assigned standard.

FCS_CKM.3 Cryptographic key access is not intended to postulate the access control on cryptographic keys.

E.2.5.2 Operations

In FCS_CKM.3.1, the author of a PP, PP-Module, functional package or ST should specify the type of cryptographic key access being used.

EXAMPLE Examples of types of cryptographic key access include (but are not limited to) cryptographic key backup, cryptographic key archival, cryptographic key escrow, and cryptographic key recovery.

In FCS_CKM.3.1, the author of a PP, PP-Module, functional package or ST should specify the cryptographic key access method to be used.

In FCS_CKM.3.1, the author of a PP, PP-Module, functional package or ST should specify the assigned standard that documents the method used to access cryptographic keys. The assigned standard may comprise none, one or more actual standards publications, for example, from international, national, industry or organizational standards.

E.2.6 FCS_CKM.5 Cryptographic key derivation

E.2.6.1 Component rationale and application notes

This component requires the specification of the methods and parameters associated with the key derivation for a specified type of key.

FCS_CKM.5 has a dependency on FCS_CKM.6, The dependency should be understood as the dependency of two directions, 1) destruction of key derivation key, and 2) destruction of derived keys. PP, PP-Module, functional package and ST authors should keep in mind that the dependency of two directions shall be fulfilled and should also consider any intermediate values (such as those from key establishment) that should be destroyed in order to preserve the confidentiality of the key.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

E.2.6.2 Operations

There are no operations specified for this component.

E.2.7 FCS_CKM.6 Timing and event of cryptographic key destruction

E.2.7.1 Component rationale and application notes

This component requires the list of keys, including any keying material and the method used to destroy cryptographic keys to be specified, this can be in accordance with an assigned standard.

The purpose of the destruction of cryptographic keys and keying material is to prevent their recovery in consideration of threats related to their compromise.

NOTE 1 Keying material includes keys and initialization vectors necessary to establish and maintain cryptographic keying relationships.

NOTE 2 When a DRBG is used to generate a cryptographic key or any keying material, and the PP/ST author desires to protect the DRBG state to avoid the possibility that knowledge of this state can compromise the key or keying material, then the PP/ST author includes DRBG entropy input, seed input, and internal state of the DRBG in the assignment in FCS_CKM.6.1. See also FCS_RBG.1 regarding the destruction of the DRBG state using the uninstantiate operation.

E.2.7.2 Operations

In FCS_CKM.6.1, the author of a PP, PP-Module, functional package or ST provides a list of cryptographic keys and keying material that should be destroyed under certain circumstances.

In FCS_CKM.6.2, the author of a PP, PP-Module, functional package or ST provides the cryptographic key destruction method and the standards specifying the cryptographic key destruction method.

In FCS_CKM.6.1, the author of a PP, PP-Module, functional package or ST selects the circumstances of the destruction of key or key material.

E.3 Cryptographic operation (FCS_COP)

E.3.1 User application notes

A cryptographic operation may have cryptographic mode(s) of operation associated with it. If this is the case, then the cryptographic mode(s) shall be specified.

EXAMPLE

Examples of cryptographic modes of operation are cipher block chaining, output feedback mode, electronic code book mode, and cipher feedback mode.

Cryptographic operations may be used to support one or more TOE security services. The Cryptographic operation (FCS_COP) component can need to be iterated more than once depending on:

a) the user application for which the security service is being used;

b) the use of different cryptographic algorithms and/or cryptographic key sizes;

c) the type or sensitivity of the data being operated on.

If Security audit data generation (FAU_GEN) Security audit data generation is included in the PP, PP-Module, functional package or ST then, in the context of the cryptographic operation events being audited:

a) the types of cryptographic operation may include digital signature generation and/or verification, cryptographic checksum generation for integrity and/or for verification of checksum, secure hash

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

(message digest) computation, data encryption and/or decryption, cryptographic key encryption and/or decryption, cryptographic key agreement, and random number generation;

b) the subject attributes may include subject role(s) and user(s) associated with the subject;

c) the object attributes may include the assigned user for the cryptographic key, user role, cryptographic operation the cryptographic key is to be used for, cryptographic key identifier, and the cryptographic key validity period.

When specifying cryptographic operations, the author of a PP, PP-Module, functional package or ST should perform due diligence in order to have confidence that the specified cryptographic operations are appropriate for the selected assurance requirements and in consideration of the technology types, environment and use cases of the TOE.

NOTE In some cases, certification bodies can apply policies in regard to the selection of cryptographic operations. (See ISO/IEC 18045:2022, A.6 n).

E.3.2 FCS_COP.1 Cryptographic operation

E.3.2.1 Component rationale and application notes

This component requires the cryptographic algorithm and key size used to perform specified cryptographic operation(s) which can be based on an assigned standard.

The dependencies to FCS_RBG.1 or FCS_RNG.1 will be required for cryptographic algorithm operations which internally generate random numbers.

EXAMPLE 1 DSA signature generation, ECDSA signature generation, RSASSA-PSS signature generation.

The dependencies to FCS_RBG.1 or FCS_RNG.1 may not be necessary for deterministic cryptographic algorithm operations.

EXAMPLE 2 AES encryption / decryption in ECB mode.

E.3.2.2 Operations

In FCS_COP.1.1, the author of a PP, PP-Module, functional package or ST specifies the cryptographic operations being performed. Typical cryptographic operations include digital signature generation and/or verification, cryptographic checksum generation for integrity and/or for verification of checksum, secure hash (message digest) computation, data encryption and/or decryption, cryptographic key encryption and/or decryption, cryptographic key agreement, and random number generation. The cryptographic operation may be performed on user data or TSF data.

In FCS_COP.1.1, the author of a PP, PP-Module, functional package or ST should specify the cryptographic algorithm to be used.

EXAMPLE Examples of typical cryptographic algorithms include, but are not limited to, DES, RSA and IDEA.

In FCS_COP.1.1, the author of a PP, PP-Module, functional package or ST should specify the cryptographic key sizes to be used. The key sizes specified should be appropriate for the algorithm and its intended use.

In FCS_COP.1.1, the author of a PP, PP-Module, functional package or ST should specify the assigned standard that documents how the identified cryptographic operation(s) are performed. The assigned standard may comprise none, one or more actual standards publications, these may include standards from international, national, industry or organizational standards.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

E.4 Random bit generation (FCS_RBG)

E.4.1 User application notes

When specifying random bit generation methods, the author of a PP, PP-Module, functional package or ST should perform due diligence in order to have confidence that the specifications are appropriate for the selected assurance requirements and in consideration of the technology types, environment and use cases of the TOE.

NOTE In some cases, certification bodies can apply policies in regard to the selection of random bit generators. (See ISO/IEC 18045:2022, A.6 n).

E.4.2 FCS_RBG.1 Random bit generation (RBG)

E.4.2.1 Component rationale and application notes

For FCS_RBG.1, these dependencies shall always be met.

ISO/IEC 15408-1:2022, 8.3 c) allows a justification to be provided if a dependency is not met is not allowed for this component.

Reseeding is the typical mechanism for updating RBG state. If reseeding is not feasible, the TSF should uninstantiate RBGs rather than produce output that is of insufficient quality.

"Uninstantiate" means that the internal state of the RBG is no longer available for use.

The situation "never" should be selected only if the RBG cannot be reseeded or uninstantiated.

The situation "on demand" indicates that there is an interface to trigger reseeding or uninstantiating of the RBG, whether internal to the TOE or presented as a TSFI (e.g. an API call).

The situation "on the condition" allows the PP/ST author to specify application-specific conditions for reseeding.

The list of standards should specify the reseed interval, and procedures for uninstantiating and reseeding. This assignment should be "None" if the situation is "never."

Health tests for the RBG are specified in FPT_TST.1.

NOTE If a TOE needs to protect the DRBG state to avoid the possibility that knowledge of this state can compromise a key or keying material derived from its output, then the PP/ST author will include DRBG entropy input, seed input, and internal state of the DRBG in the assignment in an instance of FCS_CKM.6.1. This applies particularly where neither 'reseeding' nor 're-instantiating' apply in the last selection of FCS_RBG.1.3 (and therefore where a different method of destruction needs to be specified).

E.4.2.2 Operations

There are no operations specified for this component.

E.4.3 FCS_RBG.2 Random bit generation (external seeding)

E.4.3.1 Component rationale and application notes

For this component, the interface to obtain the entropy noise source can be used multiple times to provide input. For instance, if the input length is 128 bits, it can be used twice to gather 256 bits. In this instance, the 128 bits would not be provided to the DRBG, since the DRBG can only be instantiated once, rather a function would gather the 128 bits twice and provide the DRBG with 256 bits of entropy noise source.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

This component does not describe requirements on seed quality: It is the responsibility of the operational environment to define their requirement in this regard and to ensure that it is met by the external source.

Guidance in the introduction to PP, PP-Module, functional package or ST authors should address protection from modification and disclosure of the value from the external noise source, as well as the leaking of any pertinent information (e.g. internal state) regarding the RBG.

E.4.3.2 Operations

There are no operations specified for this component.

E.4.4 FCS_RBG.3 Random bit generation (internal seeding – single source)

E.4.4.1 Component rationale and application notes

If the author of a PP, PP-Module, functional package or ST wishes to use multiple internal noise sources, they iterate this requirement for each noise source being used by the TSF.

Hardware-based noise sources are sources whose primary function is noise generation, such as ring oscillators, diodes, and thermal noise. While software is used to collect the noise from these hardware sources, these are not software-based. Software-based noise sources are those sources that have some other primary function and the noise is a byproduct of their normal operation. Examples of software-based noise sources are user or system-based events, reading the least significant bits from an event timer.

Hardware-based noise sources may be stochastically modeled, in which case the amount of entropy is well understood. Software-based noise sources are usually less well understood and therefore will typically take a more conservative approach, gathering larger numbers of bits than required and then performing a compression function to derive the final output. Software-based noise sources often rely on an entropy estimator.

E.4.4.2 Operations

There are no operations specified for this component.

E.4.5 FCS_RBG.4 Random bit generation (internal seeding – multiple sources)

E.4.5.1 Component rationale and application notes

The minimum entropy is defined per source/iteration of FCS_RBG.3.1. The resulting minimum entropy is covered by FCS_RBG.5.1 which is a dependency of FCS_RBG.4.1.

E.4.6 FCS_RBG.6 Random bit generation service

E.4.6.1 Component rationale and application notes

Specifying the interface type is important for developing evaluation activities and important information for an external instance requesting the RBG service from the TOE.

E.4.6.2 Operations

Other interface types can be a service over a network interface.

EXAMPLE Ethernet, wireless.

IECNORM.COM: Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

E.5 Generation of random numbers (FCS_RNG)

E.5.1 User application notes

When specifying random number generation methods, the author of a PP, PP-Module, functional package or ST should perform due diligence in order to have confidence that the specifications are appropriate for the selected assurance requirements and in consideration of the technology types, environment and use cases of the TOE.

NOTE In some cases, certification bodies can apply policies in regard to the selection of random bit generators. (See ISO/IEC 18045:2022, A.6 n).

E.5.2 FCS_RNG.1 Random number generation

E.5.2.1 Component rationale and application notes

The ST writer shall perform the missing operation appropriate for cryptographic application of the random numbers in the elements FCS_RNG.1.1 and FCS_RNG_1.2. The ST writer shall perform the selections for specification of the security capabilities provided by the random number generator of the TOE.

NOTE Some users of FCS_RNG can find The National Institute of Standards and Technology (NIST) Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015 and NIST Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018 useful.

The evaluation of the random number generator shall follow a recognized methodology,

EXAMPLE An example of a recognized methodology is AIS31, published by the Bundesamt für Sicherheit in der Informationstechnik (BSI) organization.

