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

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

Contents

Page

European foreword 17

Foreword 18

Introduction 20

1 Scope 21

2 Normative references 21

3 Terms and definitions, symbols and abbreviated terms 21

4 Overview 21
4.1 Organisation of this part of ISO/IEC 15408 21

5 Functional requirements paradigm 22

6 Security functional components 25
6.1 Overview 25
6.1.1 Class structure 25
6.1.2 Family structure 26
6.1.3 Component structure 28
6.2 Component catalogue 29
6.2.1 Component changes highlighting 30

7 Class FAU: Security audit 30
7.1 Security audit automatic response (FAU_ARP) 31
7.1.1 Family Behaviour 31
7.1.2 Component levelling 31
7.1.3 Management of FAU_ARP.1 31
7.1.4 Audit of FAU_ARP.1 31
7.1.5 FAU_ARP.1 Security alarms 31
7.2 Security audit data generation (FAU_GEN) 31
7.2.1 Family Behaviour 31
7.2.2 Component levelling 31
7.2.3 Management of FAU_GEN.1, FAU_GEN.2 31
7.2.4 Audit of FAU_GEN.1, FAU_GEN.2 31
7.2.5 FAU_GEN.1 Audit data generation 32
7.2.6 FAU_GEN.2 User identity association 32
7.3 Security audit analysis (FAU_SAA) 32
7.3.1 Family Behaviour 32
7.3.2 Component levelling 32
7.3.3 Management of FAU_SAA.1 33
7.3.4 Management of FAU_SAA.2 33
7.3.5 Management of FAU_SAA.3 33
7.3.6 Management of FAU_SAA.4 33
7.3.7 Audit of FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4 33
7.3.8 FAU_SAA.1 Potential violation analysis 33
7.3.9 FAU_SAA.2 Profile based anomaly detection 34
7.3.10 FAU_SAA.3 Simple attack heuristics 34
7.3.11 FAU_SAA.4 Complex attack heuristics 35
7.4 Security audit review (FAU_SAR) 35
7.4.1 Family Behaviour 35
7.4.2 Component levelling 35
7.4.3 Management of FAU_SAR.1 35
7.4.4 Management of FAU_SAR.2, FAU_SAR.3 35
7.4.5 Audit of FAU_SAR.1 35
7.4.6 Audit of FAU_SAR.2 36
7.4.7 Audit of FAU_SAR.3 36

7.4.8 FAU_SAR.1 Audit review 36
7.4.9 FAU_SAR.2 Restricted audit review 36
7.4.10 FAU_SAR.3 Selectable audit review 36
7.5 Security audit event selection (FAU_SEL) 36
7.5.1 Family Behaviour 36
7.5.2 Component levelling 37
7.5.3 Management of FAU_SEL.1 37
7.5.4 Audit of FAU_SEL.1 37
7.5.5 FAU_SEL.1 Selective audit 37
7.6 Security audit event storage (FAU_STG) 37
7.6.1 Family Behaviour 37
7.6.2 Component levelling 37
7.6.3 Management of FAU_STG.1 38
7.6.4 Management of FAU_STG.2 38
7.6.5 Management of FAU_STG.3 38
7.6.6 Management of FAU_STG.4 38
7.6.7 Audit of FAU_STG.1, FAU_STG.2 38
7.6.8 Audit of FAU_STG.3 38
7.6.9 Audit of FAU_STG.4 38
7.6.10 FAU_STG.1 Protected audit trail storage 38
7.6.11 FAU_STG.2 Guarantees of audit data availability 39
7.6.12 FAU_STG.3 Action in case of possible audit data loss 39
7.6.13 FAU_STG.4 Prevention of audit data loss 39

8 Class FCO: Communication 40
8.1 Non-repudiation of origin (FCO_NRO) 40
8.1.1 Family Behaviour 40
8.1.2 Component levelling 40
8.1.3 Management of FCO_NRO.1, FCO_NRO.2 40
8.1.4 Audit of FCO_NRO.1 40
8.1.5 Audit of FCO_NRO.2 41
8.1.6 FCO_NRO.1 Selective proof of origin 41
8.1.7 FCO_NRO.2 Enforced proof of origin 41
8.2 Non-repudiation of receipt (FCO_NRR) 42
8.2.1 Family Behaviour 42
8.2.2 Component levelling 42
8.2.3 Management of FCO_NRR.1, FCO_NRR.2 42
8.2.4 Audit of FCO_NRR.1 42
8.2.5 Audit of FCO_NRR.2 42
8.2.6 FCO_NRR.1 Selective proof of receipt 42
8.2.7 FCO_NRR.2 Enforced proof of receipt 43

9 Class FCS: Cryptographic support 44
9.1 Cryptographic key management (FCS_CKM) 44
9.1.1 Family Behaviour 44
9.1.2 Component levelling 44
9.1.3 Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 45
9.1.4 Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 45
9.1.5 FCS_CKM.1 Cryptographic key generation 45
9.1.6 FCS_CKM.2 Cryptographic key distribution 45
9.1.7 FCS_CKM.3 Cryptographic key access 45
9.1.8 FCS_CKM.4 Cryptographic key destruction 46
9.2 Cryptographic operation (FCS_COP) 46
9.2.1 Family Behaviour 46
9.2.2 Component levelling 46
9.2.3 Management of FCS_COP.1 46
9.2.4 Audit of FCS_COP.1 46
9.2.5 FCS_COP.1 Cryptographic operation 47