E.5.2.2 Operations

In FCS_RNG.1.1 the author of a PP, PP-Module, functional package or ST should specify the list of security capabilities.

EXAMPLE 1

Examples of security capabilities include:

— a total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output;

— if a total failure of the entropy source occurs while the RNG is being operated, the RNG [selection: prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy];

— the online test detection non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected;

— the online test procedure be effective to detect non-tolerable weaknesses of the random numbers soon.

— the online test procedure checks the quality of the raw random number sequence. It is triggered [selection: externally, at regular intervals, continuously, applied upon specified internal events]. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time;

— failure or severe degradation of the noise source be detectable;

— continuous tests or other mechanisms in the entropy source protect against producing output during malfunctions.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

NOTE 1 In the case of a PP, PP-Module or functional package, FCS_RNG.1 .1 can be completed with a more restrictive language such as:

— assignment: list of additional security capabilities.

In FCS_RNG.1.2 the author of a PP, PP-Module, functional package or ST should make the appropriate selection in regard to the quality metric.

EXAMPLE 2

Examples of quality metrics include

— test procedure A [assignment: additional standard test suites] does not distinguish the internal random numbers from output sequences of an ideal RNG;

NOTE 2 The assignment for additional standard statistical test suite may be empty.

— the average Shannon entropy per internal random bit exceeds 0.998;

— each output bit is independent of all other output bits.

NOTE 3 In the case of a PP, PP-Module or functional package, FCS_RNG.1 .2 can be completed with a more restrictive language such as:

— [selection:

  — full entropy output;

  — [assignment: bias and entropy rate of the output].

NOTE 4 The “quality metric” can include both qualitative metric and quantitative metric.

EXAMPLE 3

In the case of a hybrid deterministic RNG, the following is an example:

“FCS_RNG.1.1/HD

The TSF shall provide a hybrid deterministic random number generator that implements: [selection: CTR_DRBG, Hash_DRBG, HMAC_DRBG] as defined in NIST Special Publication 800-90A.

FCS_RNG.1.2/HD

The TSF shall provide [selection: bits, octets of bits, numbers [assignment: format of the numbers]] that meet [assignment: security bits].”

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Annex F
(normative)

Class FDP: User data protection — Application notes

F.1 General

This class contains families specifying requirements related to protecting user data. This class differs from FIA and FPT in that FDP: User data protection specifies components to protect user data, FIA specifies components to protect attributes associated with the user, and FPT specifies components to protect TSF information.

The class does not contain explicit requirements for traditional Mandatory Access Controls (MAC) or traditional Discretionary Access Controls (DAC); however, such requirements may be constructed using components from this class.

FDP: User data protection does not explicitly deal with confidentiality, integrity, or availability, as all three are most often intertwined in the policy and mechanisms. However, the TOE security policy shall adequately cover these three objectives in the PP, PP-Module, functional package or ST.

A final aspect of this class is that it specifies access control in terms of “operations”. An operation is defined as a specific type of access on a specific object. It depends on the level of abstraction of the author of a PP, PP-Module, functional package or ST whether these operations are described as “read” and/or “write” operations, or as more complex operations such as “update the database”.

The access control policies are policies that control access to the information container. The attributes represent attributes of the container. Once the information is out of the container, the accessor is free to modify that information, including writing the information into a different container with different attributes. By contrast, an information flow policy controls access to the information, independent of the container. The attributes of the information, which may be associated with the attributes of the container (or may not, as in the case of a multi-level database) stay with the information as it moves. The accessor does not have the ability, in the absence of an explicit authorization, to change the attributes of the information.

This class is not meant to be a complete taxonomy of IT access policies, as others can be imagined. Those policies included here are simply those for which current experience with actual systems provides a basis for specifying requirements. There may be other forms of intent that are not captured in the definitions here.

EXAMPLE 1

A goal of having user-imposed (and user-defined) controls on information flow (such as. an automated implementation of the NO FOREIGN handling caveat).

Such concepts can be handled as refinements of, or extensions to the FDP: User data protection components.

Finally, it is important when looking at the components in FDP: User data protection to remember that these components are requirements for functions that may be implemented by a mechanism that also serves or can serve another purpose.

EXAMPLE 2

It is possible to build an access control policy (Access control policy (FDP_ACC)) that uses labels (FDP_IFF.1 Simple security attributes) as the basis of the access control mechanism.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

A set of SFRs may encompass many SFPs, each to be identified by the two policy-oriented components Access control policy (FDP_ACC), and Information flow control policy (FDP_IFC). These policies will typically take confidentiality, integrity, and availability aspects into consideration as required, to satisfy the TOE requirements. Care should be taken to ensure that all objects are covered by at least one SFP and that there are no conflicts arising from implementing the multiple SFPs.

When building a PP, PP-Module, functional package or ST using components from the FDP: User data protection class, the following information provides guidance on where to look and what to select from the class.

The requirements in the FDP: User data protection class are defined in terms of a set of SFRs that will implement an SFP. Since a TOE may implement multiple SFPs simultaneously, the author of a PP, PP-Module, functional package or ST shall specify the name for each SFP, so it can be referenced in other families. This name will then be used in each component selected to indicate that it is being used as part of the definition of requirements for that SFP. This allows the author to easily indicate the scope for operations, e.g. objects covered, operations covered, authorized users.

Each instantiation of a component can apply to only one SFP. Therefore, if an SFP is specified in a component then this SFP will apply to all the elements in this component. The components may be instantiated multiple times within a PP, PP-Module, functional package or ST to account for different policies if requested.

The key to selecting components from this family is to have a well-defined set of TOE security objectives to enable proper selection of the components from the two policy components; Access control policy (FDP_ACC) and Information flow control policy (FDP_IFC). In Access control policy (FDP_ACC) and Information flow control policy (FDP_IFC) respectively, all access control policies and all information flow control policies are named. Furthermore, the scope of control of these components in terms of the subjects, objects and operations covered by this security functionality. 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).

The following steps are guidance on how this class is applied in the construction of a PP, PP-Module, functional package or ST:

a) identify the policies to be enforced from the Access control policy (FDP_ACC), and Information flow control policy (FDP_IFC) families. These families define scope of control for the policy, granularity of control and may identify some rules to go with the policy;

b) identify the components and perform any applicable operations in the policy components. The assignment operations may be performed generally (such as with a statement “All files”) or specifically (“The files “A”, “B”, etc.) depending upon the level of detail known;

c) identify any applicable function components from the Access control functions (FDP_ACF) and Information flow control functions (FDP_IFF) families to address the named policy families from Access control policy (FDP_ACC) and Information flow control policy (FDP_IFC). Perform the operations to make the components define the rules to be enforced by the named policies. This should make the components fit the requirements of the selected function envisioned or to be built;

d) identify who will have the ability to control and change security attributes under the function, such as only a security administrator, only the owner of the object, etc. Select the appropriate components from FMT: Security management and perform the operations. Refinements may be useful here to identify missing features, such as that some or all changes shall be done via trusted path;

e) identify any appropriate components from the FMT: Security management for initial values for new objects and subjects;

f) identify any applicable rollback components from the Rollback (FDP_ROL) family;

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

g) identify any applicable residual information protection requirements from the Residual information protection (FDP_RIP) family;

h) identify any applicable import or export components, and how security attributes should be handled during import and export, from the Import from outside of the TOE (FDP_ITC) and Export from the TOE (FDP_ETC) families;

i) identify any applicable internal TOE communication components from the Internal TOE transfer (FDP_ITT) family;

j) identify any requirements for integrity protection of stored information from the Stored data integrity (FDP_SDI);

k) identify any applicable inter-TSF communication components from the Inter-TSF user data confidentiality transfer protection (FDP_UCT) or Inter-TSF user data integrity transfer protection (FDP_UIT) families.

F.2 Access control policy (FDP_ACC)

F.2.1 User application notes

This family is based upon the concept of arbitrary controls on the interaction of subjects and objects. The scope and purpose of the controls is based upon the attributes of the accessor (subject), the attributes of the container being accessed (object), the actions (operations) and any associated access control rules.

The components in this family are capable of identifying the access control SFPs (by name) to be enforced by the traditional DAC mechanisms. It further defines the subjects, objects and operations that are covered by identified access control SFPs. 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 defined in Access control 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."

The access control SFP covers a set of triplets: subject, object, and operations. Therefore, a subject can be covered by multiple access control SFPs but only with respect to a different operation or a different object. Of course, the same applies to objects and operations.

A critical aspect of an access control function that enforces an access control SFP is the ability for users to modify the attributes involved in access control decisions. The Access control policy (FDP_ACC) family does not address these aspects. Some of these requirements are left undefined, but can be added as refinements, while others are covered elsewhere in other families and classes such as FMT: Security management.

There are no audit requirements in Access control policy (FDP_ACC) as this family specifies access control SFP requirements. Audit requirements will be found in families specifying functions to satisfy the access control SFPs identified in this family.

This family provides a PP, PP-Module, functional package or ST author the capability to specify several policies, for example, a fixed access control SFP to be applied to one scope of control, and a flexible access control SFP to be defined for a different scope of control. To specify more than one access control policy, the components from this family can be iterated multiple times in a PP, PP-Module, functional package or ST to different subsets of operations and objects. This will accommodate TOEs that contain multiple policies, each addressing a particular set of operations and objects. In other words, the author of a PP, PP-Module, functional package or ST should specify the required information in the ACC component for each of the access control SFPs that the TSF will enforce. For example, a TOE incorporating three access control SFPs, each covering only a subset of the objects, subjects, and operations within the TOE, will contain one FDP_ACC.1 Subset access control component for each of the three access-control SFPs, necessitating a total of three FDP_ACC.1 Subset access control components.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.2.2 FDP_ACC.1 Subset access control

F.2.2.1 Component rationale and application notes

The terms object and subject refer to generic elements in the TOE. For a policy to be implementable, the entities shall be clearly identified. For a PP, the objects and operations can be expressed as types such as: named objects, data repositories, observe accesses, etc. For a specific TOE these generic terms (subject, object) shall be refined.

EXAMPLE Files, registers, ports, daemons, open calls.

This component specifies that the policy cover some well-defined set of operations on some subset of the objects. It places no constraints on any operations outside the set - including operations on objects for which other operations are controlled.

F.2.2.2 Operations

In FDP_ACC.1.1, the author of a PP, PP-Module, functional package or ST should specify a uniquely named access control SFP to be enforced by the TSF.

In FDP_ACC.1.1, the author of a PP, PP-Module, functional package or ST should specify the list of subjects, objects, and operations among subjects and objects covered by the SFP.

F.2.3 FDP_ACC.2 Complete access control

F.2.3.1 Component rationale and application notes

This component requires that all possible operations on objects, that are included in the SFP, are covered by an access control SFP.

The author of a PP, PP-Module, functional package or ST shall demonstrate that each combination of objects and subjects is covered by an access control SFP.

F.2.3.2 Operations

In FDP_ACC.2.1, the author of a PP, PP-Module, functional package or ST should specify a uniquely named access control SFP to be enforced by the TSF.

In FDP_ACC.2.1, the author of a PP, PP-Module, functional package or ST should specify the list of subjects and objects covered by the SFP. All operations among those subjects and objects will be covered by the SFP.

F.3 Access control functions (FDP_ACF)

F.3.1 User application notes

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

This family provides a PP, PP-Module, functional package or ST author the capability to describe the rules for access control. This results in a TOE where the access to objects will not change.

EXAMPLE 1

An example of such an object is “Message of the Day”, which is readable by all, and changeable only by the authorized administrator.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

This family also provides the author of a PP, PP-Module, functional package or ST with the ability to describe rules that provide for exceptions to the general access control rules. Such exceptions would either explicitly allow or deny authorization to access an object.

There are no explicit components to specify other possible functions such as two-person control, sequence rules for operations, or exclusion controls. However, these mechanisms, as well as traditional DAC mechanisms, can be represented with the existing components, by careful drafting of the access control rules.

A variety of acceptable access control functionality may be specified in this family.

EXAMPLE 2

— access control lists (ACLs);

— time-based access control specifications;

— origin-based access control specifications;

— owner-controlled access control attributes.

F.3.2 FDP_ACF.1 Security attribute-based access control

F.3.2.1 Component rationale and application notes

This component provides requirements for a mechanism that mediates access control based on security attributes associated with subjects and objects. Each object and subject have a set of associated attributes, such as location, time of creation, access rights such as Access Control Lists (ACLs)). This component allows the author of a PP, PP-Module, functional package or ST to specify the attributes that will be used for the access control mediation. This component allows access control rules, using these attributes, to be specified.

EXAMPLE

Examples of the attributes that a PP, PP-Module, functional package or ST author can assign are:

— an identity attribute may be associated with users, subjects, or objects to be used for mediation. Examples of such attributes can be the name of the program image used in the creation of the subject, or a security attribute assigned to the program image;

— a time attribute can be used to specify that access will be authorized during certain times of the day, during certain days of the week, or during a certain calendar year;

— a location attribute can specify whether the location is the location of the request for the operation, the location where the operation will be carried out, or both. It can be based upon internal tables to translate the logical interfaces of the TSF into locations such as through terminal locations, CPU locations, etc.;

— a grouping attribute allows a single group of users to be associated with an operation for the purposes of access control. If required, the refinement operation should be used to specify the maximum number of definable groups, the maximum membership of a group, and the maximum number of groups to which a user can concurrently be associated.

This component also provides requirements for the access control security functions to be able to explicitly authorize or deny access to an object based upon security attributes. This can be used to provide privilege, access rights, or access authorizations within the TOE. Such privileges, rights, or authorizations can apply to users, subjects (representing users or applications), and objects.

F.3.2.2 Operations

In FDP_ACF.1.1, the author of a PP, PP-Module, functional package or ST should specify an access control SFP name that the TSF is to enforce. The name of the access control SFP, and the scope of control for that policy are defined in components from Access control policy (FDP_ACC).

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

In FDP_ACF.1.1, the author of a PP, PP-Module, functional package or ST should specify, for each controlled subject and object, the security attributes and/or named groups of security attributes that the function will use in the specification of the rules.

EXAMPLE 1

Such attributes may be things such as the user identity, subject identity, role, time of day, location, ACLs, or any other attribute specified by the author of a PP, PP-Module, functional package or ST.

Named groups of security attributes can be specified to provide a convenient means to refer to multiple security attributes. Named groups can provide a useful way to associate "roles" defined in Security management roles (FMT_SMR), and all of their relevant attributes, with subjects. In other words, each role can relate to a named group of attributes.

In FDP_ACF.1.2, the author of a PP, PP-Module, functional package or ST should specify the SFP rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects. These rules specify when access is granted or denied. It can specify general access control functions or granular access control functions.

EXAMPLE 2

— General access control functions: typical permission bits;

— Granular access control: Access Control Lists (ACL).

In FDP_ACF.1.3, the author of a PP, PP-Module, functional package or ST should specify the rules, based on security attributes, that explicitly authorize access of subjects to objects that will be used to explicitly authorize access. These rules are in addition to those specified in FDP_ACF.1.1. They are included in FDP_ACF.1.3 as they are intended to contain exceptions to the rules in FDP_ACF.1.1.

EXAMPLE 3

An example of rules to explicitly authorize access is based on a privilege vector associated with a subject that always grants access to objects covered by the access control SFP that has been specified.

If such a capability is not desired, then the author of a PP, PP-Module, functional package or ST should specify "none".

In FDP_ACF.1.4, the author of a PP, PP-Module, functional package or ST should specify the rules, based on security attributes, that explicitly deny access of subjects to objects. These rules are in addition to those specified in FDP_ACF.1.1 . They are included in FDP_ACF.1.4 as they are intended to contain exceptions to the rules in FDP_ACF.1.1 . An example of rules to explicitly deny access is based on a privilege vector associated with a subject that always denies access to objects covered by the access control SFP that has been specified. If such a capability is not desired, then the author of a PP, PP-Module, functional package or ST should specify "none".

F.4 Data authentication (FDP_DAU)

F.4.1 User application notes

This family describes specific functions that can be used to authenticate "static" data.

Components in this family are to be used when there is a requirement for "static" data authentication, i.e. where data is to be signed but not transmitted.

NOTE The non-repudiation of origin (FCO_NRO) family provides for non-repudiation of origin of information received during a data exchange.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.4.2 FDP_DAU.1 Basic Data Authentication

F.4.2.1 Component rationale and application notes

This component may be satisfied by one-way hash functions to generate a hash value for a definitive document that may be used as verification of the validity or authenticity of its information content.

EXAMPLE Cryptographic checksum, fingerprint, message digest.

F.4.2.2 Operations

In FDP_DAU.1.1, the author of a PP, PP-Module, functional package or ST should specify the list of objects or information types for which the TSF shall be capable of generating data authentication evidence.

In FDP_DAU.1.2, the author of a PP, PP-Module, functional package or ST should specify the list of subjects that will have the ability to verify data authentication evidence for the objects identified in the previous element. The list of subjects can be very specific, if the subjects are known, or it can be more generic and refer to a "type" of subject such as an identified role.

F.4.3 FDP_DAU.2 Data Authentication with Identity of Guarantor

F.4.3.1 Component rationale and application notes

This component additionally requires the ability to verify the identity of the user that provided the guarantee of authenticity

EXAMPLE A trusted third party.

F.4.3.2 Operations

In FDP_DAU.2.1, the author of a PP, PP-Module, functional package or ST should specify the list of objects or information types for which the TSF shall be capable of generating data authentication evidence.

In FDP_DAU.2.2, the author of a PP, PP-Module, functional package or ST should specify the list of subjects that will have the ability to verify data authentication evidence for the objects identified in the previous element as well as the identity of the user that created the data authentication evidence.

F.5 Export from the TOE (FDP_ETC)

F.5.1 User application notes

This family defines functions for TSF-mediated exporting of user data from the TOE such that its security attributes either can be explicitly preserved or can be ignored once it has been exported. Consistency of these security attributes are addressed by Inter-TSF TSF data consistency (FPT_TDC).

Export from the TOE (FDP_ETC) is concerned with limitations on export and association of security attributes with the exported user data.

This family, and the corresponding Import family Import from outside of the TOE (FDP_ITC), address how the TOE deals with user data transferred into and outside its control. In principle, this family is concerned with the TSF-mediated exporting of user data and its related security attributes.

A variety of activities can be involved here:

a) exporting of user data without any security attributes;

b) exporting user data including security attributes where the two are associated with one another and the security attributes unambiguously represent the exported user data.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

If there are multiple SFPs (access control and/or information flow control) then it may be appropriate to iterate these components once for each named SFP.

F.5.2 FDP_ETC.1 Export of user data without security attributes

F.5.2.1 Component rationale and application notes

This component is used to specify the TSF-mediated exporting of user data without the export of its security attributes.

F.5.2.2 Operations

In FDP_ETC.1.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) that will be enforced when exporting user data. The user data that this function exports is scoped by the assignment of these SFPs.

F.5.3 FDP_ETC.2 Export of user data with security attributes

F.5.3.1 Component rationale and application notes

The user data is exported together with its security attributes. The security attributes are unambiguously associated with the user data. There are several ways of achieving this association. One way that this can be achieved is by physically collocating the user data and the security attributes.

EXAMPLE On the same external media.

An alternative way is by using cryptographic techniques such as secure signatures to associate the attributes and the user data. Inter-TSF trusted channel (FTP_ITC) can be used to assure that the attributes are correctly received at the other trusted IT product while Inter-TSF TSF data consistency (FPT_TDC) can be used to make sure that those attributes are properly interpreted. Furthermore, Trusted path (FTP_TRP) can be used to make sure that the export is being initiated by the proper user.

F.5.3.2 Operations

In FDP_ETC.2.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) that will be enforced when exporting user data. The user data that this function exports is scoped by the assignment of these SFPs.

In FDP_ETC.2.5, the author of a PP, PP-Module, functional package or ST should specify any additional exportation control rules or "none" if there are no additional exportation control rules. These rules will be enforced by the TSF in addition to the access control SFPs and/or information flow control SFPs selected in FDP_ETC.2.1.

F.6 Information flow control policy (FDP_IFC)

F.6.1 User application notes

This family covers the identification of information flow control SFPs and, for each, specifies the scope of control of the SFP.

The components in this family are capable of identifying the information flow control SFPs to be enforced by the traditional MAC mechanisms that would be found in a TOE. However, they go beyond just the traditional MAC mechanisms and can be used to identify and describe non-interference policies and state-transitions. It further defines the subjects under control of the policy, the information under control of the policy, and operations which cause controlled information to flow to and from controlled subjects for each information flow control SFP in the TOE. The information flow control SFP will be defined by other families such as Information flow control functions (FDP_IFF) and Export from the TOE (FDP_ETC). The information flow control SFPs named here in Information flow control policy

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

(FDP_IFC) are intended to be used throughout the remainder of the functional components that have an operation that calls for an assignment or selection of an "information flow control SFP."

These components are quite flexible. They allow the domain of flow control to be specified and there is no requirement that the mechanism be based upon labels. The different elements of the information flow control components also permit different degrees of exception to the policy.

Each SFP covers a set of triplets: subject, information, and operations that cause information to flow to and from subjects. Some information flow control policies may be at a very low level of detail and explicitly describe subjects in terms of processes within an operating system. Other information flow control policies may be at a high level and describe subjects in the generic sense of users or input/output channels. If the information flow control policy is at too high a level of detail, it may not clearly define the desired IT security functions. In such cases, it is more appropriate to include such descriptions of information flow control policies as objectives. In this case the desired IT security functions can be specified as supportive of those objectives.

In the second component (FDP_IFC.2 Complete information flow control) each information flow control SFP will cover all possible operations that cause information covered by that SFP to flow to and from subjects covered by that SFP. Furthermore, all information flows will need to be covered by a SFP. Therefore, for each action that causes information to flow, there will be a set of rules that define whether the action is allowed. If there are multiple SFPs that are applicable for a given information flow, all involved SFPs shall allow this flow before it is permitted to take place.

An information flow control SFP covers a well-defined set of operations. The SFPs coverage may be "complete" with respect to some information flows, or it may address only some of the operations that affect the information flow.

An access control SFP controls access to the objects that contain information. An information flow control SFP controls access to the information, independent of its container. The attributes of the information, which may be associated with the attributes of the container (or may not, as in the case of a multi-level database) stay with the information as it flows. The accessor does not have the ability, in the absence of an explicit authorization, to change the attributes of the information.

Information flows and operations can be expressed at multiple levels. In the case of a ST, the information flows and operations can be specified at a system-specific level: TCP/IP packets flowing through a firewall based upon known IP addresses. For a PP, the information flows and operations can be expressed as types, e.g. email, data repositories, observe accesses.

The components in this family can be applied multiple times in a PP, PP-Module, functional package or ST to different subsets of operations and objects. This will accommodate TOEs that contain multiple policies, each addressing a particular set of objects, subjects, and operations.

F.6.2 FDP_IFC.1 Subset information flow control

F.6.2.1 Component rationale and application notes

This component requires that an information flow control policy apply to a subset of the possible operations in the TOE.

F.6.2.2 Operations

In FDP_IFC.1.1, the author of a PP, PP-Module, functional package or ST should specify a uniquely named information flow control SFP to be enforced by the TSF.

In FDP_IFC.1.1, the author of a PP, PP-Module, functional package or ST should specify the list of subjects, information, and operations which cause controlled information to flow to and from controlled subjects covered by the SFP. As mentioned above, the list of subjects can be at various levels of detail depending on the needs of the author of a PP, PP-Module, functional package or ST.

EXAMPLE It can specify users, machines, or processes.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Information can refer to data such as email or network protocols, or more specific objects similar to those specified under an access control policy. If the information that is specified is contained within an object that is subject to an access control policy, then both the access control policy and information flow control policy shall be enforced before the specified information can flow to or from the object.

F.6.3 FDP_IFC.2 Complete information flow control

F.6.3.1 Component rationale and application notes

This component requires that all possible operations that cause information to flow to and from subjects included in the SFP, are covered by an information flow control SFP.

The author of a PP, PP-Module, functional package or ST shall demonstrate that each combination of information flows and subjects is covered by an information flow control SFP.

F.6.3.2 Operations

In FDP_IFC.2.1, the author of a PP, PP-Module, functional package or ST should specify a uniquely named information flow control SFP to be enforced by the TSF.

In FDP_IFC.2.1, the author of a PP, PP-Module, functional package or ST should specify the list of subjects and information that will be covered by the SFP. All operations that cause that information to flow to and from subjects will be covered by the SFP. As mentioned above, the list of subjects can be at various levels of detail depending on the needs of the author of a PP, PP-Module, functional package or ST.

EXAMPLE The list can specify users, machines, or processes.

Information can refer to data such as email or network protocols, or more specific objects similar to those specified under an access control policy. If the information that is specified is contained within an object that is subject to an access control policy, then both the access control policy and information flow control policy shall be enforced before the specified information can flow to or from the object.

F.7 Information flow control functions (FDP_IFF)

F.7.1 User application notes

This family describes the rules for the specific functions that can implement the information flow control SFPs named in Information flow control policy (FDP_IFC), which also specifies the scope of control of the policies. It consists of two “trees:” one addressing the common information flow control function issues, and a second addressing illicit information flows (i.e. covert channels) with respect to one or more information flow control SFPs. This division arises because the issues concerning illicit information flows are, in some sense, orthogonal to the rest of an SFP. Illicit information flows are flows in violation of policy; thus, they are not a policy issue.

In order to implement strong protection against disclosure or modification in the face of untrusted software, controls on information flow are required. Access controls alone are not sufficient because they only control access to containers, allowing the information they contain to flow, without controls, throughout a system.

In this family, the phrase “types of illicit information flows” is used. This phrase may be used to refer to the categorization of flows as “Storage Channels” or “Timing Channels”, or it can refer to improved categorizations reflective of the needs of a PP, PP-Module, functional package or ST author.

The flexibility of these components allows the definition of a privilege policy within FDP_IFF.1 Simple security attributes and FDP_IFF.2 Hierarchical security attributes to allow the controlled bypass of all or part of a particular SFP. If there is a need for a predefined approach to SFP bypass, the author of a PP, PP-Module, functional package or ST should consider incorporating a privilege policy.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.7.2 FDP_IFF.1 Simple security attributes

F.7.2.1 Component rationale and application notes

This component requires security attributes on information, and on subjects that cause that information to flow and subjects that act as recipients of that information. The attributes of the containers of the information should also be considered if it is desired that they should play a part in information flow control decisions or if they are covered by an access control policy. This component specifies the key rules that are enforced and describes how security attributes are derived.

This component does not specify the details of how a security attribute is assigned (i.e. user versus process). Flexibility in policy is provided by having assignments that allow specification of additional policy and function requirements, as necessary.

This component also provides requirements for the information flow control functions to be able to explicitly authorize and deny an information flow based upon security attributes. This can be used to implement a privilege policy that covers exceptions to the basic policy defined in this component.

F.7.2.2 Operations

In FDP_IFF.1.1, the author of a PP, PP-Module, functional package or ST should specify the information flow control SFPs enforced by the TSF. The name of the information flow control SFP, and the scope of control for that policy are defined in components from Information flow control policy (FDP_IFC).

In FDP_IFF.1.1, the author of a PP, PP-Module, functional package or ST should specify, for each type of controlled subject and information, the security attributes that are relevant to the specification of the SFP rules.

EXAMPLE 1

Such security attributes can be things such the subject identifier, subject sensitivity label, subject clearance label, information sensitivity label.

The types of security attributes should be sufficient to support the environmental needs.

In FDP_IFF.1.2, the author of a PP, PP-Module, functional package or ST should specify for each operation, the security attribute-based relationship that holds between subject and information security attributes that the TSF will enforce.

In FDP_IFF.1.3, the author of a PP, PP-Module, functional package or ST should specify any additional information flow control SFP rules that the TSF is to enforce. This includes all rules of the SFP that are either not based on the security attributes of the information and the subject or rules that automatically modify the security attributes of information or subjects as a result of an access operation. An example for the first case is a rule of the SFP controlling a threshold value for specific types of information. This would for example be the case when the information flow SFP contains rules on access to statistical data where a subject is only allowed to access this type of information up to a specific number of accesses. An example for the second case would be a rule stating under which conditions and how the security attributes of a subject or object change as the result of an access operation. Some information flow policies for example may limit the number of access operations to information with specific security attributes. If there are no additional rules then the author of a PP, PP-Module, functional package or ST should specify “none”.

In FDP_IFF.1.4, the author of a PP, PP-Module, functional package or ST should specify the rules, based on security attributes, that explicitly authorize information flows. These rules are in addition to those specified in the preceding elements. They are included in FDP_IFF.1.4 as they are intended to contain exceptions to the rules in the preceding elements.

EXAMPLE 2

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

An example of rules to explicitly authorize information flows is based on a privilege vector associated with a subject that always grants the subject the ability to cause an information flow for information that is covered by the SFP that has been specified.

If such a capability is not desired, then the author of a PP, PP-Module, functional package or ST should specify "none".

In FDP_IFF.1.5, the author of a PP, PP-Module, functional package or ST should specify the rules, based on security attributes, that explicitly deny information flows. These rules are in addition to those specified in the preceding elements. They are included in FDP_IFF.1.5 as they are intended to contain exceptions to the rules in the preceding elements. An example of rules to explicitly deny information flows is based on a privilege vector associated with a subject that always denies the subject the ability to cause an information flow for information that is covered by the SFP that has been specified. If such a capability is not desired, then the author of a PP, PP-Module, functional package or ST should specify "none".

F.7.3 FDP_IFF.2 Hierarchical security attributes

F.7.3.1 Component rationale and application notes

This component requires that the named information flow control SFP uses hierarchical security attributes that form a lattice.

It is important to note that the hierarchical relationship requirements identified in FDP_IFF.2.4 need only apply to the information flow control security attributes for the information flow control SFPs that have been identified in FDP_IFF.2.1. This component is not meant to apply to other SFPs such as access control SFPs.

FDP_IFF.2.6 phrases the requirements for the set of security attributes to form a lattice. A number of information flow policies defined in the literature and implemented in IT products are based on a set of security attributes that form a lattice. FDP_IFF.2.6 is specifically included to address this type of information flow policies.

If it is the case that multiple information flow control SFPs are to be specified, and that each of these SFPs will have their own security attributes that are not related to one another, then the author of a PP, PP-Module, functional package or ST should iterate this component once for each of those SFPs. Otherwise, a conflict can arise with the sub-items of FDP_IFF.2.4 since the required relationships will not exist.

F.7.3.2 Operations

In FDP_IFF.2.1, the author of a PP, PP-Module, functional package or ST should specify the information flow control SFPs enforced by the TSF. The name of the information flow control SFP, and the scope of control for that policy are defined in components from Information flow control policy (FDP_IFC).

In FDP_IFF.2.1, the author of a PP, PP-Module, functional package or ST should specify, for each type of controlled subject and information, the security attributes that are relevant to the specification of the SFP rules. For example, such security attributes may be things such the subject identifier, subject sensitivity label, subject clearance label, information sensitivity label, etc. The types of security attributes should be sufficient to support the environmental needs.

In FDP_IFF.2.2, the author of a PP, PP-Module, functional package or ST should specify for each operation, the security attribute-based relationship that holds between a subject and the information security attributes that the TSF will enforce. These relationships should be based upon the ordering relationships between the security attributes.

In FDP_IFF.2.3, the author of a PP, PP-Module, functional package or ST should specify any additional information flow control SFP rules that the TSF is to enforce. This includes all rules of the SFP that are either not based on the security attributes of the information and the subject or rules that automatically

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

modify the security attributes of information or subjects as a result of an access operation. An example for the first case is a rule of the SFP controlling a threshold value for specific types of information.

EXAMPLE 1

This would for example be the case when the information flow SFP contains rules on access to statistical data where a subject is only allowed to access this type of information up to a specific number of accesses. An example for the second case would be a rule stating under which conditions and how the security attributes of a subject or object change as the result of an access operation.

Some information flow policies may limit the number of access operations to information with specific security attributes. If there are no additional rules then the author of a PP, PP-Module, functional package or ST should specify "none".

In FDP_IFF.2.4, the author of a PP, PP-Module, functional package or ST should specify the rules, based on security attributes, that explicitly authorize information flows. These rules are in addition to those specified in the preceding elements. They are included in FDP_IFF.2.4 as they are intended to contain exceptions to the rules in the preceding elements.

EXAMPLE 2

An example of rules to explicitly authorize information flows is based on a privilege vector associated with a subject that always grants the subject the ability to cause an information flow for information that is covered by the SFP that has been specified.

If such a capability is not desired, then the author of a PP, PP-Module, functional package or ST should specify "none".

In FDP_IFF.2.5, the author of a PP, PP-Module, functional package or ST should specify the rules, based on security attributes, that explicitly deny information flows. These rules are in addition to those specified in the preceding elements. They are included in FDP_IFF.2.5 as they are intended to contain exceptions to the rules in the preceding elements. An example of rules to explicitly deny information flows is based on a privilege vector associated with a subject that always denies the subject the ability to cause an information flow for information that is covered by the SFP that has been specified. If such a capability is not desired, then the author of a PP, PP-Module, functional package or ST should specify "none".

F.7.4 FDP_IFF.3 Limited illicit information flows

F.7.4.1 Component rationale and application notes

This component should be used when at least one of the SFPs that requires control of illicit information flows does not require elimination of flows.

For the specified illicit information flows, certain maximum capacities should be provided. In addition, a PP, PP-Module, functional package or ST author has the ability to specify whether the illicit information flows must be audited.

F.7.4.2 Operations

In FDP_IFF.3.1, the author of a PP, PP-Module, functional package or ST should specify the information flow control SFPs enforced by the TSF. The name of the information flow control SFP, and the scope of control for that policy are defined in components from Information flow control policy (FDP_IFC).

In FDP_IFF.3.1, the author of a PP, PP-Module, functional package or ST should specify the types of illicit information flows that are subject to a maximum capacity limitation.

In FDP_IFF.3.1, the author of a PP, PP-Module, functional package or ST should specify the maximum capacity permitted for any identified illicit information flows.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.7.5 FDP_IFF.4 Partial elimination of illicit information flows

F.7.5.1 Component rationale and application notes

This component should be used when all the SFPs that requires control of illicit information flows require elimination of some (but not necessarily all) illicit information flows.

F.7.5.2 Operations

In FDP_IFF.4.1, the author of a PP, PP-Module, functional package or ST should specify the information flow control SFPs enforced by the TSF. The name of the information flow control SFP, and the scope of control for that policy are defined in components from Information flow control policy (FDP_IFC).

In FDP_IFF.4.1, the author of a PP, PP-Module, functional package or ST should specify the types of illicit information flows which are subject to a maximum capacity limitation.

In FDP_IFF.4.1, the author of a PP, PP-Module, functional package or ST should specify the maximum capacity permitted for any identified illicit information flows.

In FDP_IFF.4.2, the author of a PP, PP-Module, functional package or ST should specify the types of illicit information flows to be eliminated. This list may not be empty as this component requires that some illicit information flows are to be eliminated.

F.7.6 FDP_IFF.5 No illicit information flows

F.7.6.1 Component rationale and application notes

This component should be used when the SFPs that require control of illicit information flows require elimination of all illicit information flows. However, the author of a PP, PP-Module, functional package or ST should carefully consider the potential impact that eliminating all illicit information flows can have on the normal functional operation of the TOE. Many practical applications have shown that there is an indirect relationship between illicit information flows and normal functionality within a TOE and eliminating all illicit information flows may result in less than desired functionality.

F.7.6.2 Operations

In FDP_IFF.5.1, the author of a PP, PP-Module, functional package or ST should specify the information flow control SFP for which illicit information flows are to be eliminated. The name of the information flow control SFP, and the scope of control for that policy are defined in components from Information flow control policy (FDP_IFC).

F.7.7 FDP_IFF.6 Illicit information flow monitoring

F.7.7.1 Component rationale and application notes

This component should be used when it is desired that the TSF provide the ability to monitor the use of illicit information flows that exceed a specified capacity. If it is desired that such flows be audited, then this component can serve as the source of audit events to be used by components from the Security audit data generation (FAU_GEN) family.

F.7.7.2 Operations

In FDP_IFF.6.1, the author of a PP, PP-Module, functional package or ST should specify the information flow control SFPs enforced by the TSF. The name of the information flow control SFP, and the scope of control for that policy are defined in components from Information flow control policy (FDP_IFC).

In FDP_IFF.6.1, the author of a PP, PP-Module, functional package or ST should specify the types of illicit information flows that will be monitored for exceeding a maximum capacity.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

In FDP_IFF.6.1, the author of a PP, PP-Module, functional package or ST should specify the maximum capacity above which illicit information flows will be monitored by the TSF.

NOTE Here the controlled subjects indicate both subjects that cause the information to flow and subjects that act as recipients of that information.

F.8 Information retention control (FDP_IRC)

F.8.1 User application notes

While a great aspect of the elimination of the objects as required by FDP_IRC refers to the information stored within the object as a container, it also includes all attributes (also in the meaning of metadata) that may be associated with the object.

In this aspect, the focus of FDP_IRC differs from other components related to access or information flow control policies, such as FDP_IFF and FDP_IFC. More important, objects here are always considered in the context of selected activities that are performed on these objects. In contrast to residual information protection (FDP_RIP), FDP_IRC excludes objects from any access or information flow and deletes them, irreversibly and untraceably when they are no longer needed by a set of activities.

While it may not be completely clear, which objects to consider, it is essential that the list of objects is assigned by the author of a PP, PP-Module, functional package or ST at the very latest in order to allow for concrete tests. In any case the list of objects shall be derived from a structured analysis.

F.8.2 FDP_IRC.1 Information retention control

F.8.2.1 Component rationale and application notes

The information erasure policy as defined in FDP_IRC.1 serves to protect all information that is contained in the assigned objects from being misused, regardless of whether the information is primary content or any kind of attribute. The policy covers combinations of objects and activities. The policy's coverage may be "complete" with respect to all the objects related to one or more activities, or it may address only some of the objects related to one or more activities.

The term "promptly" in FDP_IRC.1 specifically refers to the fact that the objects shall be terminated in a manner that ensures that they cannot be accessed as before.

F.8.2.2 Operations

In FDP_IRC.1.1, the author of a PP, PP-Module, functional package or ST should specify a uniquely named information erasure policy to be enforced by the TSF.

In FDP_IRC.1.1, the author of a PP, PP-Module, functional package or ST should specify the list of objects that are required for the respective list of activities, e.g. "all message objects".

In FDP_IRC.1.1, the author of a PP, PP-Module, functional package or ST should specify the list of activities that the information erasure policy is concerned with, e.g. "all activities related to passing a message on, such as receiving a message, cryptographic handling of a message, sending a message".

In FDP_IRC.1.2, the author of a PP, PP-Module, functional package or ST should specify the list of objects that are required for the respective list of activities. This assignment shall be identical to the assigned objects in FDP_IRC.1.1.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.9 Import from outside of the TOE (FDP_ITC)

F.9.1 User application notes

This family defines mechanisms for TSF-mediated importing of user data from outside the TOE into the TOE such that the user data security attributes can be preserved. Consistency of these security attributes are addressed by Inter-TSF TSF data consistency (FPT_TDC).

Import from outside of the TOE (FDP_ITC) is concerned with limitations on import, user specification of security attributes, and association of security attributes with the user data.

This family, and the corresponding export family Export from the TOE (FDP_ETC), address how the TOE deals with user data outside its control. This family is concerned with assigning and abstraction of the user data security attributes.

EXAMPLE 1

A variety of activities can be involved here:

a) importing user data from an unformatted medium (e.g. tape, scanner, video or audio signal), without including any security attributes, and physically marking the medium to indicate its contents;

b) importing user data, including security attributes, from a medium and verifying that the object security attributes are appropriate;

c) importing user data, including security attributes, from a medium using a cryptographic sealing technique to protect the association of user data and security attributes.

This family is not concerned with the determination of whether the user data may be imported. It is concerned with the values of the security attributes to associate with the imported user data.

There are two possibilities for the import of user data: either the user data is unambiguously associated with reliable object security attributes (values and meaning of the security attributes is not modified), or no reliable security attributes (or no security attributes at all) are available from the import source. This family addresses both cases.

If there are reliable security attributes available, they may have been associated with the user data by physical means (the security attributes are on the same media), or by logical means (the security attributes are distributed differently but include unique object identification).

EXAMPLE 2 Cryptographic checksum.

This family is concerned with TSF-mediated importing of user data and maintaining the association of security attributes as required by the SFP. Other families are concerned with other import aspects such as consistency, trusted channels, and integrity that are beyond the scope of this family. Furthermore, Import from outside of the TOE (FDP_ITC) is only concerned with the interface to the import medium. Export from the TOE (FDP_ETC) is responsible for the other end point of the medium (the source).

Some of the well-known import requirements are:

a) importing of user data without any security attributes;

b) importing of user data including security attributes where the two are associated with one another and the security attributes unambiguously represent the information being imported.

These import requirements may be handled by the TSF with or without human intervention, depending on the IT limitations and the organizational security policy. For example, if user data is received on a “confidential” channel, the security attributes of the objects will be set to “confidential”.

If there are multiple SFPs (access control and/or information flow control) then it may be appropriate to iterate these components once for each named SFP.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.9.2 FDP_ITC.1 Import of user data without security attributes

F.9.2.1 Component rationale and application notes

This component is used to specify the import of user data that does not have reliable (or any) security attributes associated with it. This function requires that the security attributes for the imported user data be initialized within the TSF. It can also be the case that the author of a PP, PP-Module, functional package or ST specifies the rules for import. It may be appropriate, in some environments, to require that these attributes be supplied via a trusted path or a trusted channel mechanism.

F.9.2.2 Operations

In FDP_ITC.1.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) that will be enforced when importing user data from outside of the TOE. The user data that this function imports is scoped by the assignment of these SFPs.

In FDP_ITC.1.3, the author of a PP, PP-Module, functional package or ST should specify any additional importation control rules or "none" if there are no additional importation control rules. These rules will be enforced by the TSF in addition to the access control SFPs and/or information flow control SFPs selected in FDP_ITC.1.1.

F.9.3 FDP_ITC.2 Import of user data with security attributes

F.9.3.1 Component rationale and application notes

This component is used to specify the import of user data that has reliable security attributes associated with it. This function relies upon the security attributes that are accurately and unambiguously associated with the objects on the import medium. Once imported, those objects will have those same attributes. This requires Inter-TSF TSF data consistency (FPT_TDC) to ensure the consistency of the data. It can also be the case that the author of a PP, PP-Module, functional package or ST specifies the rules for import.

F.9.3.2 Operations

In FDP_ITC.2.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) that will be enforced when importing user data from outside of the TOE. The user data that this function imports is scoped by the assignment of these SFPs.

In FDP_ITC.2.5, the author of a PP, PP-Module, functional package or ST should specify any additional importation control rules or "none" if there are no additional importation control rules. These rules will be enforced by the TSF in addition to the access control SFPs and/or information flow control SFPs selected in FDP_ITC.2.1.

F.10 Internal TOE transfer (FDP_ITT)

F.10.1 User application notes

This family provides requirements that address protection of user data when it is transferred between parts of a TOE across an internal channel. This may be contrasted with the Inter-TSF user data confidentiality transfer protection (FDP_UCT) and Inter-TSF user data integrity transfer protection (FDP_UIT) family, which provide protection for user data when it is transferred between distinct TSFs across an external channel, and Export from the TOE (FDP_ETC) and Import from outside of the TOE (FDP_ITC), which address TSF-mediated transfer of data to or from outside the TOE.

The requirements in this family allow a PP, PP-Module, functional package or ST author to specify the desired security for user data while in transit within the TOE. This security can be protection against disclosure, modification, or loss of availability.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The determination of the degree of physical separation above which this family should apply depends on the intended environment of use. In a hostile environment, there may be risks arising from transfers between parts of the TOE separated by only a system bus. In more benign environments, the transfers may be across more traditional network media.

If there are multiple SFPs (access control and/or information flow control) then it may be appropriate to iterate these components once for each named SFP.

F.10.2 FDP_ITT.1 Basic internal transfer protection

F.10.2.1 Component rationale and application notes

No component rationale or application notes have been given.

F.10.2.2 Operations

In FDP_ITT.1.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) covering the information being transferred.

In FDP_ITT.1.1, the author of a PP, PP-Module, functional package or ST should specify the types of transmission errors that the TSF should prevent occurring for user data while in transport. The options are disclosure, modification, loss of use.

F.10.3 FDP_ITT.2 Transmission separation by attribute

F.10.3.1 Component rationale and application notes

This component can, for example, be used to provide different forms of protection to information with different clearance levels.

One of the ways to achieve separation of data when it is transmitted is through the use of separate logical or physical channels.

F.10.3.2 Operations

In FDP_ITT.2.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) covering the information being transferred.

In FDP_ITT.2.1, the author of a PP, PP-Module, functional package or ST should specify the types of transmission errors that the TSF should prevent occurring for user data while in transport. The options are disclosure, modification, loss of use.

In FDP_ITT.2.2, the author of a PP, PP-Module, functional package or ST should specify the security attributes, the values of which the TSF will use to determine when to separate data that is being transmitted between physically-separated parts of the TOE. An example is that user data associated with the identity of one owner is transmitted separately from the user data associated with the identify of a different owner. In this case, the value of the identity of the owner of the data is what is used to determine when to separate the data for transmission.

F.10.4 FDP_ITT.3 Integrity monitoring

F.10.4.1 Component rationale and application notes

This component is used in combination with either FDP_ITT.1 Basic internal transfer protection or FDP_ITT.2 Transmission separation by attribute. It ensures that the TSF checks received user data (and their attributes) for integrity. FDP_ITT.1 Basic internal transfer protection or FDP_ITT.2 Transmission separation by attribute will provide the data in a manner such that it is protected from modification (so that FDP_ITT.3 Integrity monitoring can detect any modifications).

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

The author of a PP, PP-Module, functional package or ST shall specify the types of errors that must be detected. The author of a PP, PP-Module, functional package or ST should consider: modification of data, substitution of data, unrecoverable ordering change of data, replay of data, incomplete data, in addition to other integrity errors.

The author of a PP, PP-Module, functional package or ST specifies the actions that the TSF should take on detection of a failure.

EXAMPLE

Ignore the user data, request the data again, inform the authorized administrator, reroute traffic for other lines.

F.10.4.2 Operations

In FDP_ITT.3.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) covering the information being transferred and monitored for integrity errors.

In FDP_ITT.3.1, the author of a PP, PP-Module, functional package or ST should specify the type of possible integrity errors to be monitored during transmission of the user data.

In FDP_ITT.3.2, the author of a PP, PP-Module, functional package or ST should specify the action to be taken by the TSF when an integrity error is encountered.

EXAMPLE

The TSF should request the resubmission of the user data. The SFP(s) specified in FDP_ITT.3.1 will be enforced as the actions are taken by the TSF.

F.10.5 FDP_ITT.4 Attribute-based integrity monitoring

F.10.5.1 Component rationale and application notes

This component is used in combination with FDP_ITT.2 Transmission separation by attribute. It ensures that the TSF checks received user data, that has been transmitted by separate channels (based on values of specified security attributes), for integrity. It allows the author of a PP, PP-Module, functional package or ST to specify actions to be taken upon detection of an integrity error.

EXAMPLE 1

This component can be used to provide different integrity error detection and action for information at different integrity levels.

The author of a PP, PP-Module, functional package or ST shall specify the types of errors that must be detected. The author of a PP, PP-Module, functional package or ST should consider: modification of data, substitution of data, unrecoverable ordering change of data, replay of data, incomplete data, in addition to other integrity errors.

The author of a PP, PP-Module, functional package or ST should specify the attributes (and associated transmission channels) that necessitate integrity error monitoring.

The author of a PP, PP-Module, functional package or ST specifies the actions that the TSF should take on detection of a failure.

EXAMPLE 2

Ignore the user data, request the data again, inform the authorized administrator, reroute traffic for other lines.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.10.5.2 Operations

In FDP_ITT.4.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) covering the information being transferred and monitored for integrity errors.

In FDP_ITT.4.1, the author of a PP, PP-Module, functional package or ST should specify the type of possible integrity errors to be monitored during transmission of the user data.

In FDP_ITT.4.1, the author of a PP, PP-Module, functional package or ST should specify a list of security attributes that require separate transmission channels. This list is used to determine which user data to monitor for integrity errors., based on its security attributes and its transmission channel. This element is directly related to FDP_ITT.2 Transmission separation by attribute.

In FDP_ITT.4.2, the author of a PP, PP-Module, functional package or ST should specify the action to be taken by the TSF when an integrity error is encountered. An example can be that the TSF should request the resubmission of the user data. The SFP(s) specified in FDP_ITT.4.1 will be enforced as the actions are taken by the TSF.

F.11 Residual information protection (FDP_RIP)

F.11.1 User application notes

Residual information protection ensures that TSF-controlled resources when de-allocated from an object and before they are reallocated to another object are treated by the TSF in a way that it is not possible to reconstruct all or part of the data contained in the resource before it was de-allocated.

A TOE usually has a number of functions that potentially de-allocate resources from an object and potentially re-allocate those resources to objects. Some, but not all of those resources may have been used to store critical data from the previous use of the resource and for those resources FDP_RIP requires that they are prepared for reuse. Object reuse applies to explicit requests of a subject or user to release resources as well as implicit actions of the TSF that result in the de-allocation and subsequent re-allocation of resources to different objects.

EXAMPLE

Examples of explicit requests are the deletion or truncation of a file or the release of an area of main memory. Examples of implicit actions of the TSF are the de-allocation and re-allocation of cache regions.

The requirement for object reuse is related to the content of the resource belonging to an object, not all information about the resource or object that may be stored elsewhere in the TSF. As an example, to satisfy the FDP_RIP requirement for files as objects requires that all sectors that make up the file need to be prepared for re-use.

It also applies to resources that are serially reused by different subjects within the system. For example, most operating systems typically rely upon hardware registers (resources) to support processes within the system. As processes are swapped from a “run” state to a “sleep” state (and vice versa), these registers are serially reused by different subjects. While this “swapping” action may not be considered an allocation or deallocation of a resource, Residual information protection (FDP_RIP) can apply to such events and resources.

Residual information protection (FDP_RIP) typically controls access to information that is not part of any currently defined or accessible object; however, in certain cases this may not be true. For example, object “A” is a file and object “B” is the disk upon which that file resides. If object “A” is deleted, the information from object “A” is under the control of Residual information protection (FDP_RIP) even though it is still part of object “B”.

It is important to note that Residual information protection (FDP_RIP) applies only to on-line objects and not off-line objects such as those backed-up on tapes. For example, if a file is deleted in the TOE, Residual information protection (FDP_RIP) can be instantiated to require that no residual information

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

exists upon deallocation; however, the TSF cannot extend this enforcement to that same file that exists on the off-line back-up. Therefore, that same file is still available. If this is a concern, then the author of a PP, PP-Module, functional package or ST should make sure that the proper environmental objectives are in place to support operational user guidance to address off-line objects.

Residual information protection (FDP_RIP) and Rollback (FDP_ROL) can conflict when Residual information protection (FDP_RIP) is instantiated to require that residual information be cleared at the time the application releases the object to the TSF (i.e. upon deallocation). Therefore, the Residual information protection (FDP_RIP) selection of "deallocation" should not be used with Rollback (FDP_ROL) since there would be no information to roll back. The other selection, "unavailability upon allocation", may be used with Rollback (FDP_ROL), but there is the risk that the resource which held the information has been allocated to a new object before the roll back took place. If that were to occur, then the roll back would not be possible.

There are no audit requirements in Residual information protection (FDP_RIP) because this is not a user-invokable function. Auditing of allocated or deallocated resources would be auditable as part of the access control SFP or the information flow control SFP operations.

This family should apply to the objects specified in the access control SFP(s) or the information flow control SFP(s) as specified by the author of a PP, PP-Module, functional package or ST.

F.11.2 FDP_RIP.1 Subset residual information protection

F.11.2.1 Component rationale and application notes

This component requires that, for a subset of the objects in the TOE, the TSF will ensure that there is no available residual information contained in a resource allocated to those objects or deallocated from those objects.

F.11.2.2 Operations

In FDP_RIP.1.1, the author of a PP, PP-Module, functional package or ST should specify the event, allocation of the resource to or deallocation of the resource from, that invokes the residual information protection function.

In FDP_RIP.1.1, the author of a PP, PP-Module, functional package or ST should specify the list of objects subject to residual information protection.

F.11.3 FDP_RIP.2 Full residual information protection

F.11.3.1 Component rationale and application notes

This component requires that for all objects in the TOE, the TSF will ensure that there is no available residual information contained in a resource allocated to those objects or deallocated from those objects.

F.11.3.2 Operations

In FDP_RIP.2.1, the author of a PP, PP-Module, functional package or ST should specify the event, allocation of the resource to or deallocation of the resource from, that invokes the residual information protection function.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.12 Rollback (FDP_ROL)

F.12.1 User application notes

This family addresses the need to return to a well-defined valid state, such as the need of a user to undo modifications to a file or to undo transactions in case of an incomplete series of transaction as in the case of databases.

This family is intended to assist a user in returning to a well-defined valid state after the user undoes the last set of actions, or, in distributed databases, the return of all of the distributed copies of the databases to the state before an operation failed.

Residual information protection (FDP_RIP) and Rollback (FDP_ROL) conflict when Residual information protection (FDP_RIP) enforces that the contents will be made unavailable at the time that a resource is deallocated from an object. Therefore, this use of Residual information protection (FDP_RIP) cannot be combined with Rollback (FDP_ROL) as there would be no information to roll back. Residual information protection (FDP_RIP) can be used only with Rollback (FDP_ROL) when it enforces that the contents will be unavailable at the time that a resource is allocated to an object. This is because the Rollback (FDP_ROL) mechanism will have an opportunity to access the previous information that may still be present in the TOE in order to successfully roll back the operation.

The rollback requirement is bounded by certain limits.

EXAMPLE 1

A text editor typically only allows you roll back up to a certain number of commands.

EXAMPLE 2

Backups. If backup tapes are rotated, after a tape is reused, the information can no longer be retrieved. This also poses a bound on the rollback requirement.

F.12.2 FDP_ROL.1 Basic rollback

F.12.2.1 Component rationale and application notes

This component allows a user or subject to undo a set of operations on a predefined set of objects. The undo is only possible within certain limits, for example up to a number of characters or up to a time limit.

F.12.2.2 Operations

In FDP_ROL.1.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) that will be enforced when performing rollback operations. This is necessary to make sure that roll back is not used to circumvent the specified SFPs.

In FDP_ROL.1.1, the author of a PP, PP-Module, functional package or ST should specify the list of operations that can be rolled back.

In FDP_ROL.1.1, the author of a PP, PP-Module, functional package or ST should specify the information and/or list of objects that are subjected to the rollback policy.

In FDP_ROL.1.2, the author of a PP, PP-Module, functional package or ST should specify the boundary limit to which rollback operations may be performed. The boundary may be specified as a predefined period of time,

EXAMPLE

Operations may be undone which were performed within the past two minutes. Other possible boundaries may be defined as the maximum number of operations allowable or the size of a buffer.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.12.3 FDP_ROL.2 Advanced rollback

F.12.3.1 Component rationale and application notes

This component enforces that the TSF provide the capability to rollback all operations; however, the user can choose to rollback only a part of them.

F.12.3.2 Operations

In FDP_ROL.2.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) that will be enforced when performing rollback operations. This is necessary to make sure that roll back is not used to circumvent the specified SFPs.

In FDP_ROL.2.1, the author of a PP, PP-Module, functional package or ST should specify the list of objects that are subjected to the rollback policy.

In FDP_ROL.2.2, the author of a PP, PP-Module, functional package or ST should specify the boundary limit to which rollback operations may be performed. The boundary may be specified as a predefined period of time,

EXAMPLE

Operations may be undone which were performed within the past two minutes.

Other possible boundaries may be defined as the maximum number of operations allowable or the size of a buffer.

F.13 Stored data confidentiality (FDP_SDC)

F.13.1 User application notes

This family provides requirements that address protection of user data confidentiality while the data is stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromise of their information bypassing these interfaces. It complements the family Stored data integrity (FDP_SDI) which protects the user data from integrity errors while being stored in the memory.

F.13.2 Evaluator notes

In practice, the dependency to FCS_COP.1 may be satisfied by a PP, PP-Module, functional package or ST author by providing a rationale explaining an alternative method to cryptography is used in some dedicated cases.

F.13.3 FDP_SDC.1 Stored data confidentiality

F.13.3.1 Component rationale and application notes

In FDP_SDC.1 Stored data confidentiality, the author of a PP, PP-Module, functional package or ST specifies which user data is to be protected and in which type of memory the user data is requested to be protected. In the second selection the author of a PP, PP-Module, functional package or ST provides the memory type where the user data is to be protected.

F.13.3.2 Operations

In FDP_SDC.1.1 the author of a PP, PP-Module, functional package or ST shall select either “all user data” or provide a list of user data using the assignment below. In the second selection, the author of a PP, PP-Module, functional package or ST can specify either temporary memory, persistent memory or any memory. “Any memory” includes both temporary (volatile) and persistent (non-volatile) memory.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

In FDP_SDC.1.1 the author of a PP, PP-Module, functional package or ST provides a list of the user data that is to be protected in memory.

F.13.4 FDP_SDC.2 Stored data confidentiality with dedicated method

F.13.4.1 Component rationale and application notes

FDP_SDC.2 Stored data confidentiality with dedicated method refines the FDP_SDC.1.1 element by allowing the author of a PP, PP-Module, functional package or ST to refine the list of user data using a variety of data characteristics.

F.13.4.2 Operations

The operations of selection and the first assignment are the same as that in FDP_SDC.1.

For the second assignment the author of a PP, PP-Module, functional package or ST provides the data characteristics. Data characteristics can include items such as data length (shorter or longer than a threshold), data type (binary, text, image, sound, video), and data representation (binary, vector, character, frame).

F.14 Stored data integrity (FDP_SDI)

F.14.1 User application notes

This family provides requirements that address protection of user data while it is stored within containers controlled by the TSF.

Hardware glitches or errors may affect data stored in memory. This family provides requirements to detect these unintentional errors. The integrity of user data while stored on storage devices controlled by the TSF are also addressed by this family.

To prevent a subject from modifying the data, the Information flow control functions (FDP_IFF) or Access control functions (FDP_ACF) families are required (rather than this family).

This family differs from Internal TOE transfer (FDP_ITT) that protects the user data from integrity errors while being transferred within the TOE.

F.14.2 FDP_SDI.1 Stored data integrity monitoring

F.14.2.1 Component rationale and application notes

This component monitors data stored on media for integrity errors. The author of a PP, PP-Module, functional package or ST can specify different kinds of user data attributes that will be used as the basis for monitoring.

F.14.2.2 Operations

In FDP_SDI.1.1, the author of a PP, PP-Module, functional package or ST should specify the integrity errors that the TSF will detect.

In FDP_SDI.1.1, the author of a PP, PP-Module, functional package or ST should specify the user data attributes that will be used as the basis for the monitoring.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.14.3 FDP_SDI.2 Stored data integrity monitoring and action

F.14.3.1 Component rationale and application notes

This component monitors data stored on media for integrity errors. The author of a PP, PP-Module, functional package or ST can specify which action should be taken in case an integrity error is detected.

F.14.3.2 Operations

In FDP_SDI.2.1, the author of a PP, PP-Module, functional package or ST should specify the integrity errors that the TSF will detect.

In FDP_SDI.2.1, the author of a PP, PP-Module, functional package or ST should specify the user data attributes that will be used as the basis for the monitoring.

In FDP_SDI.2.2, the author of a PP, PP-Module, functional package or ST should specify the actions to be taken in case an integrity error is detected.

F.15 Inter-TSF user data confidentiality transfer protection (FDP_UCT)

F.15.1 User application notes

This family defines the requirements for ensuring the confidentiality of user data when it is transferred using an external channel between the TOE and another trusted IT product. Confidentiality is enforced by preventing unauthorized disclosure of user data in transit between the two end points. The end points may be a TSF or a user.

This family provides a requirement for the protection of user data during transit. In contrast, Confidentiality of exported TSF data (FPT_ITC) handles TSF data.

F.15.2 FDP_UCT.1 Basic data exchange confidentiality

F.15.2.1 Component rationale and application notes

Depending on the access control or information flow policies the TSF is required to send or receive user data in a manner such that the confidentiality of the user data is protected.

F.15.2.2 Operations

In FDP_UCT.1.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) that will be enforced when exchanging user data. The specified policies will be enforced to make decisions about who can exchange data and which data can be exchanged.

In FDP_UCT.1.1, the author of a PP, PP-Module, functional package or ST should specify whether this element applies to a mechanism that transmits or receives user data.

F.16 Inter-TSF user data integrity transfer protection (FDP_UIT)

F.16.1 User application notes

This family defines the requirements for providing integrity for user data in transit between the TSF and another trusted IT product and recovering from detectable errors. At a minimum, this family monitors the integrity of user data for modifications. Furthermore, this family supports different ways of correcting detected integrity errors.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

This family defines the requirements for providing integrity for user data in transit; while Integrity of exported TSF data (FPT_ITI) handles TSF data.

Inter-TSF user data integrity transfer protection (FDP_UIT) and Inter-TSF user data confidentiality transfer protection (FDP_UCT) are duals of each other, as Inter-TSF user data confidentiality transfer protection (FDP_UCT) addresses user data confidentiality. Therefore, the same mechanism that implements Inter-TSF user data integrity transfer protection (FDP_UIT) can possibly be used to implement other families such as Inter-TSF user data confidentiality transfer protection (FDP_UCT) and Import from outside of the TOE (FDP_ITC).

F.16.2 FDP_UIT.1 Data exchange integrity

F.16.2.1 Component rationale and application notes

Depending on the access control or information flow policies the TSF is required to send or receive user data in a manner such that modification of the user data is detected. There is no requirement for a TSF mechanism to attempt to recover from the modification.

F.16.2.2 Operations

In FDP_UIT.1.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) that will be enforced on the transmitted data or on the received data. The specified policies will be enforced to make decisions about who can transmit or who can receive data, and which data can be transmitted or received.

In FDP_UIT.1.1, the author of a PP, PP-Module, functional package or ST should specify whether this element applies to a TSF that is transmitting or receiving objects.

In FDP_UIT.1.1, the author of a PP, PP-Module, functional package or ST should specify whether the data should be protected from modification, deletion, insertion, or replay.

In FDP_UIT.1.2, the author of a PP, PP-Module, functional package or ST should specify whether the errors of the type: modification, deletion, insertion, or replay are detected.

F.16.3 FDP_UIT.2 Source data exchange recovery

F.16.3.1 Component rationale and application notes

This component provides the ability to recover from a set of identified transmission errors, if required, with the help of the other trusted IT product. As the other trusted IT product is outside the TOE, the TSF cannot control its behaviour. However, it can provide functions that have the ability to cooperate with the other trusted IT product for the purposes of recovery.

EXAMPLE

The TSF can include functions that depend upon the source trusted IT product to re-send the data in the event that an error is detected.

This component deals with the ability of the TSF to handle such an error recovery.

F.16.3.2 Operations

In FDP_UIT.2.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) that will be enforced when recovering user data. The specified policies will be enforced to make decisions about which data can be recovered and how it can be recovered.

In FDP_UIT.2.1, the author of a PP, PP-Module, functional package or ST should specify the list of integrity errors from which the TSF, with the help of the source trusted IT product, is be able to recover the original user data.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

F.16.4 FDP_UIT.3 Destination data exchange recovery

F.16.4.1 Component rationale and application notes

This component provides the ability to recover from a set of identified transmission errors. It accomplishes this task without help from the source trusted IT product.

EXAMPLE

If certain errors are detected, the transmission protocol must be robust enough to allow the TSF to recover from the error based on checksums and other information available within that protocol.

F.16.4.2 Operations

In FDP_UIT.3.1, the author of a PP, PP-Module, functional package or ST should specify the access control SFP(s) and/or information flow control SFP(s) that will be enforced when recovering user data. The specified policies will be enforced to make decisions about which data can be recovered and how it can be recovered.

In FDP_UIT.3.1, the author of a PP, PP-Module, functional package or ST should specify the list of integrity errors from which the receiving TSF, alone, is able to recover the original user data.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Annex G
(normative)

Class FIA: Identification and authentication — Application notes

G.1 General

A common security requirement is to unambiguously identify the person and/or entity performing functions in a TOE. This involves not only establishing the claimed identity of each user, but also verifying that each user is indeed who he/she claims to be. This is achieved by requiring users to provide the TSF with some information that is known by the TSF to be associated with the user in question.

Families in this class address the requirements for functions to establish and verify a claimed user identity. Identification and Authentication is required to ensure that users are associated with the proper security attributes.

EXAMPLE Security attributes include identity, groups, roles, security, or integrity levels.

The unambiguous identification of authorized users and the correct association of security attributes with users and subjects is critical to the enforcement of the security policies.

The Authentication failures (FIA_AFL) family addresses defining limits on repeated unsuccessful authentication attempts.

The Authentication proof of identity (FIA_API) family addresses defining the functionality provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

The User attribute definition (FIA_ATD) family addresses the definition of user attributes that are used in the enforcement of the SFRs.

The Specification of secrets (FIA_SOS) family addresses the generation and verification of secrets that satisfy a defined metric.

The User authentication (FIA_UAU) family addresses verifying the identity of a user.

The User identification (FIA_UID) family addresses determining the identity of a user.

The User-subject binding (FIA_USB) family addresses the correct association of security attributes for each authorized user.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

G.2 Authentication failures (FIA_AFL)

G.2.1 User application notes

This family addresses requirements for defining values for authentication attempts and TSF actions in cases of authentication attempt failure. Parameters include, but are not limited to, the number of attempts and time thresholds.

The session establishment process is the interaction with the user to perform the session establishment independent of the actual implementation. If the number of unsuccessful authentication attempts exceeds the indicated threshold, either the user account or the terminal (or both) will be locked. If the user account is disabled, the user cannot log-on to the system. If the terminal is disabled, the terminal (or the address that the terminal has) cannot be used for any log-on. Both of these situations continues until the condition for re-establishment is satisfied.

© ISO/IEC 2022 – All rights reserved

G.2.2 FIA_AFL.1 Authentication failure handling

G.2.2.1 Component rationale and application notes

The author of a PP, PP-Module, functional package or ST may define the number of unsuccessful authentication attempts or may choose to let the TOE developer or the authorized user to define this number. The unsuccessful authentication attempts need not be consecutive, but rather related to an authentication event. Such an authentication event can be the count from the last successful session establishment at a given terminal.

The author of a PP, PP-Module, functional package or ST can specify a list of actions that the TSF shall take in the case of authentication failure. An authorized administrator can also be allowed to manage the events, if deemed opportune by the author of a PP, PP-Module, functional package or ST. These actions can be, among other things, terminal deactivation, user account deactivation or administrator alarm. The conditions under which the situation will be restored to normal be specified on the action.

In order to prevent denial of service, TOEs usually ensure that there is at least one user account that cannot be disabled.

Further actions for the TSF can be stated by the author of a PP, PP-Module, functional package or ST, including rules for re-enabling the user session establishment process, or sending an alarm to the administrator.

EXAMPLE

Examples of these actions are:

— until a specified time has lapsed;

— until the authorized administrator re-enables the terminal/account;

— a time related to failed previous attempts (every time the attempt fails, the disabling time is doubled).

G.2.2.2 Operations

In FIA_AFL.1 Authentication failure handling, the author of a PP, PP-Module, functional package or ST should select either the assignment of a positive integer, or the phrase “an administrator configurable positive integer” specifying the range of acceptable values.

In FIA_AFL.1 Authentication failure handling, the author of a PP, PP-Module, functional package or ST should specify the authentication events.

EXAMPLE

Examples of these authentication events are:

— the unsuccessful authentication attempts since the last successful authentication for the indicated user identity;

— the unsuccessful authentication attempts since the last successful authentication for the current terminal;

— the number of unsuccessful authentication attempts in the last 10 min;

— at least one authentication event shall be specified.

In FIA_AFL.1 Authentication failure handling, if the assignment of a positive integer is selected, the author of a PP, PP-Module, functional package or ST should specify the default number (positive integer) of unsuccessful authentication attempts that, when met or surpassed, will trigger the events.

In FIA_AFL.1 Authentication failure handling, if an administrator configurable positive integer is selected, the author of a PP, PP-Module, functional package or ST should specify the range of acceptable values from which the administrator of the TOE may configure the number of unsuccessful

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

authentication attempts. The number of authentication attempts should be less than or equal to the upper bound and greater or equal to the lower bound values.

In FIA_AFL.1.2, the author of a PP, PP-Module, functional package or ST should select whether the event of meeting or surpassing the defined number of unsuccessful authentication attempts shall trigger an action by the TSF.

In FIA_AFL.1.2, the author of a PP, PP-Module, functional package or ST should specify the actions to be taken in case the threshold is met or surpassed, as selected. These actions can be disabling of an account for 5 minutes, disabling the terminal for an increasing amount of time (2 to the power of the number of unsuccessful attempts in seconds), or disabling of the account until unlocked by the administrator and simultaneously informing the administrator. The actions should specify the measures and if applicable the duration of the measure (or the conditions under which the measure will be ended).

G.3 Authentication proof of identity (FIA_API)

G.3.1 User application notes

The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The family FIA_API allows the specification the functionality allowing a TOE to prove its own identity.

G.3.2 FIA_API.1 Authentication proof of identity

G.3.2.1 Component rationale and application notes

FIA_API.1 Authentication proof of identity allows the specification of the authentication mechanism used to support proving the identity of the TOE to external entities.

G.3.2.2 Operations

The first assignment is where a PP, PP-Module, functional package or ST author specifies the authentication mechanism to be used.

EXAMPLE

Examples of such an authentication method is "an Authentication Mechanism based on Triple-DES" and "Chip Authentication Protocol according to TR-03110".

The second assignment allows the author of a PP, PP-Module, functional package or ST to specify to what entity the proof of identity is associated with.

The third assignment is used to provide a list of properties. The property list may include roles or credentials.

G.4 User attribute definition (FIA_ATD)

G.4.1 User application notes

All authorized users may have a set of security attributes, other than the user's identity, that are used to enforce the SFRs. This family defines the requirements for associating user security attributes with users as needed to support the TSF in making security decisions.

There are dependencies on the individual security policy (SFP) definitions. These individual definitions should contain the listing of attributes that are necessary for policy enforcement.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

G.4.2 FIA_ATD.1 User attribute definition

G.4.2.1 Component rationale and application notes

This component specifies the security attributes that should be maintained at the level of the user. This means that the security attributes listed are assigned to and can be changed at the level of the user. In other words, changing a security attribute in this list associated with a user should have no impact on the security attributes of any other user.

In case security attributes belong to a group of users (such as a capability list for a group), the user will need to have a reference (as a security attribute) to the relevant group.

G.4.2.2 Operations

In FIA_ATD.1.1, the author of a PP, PP-Module, functional package or ST should specify the security attributes that are associated to an individual user.

EXAMPLE An example of such a list is {“clearance”, “group identifier”, “rights”}.

G.5 Specification of secrets (FIA_SOS)

G.5.1 User application notes

This family defines requirements for mechanisms that enforce defined quality metrics on provided secrets and generate secrets to satisfy the defined metric.

EXAMPLE 1

Examples of such mechanisms may include automated checking of user supplied passwords, or automated password generation.

A secret can be generated outside the TOE.

EXAMPLE 2

An example of a secret generated outside of the TOE can be one that is selected by the user and introduced in the TOE.

In such cases, the FIA_SOS.1 Verification of secrets component can be used to ensure that the external generated secret adheres to certain standards, for example a minimum size, not present in a dictionary, and/or not previously used.

Secrets can also be generated by the TOE. In those cases, the FIA_SOS.2 TSF Generation of secrets component can be used to require the TOE to ensure that the secrets that will adhere to some specified metrics.

Secrets contain the authentication data provided by the user for an authentication mechanism that is based on knowledge the user possesses. When cryptographic keys are employed, the class FCS: Cryptographic support should be used instead of this family.

G.5.2 FIA_SOS.1 Verification of secrets

G.5.2.1 Component rationale and application notes

Secrets can be generated by the user. This component ensures that those user generated secrets can be verified to meet a certain quality metric.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

G.5.2.2 Operations

In FIA_SOS.1.1, the author of a PP, PP-Module, functional package or ST provides a defined quality metric. The quality metric specification may be as simple as a description of the quality checks to be performed, or as formal as a reference to a government published standard that defines the quality metrics that secrets must meet.

EXAMPLE

Quality metrics can include a description of the alphanumeric structure of acceptable secrets and/or the space size that acceptable secrets must meet.

G.5.3 FIA_SOS.2 TSF Generation of secrets

G.5.3.1 Component rationale and application notes

This component allows the TSF to generate secrets for specific functions such as authentication by means of passwords.

When a pseudo-random number generator is used in a secret generation algorithm, it should accept as input random data that would provide output that has a high degree of unpredictability. This random data (seed) can be derived from a number of available parameters such as a system clock, system registers, date, time, etc. The parameters should be selected to ensure that the number of unique seeds that can be generated from these inputs should be at least equal to the minimum number of secrets that must be generated.

G.5.3.2 Operations

In FIA_SOS.2.1, the author of a PP, PP-Module, functional package or ST provides a defined quality metric. The quality metric specification can be as simple as a description of the quality checks to be performed or as formal as a reference to a government published standard that defines the quality metrics that secrets must meet.

EXAMPLE 1

Quality metrics can include a description of the alphanumeric structure of acceptable secrets and/or the space size that acceptable secrets must meet.

In FIA_SOS.2.2, the author of a PP, PP-Module, functional package or ST provides a list of TSF functions for which the TSF generated secrets shall be used.

EXAMPLE 2 An example of such a function can include a password-based authentication mechanism.

G.6 User authentication (FIA_UAU)

G.6.1 User application notes

This family defines the types of user authentication mechanisms supported by the TSF. This family defines the required attributes on which the user authentication mechanisms are based.

G.6.2 FIA_UAU.1 Timing of authentication

G.6.2.1 Component rationale and application notes

This component requires that the author of a PP, PP-Module, functional package or ST define the TSF-mediated actions that can be performed by the TSF on behalf of the user before the claimed identity of the user is authenticated. The TSF-mediated actions should have no security concerns with users incorrectly identifying themselves prior to being authenticated. For all other TSF-mediated actions not

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

in the list, the user shall be authenticated before the action can be performed by the TSF on behalf of the user.

This component cannot control whether the actions can also be performed before the identification took place. This requires the use of either FIA_UID.1 Timing of identification or FIA_UID.2 User identification before any action with the appropriate assignments.

G.6.2.2 Operations

In FIA_UAU.1.1, the author of a PP, PP-Module, functional package or ST specifies a list of TSF-mediated actions that can be performed by the TSF on behalf of a user before the claimed identity of the user is authenticated. This list cannot be empty. If no actions are appropriate, component FIA_UAU.2 User authentication before any action should be used instead.

EXAMPLE Such an action can include the request for help on the login procedure.

G.6.3 FIA_UAU.2 User authentication before any action

G.6.3.1 Component rationale and application notes

This component requires that a user is authenticated before any other TSF-mediated action can take place on behalf of that user.

G.6.3.2 Operations

No operations have been specified for this component.

G.6.4 FIA_UAU.3 Unforgeable authentication

G.6.4.1 Component rationale and application notes

This component addresses requirements for mechanisms that provide protection of authentication data. Authentication data that is copied from another user or is in some way constructed should be detected and/or rejected. These mechanisms provide confidence that users authenticated by the TSF are actually who they claim to be.

This component may be useful only with authentication mechanisms that are based on authentication data that cannot be shared. It is impossible for a TSF to detect or prevent the sharing of passwords outside the control of the TSF.

G.6.4.2 Operations

In FIA_UAU.3.1, the author of a PP, PP-Module, functional package or ST should specify whether the TSF will detect, prevent, or detect and prevent forging of authentication data.

In FIA_UAU.3.2, the author of a PP, PP-Module, functional package or ST should specify whether the TSF will detect, prevent, or detect and prevent copying of authentication data.

G.6.5 FIA_UAU.4 Single-use authentication mechanisms

G.6.5.1 Component rationale and application notes

This component addresses requirements for authentication mechanisms based on single-use authentication data. Single-use authentication data can be something the user has or knows, but not something the user is.

EXAMPLE

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

Single-use authentication data include single-use passwords, encrypted time-stamps, and/or random numbers from a secret lookup table.

The author of a PP, PP-Module, functional package or ST can specify to which authentication mechanism(s) this requirement applies.

G.6.5.2 Operations

In FIA_UAU.4.1, the author of a PP, PP-Module, functional package or ST should specify the list of authentication mechanisms to which this requirement applies. This assignment can be "all authentication mechanisms".

EXAMPLE

An example of this assignment can be "the authentication mechanism employed to authenticate people on the external network".

G.6.6 FIA_UAU.5 Multiple authentication mechanisms

G.6.6.1 Component rationale and application notes

The use of this component allows specification of requirements for more than one authentication mechanism to be used within a TOE. For each distinct mechanism, applicable requirements are chosen from the FIA: Identification and authentication class to be applied to each mechanism. It is possible that the same component is selected multiple times in order to reflect different requirements for the different use of the authentication mechanism.

The management functions in the class FMT provide maintenance capabilities for the set of authentication mechanisms, as well as the rules that determine whether the authentication was successful.

To allow anonymous users to interact with the TOE, a "none" authentication mechanism may be incorporated. The use of such access needs to be clearly explained in the rules of FIA_UAU.5.2.

G.6.6.2 Operations

In FIA_UAU.5.1, the author of a PP, PP-Module, functional package or ST defines the available authentication mechanisms.

EXAMPLE 1

Such a list can be, "none, password mechanism, biometric (retinal scan), S/key mechanism".

In FIA_UAU.5.2, the author of a PP, PP-Module, functional package or ST specifies the rules that describe how the authentication mechanisms provide authentication and when each is to be used. This means that for each situation the set of mechanisms used for authenticating the user shall be described.

EXAMPLE 2

A list of such rules is, "if the user has special privileges a password mechanism and a biometric mechanism both shall be used, with success only if both succeed; for all other users a password mechanism shall be used."

The author of a PP, PP-Module, functional package or ST may give the boundaries within which the authorized administrator may specify specific rules.

EXAMPLE 3

An example of a rule is, "the user shall always be authenticated by means of a token; the administrator can specify additional authentication mechanisms that also must be used."

The author of a PP, PP-Module, functional package or ST also may choose not to specify any boundaries but leave the authentication mechanisms and their rules completely up to the authorized administrator.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved

G.6.7 FIA_UAU.6 Re-authenticating

G.6.7.1 Component rationale and application notes

This component addresses potential needs to re-authenticate users at defined points in time. These may include user requests for the TSF to perform security relevant actions, as well as requests from non-TSF entities for re-authentication.

EXAMPLE A server application requesting that the TSF re-authenticate the client it is serving.

G.6.7.2 Operations

In FIA_UAU.6.1, the author of a PP, PP-Module, functional package or ST specifies the list of conditions requiring re-authentication. This list may include a specified user inactivity period that has elapsed, the user requesting a change in active security attributes, or the user requesting the TSF to perform some security critical function.

The author of a PP, PP-Module, functional package or ST may give the boundaries within which the re-authentication occurs and leave the specifics to the authorized administrator.

EXAMPLE

"The user shall always be re-authenticated at least once a day; the administrator may specify that the re-authentication happens more often but not more often than once every 10 min."

G.6.8 FIA_UAU.7 Protected authentication feedback

G.6.8.1 Component rationale and application notes

This component addresses the feedback on the authentication process that will be provided to the user. In some systems, the feedback consists of indicating how many characters have been typed but not showing the characters themselves, in other systems even this information can not be appropriate.

This component requires that the authentication data is not provided as-is back to the user. In a workstation environment, it can display a substitute character for each password character provided, and not the original character.

EXAMPLE A star "*" character.

G.6.8.2 Operations

In FIA_UAU.7 Protected authentication feedback, the author of a PP, PP-Module, functional package or ST should specify the feedback related to the authentication process that will be provided to the user.

EXAMPLE

A feedback assignment can be "the number of characters typed", another type of feedback is "the authentication mechanism that failed the authentication".

G.7 User identification (FIA_UID)

G.7.1 User application notes

This family defines the conditions under which users are required to identify themselves before performing any other actions that are to be mediated by the TSF and that require user identification.

IECNORM.COM : Click to view the full PDF of ISO/IEC 15408-2:2022

© ISO/IEC 2022 – All rights reserved