10 Class FDP: User data protection 47
10.1 Access control policy (FDP_ACC) 49

10.1.1 Family Behaviour 49
10.1.2 Component levelling 50
10.1.3 Management of FDP_ACC.1, FDP_ACC.2 50
10.1.4 Audit of FDP_ACC.1, FDP_ACC.2 50
10.1.5 FDP_ACC.1 Subset access control 50
10.1.6 FDP_ACC.2 Complete access control 50
10.2 Access control functions (FDP_ACF) 50
10.2.1 Family Behaviour 50
10.2.2 Component levelling 50
10.2.3 Management of FDP_ACF.1 51
10.2.4 Audit of FDP_ACF.1 51
10.2.5 FDP_ACF.1 Security attribute based access control 51
10.3 Data authentication (FDP_DAU) 52
10.3.1 Family Behaviour 52
10.3.2 Component levelling 52
10.3.3 Management of FDP_DAU.1, FDP_DAU.2 52
10.3.4 Audit of FDP_DAU.1 52
10.3.5 Audit of FDP_DAU.2 52
10.3.6 FDP_DAU.1 Basic Data Authentication 52
10.3.7 FDP_DAU.2 Data Authentication with Identity of Guarantor 53
10.4 Export from the TOE (FDP_ETC) 53
10.4.1 Family Behaviour 53
10.4.2 Component levelling 53
10.4.3 Management of FDP_ETC.1 53
10.4.4 Management of FDP_ETC.2 53
10.4.5 Audit of FDP_ETC.1, FDP_ETC.2 53
10.4.6 FDP_ETC.1 Export of user data without security attributes 54
10.4.7 FDP_ETC.2 Export of user data with security attributes 54
10.5 Information flow control policy (FDP_IFC) 54
10.5.1 Family Behaviour 54
10.5.2 Component levelling 55
10.5.3 Management of FDP_IFC.1, FDP_IFC.2 55
10.5.4 Audit of FDP_IFC.1, FDP_IFC.2 55
10.5.5 FDP_IFC.1 Subset information flow control 55
10.5.6 FDP_IFC.2 Complete information flow control 55
10.6 Information flow control functions (FDP_IFF) 55
10.6.1 Family Behaviour 55
10.6.2 Component levelling 56
10.6.3 Management of FDP_IFF.1, FDP_IFF.2 56
10.6.4 Management of FDP_IFF.3, FDP_IFF.4, FDP_IFF.5 56
10.6.5 Management of FDP_IFF.6 56
10.6.6 Audit of FDP_IFF.1, FDP_IFF.2, FDP_IFF.5 56
10.6.7 Audit of FDP_IFF.3, FDP_IFF.4, FDP_IFF.6 57
10.6.8 FDP_IFF.1 Simple security attributes 57
10.6.9 FDP_IFF.2 Hierarchical security attributes 57
10.6.10 FDP_IFF.3 Limited illicit information flows 58
10.6.11 FDP_IFF.4 Partial elimination of illicit information flows 59
10.6.12 FDP_IFF.5 No illicit information flows 59
10.6.13 FDP_IFF.6 Illicit information flow monitoring 59
10.7 Import from outside of the TOE (FDP_ITC) 59
10.7.1 Family Behaviour 59
10.7.2 Component levelling 59
10.7.3 Management of FDP_ITC.1, FDP_ITC.2 60
10.7.4 Audit of FDP_ITC.1, FDP_ITC.2 60
10.7.5 FDP_ITC.1 Import of user data without security attributes 60
10.7.6 FDP_ITC.2 Import of user data with security attributes 60
10.8 Internal TOE transfer (FDP_ITT) 61
10.8.1 Family Behaviour 61
10.8.2 Component levelling 61
10.8.3 Management of FDP_ITT.1, FDP_ITT.2 61

10.8.4 Management of FDP_ITT.3, FDP_ITT.4 62
10.8.5 Audit of FDP_ITT.1, FDP_ITT.2 62
10.8.6 Audit of FDP_ITT.3, FDP_ITT.4 62
10.8.7 FDP_ITT.1 Basic internal transfer protection 62
10.8.8 FDP_ITT.2 Transmission separation by attribute 62
10.8.9 FDP_ITT.3 Integrity monitoring 63
10.8.10 FDP_ITT.4 Attribute-based integrity monitoring 63
10.9 Residual information protection (FDP_RIP) 63
10.9.1 Family Behaviour 63
10.9.2 Component levelling 64
10.9.3 Management of FDP_RIP.1, FDP_RIP.2 64
10.9.4 Audit of FDP_RIP.1, FDP_RIP.2 64
10.9.5 FDP_RIP.1 Subset residual information protection 64
10.9.6 FDP_RIP.2 Full residual information protection 64
10.10 Rollback (FDP_ROL) 64
10.10.1 Family Behaviour 64
10.10.2 Component levelling 64
10.10.3 Management of FDP_ROL.1, FDP_ROL.2 65
10.10.4 Audit of FDP_ROL.1, FDP_ROL.2 65
10.10.5 FDP_ROL.1 Basic rollback 65
10.10.6 FDP_ROL.2 Advanced rollback 65
10.11 Stored data integrity (FDP_SDI) 66
10.11.1 Family Behaviour 66
10.11.2 Component levelling 66
10.11.3 Management of FDP_SDI.1 66
10.11.4 Management of FDP_SDI.2 66
10.11.5 Audit of FDP_SDI.1 66
10.11.6 Audit of FDP_SDI.2 66
10.11.7 FDP_SDI.1 Stored data integrity monitoring 66
10.11.8 FDP_SDI.2 Stored data integrity monitoring and action 67
10.12 Inter-TSF user data confidentiality transfer protection (FDP_UCT) 67
10.12.1 Family Behaviour 67
10.12.2 Component levelling 67
10.12.3 Management of FDP_UCT.1 67
10.12.4 Audit of FDP_UCT.1 67
10.12.5 FDP_UCT.1 Basic data exchange confidentiality 67
10.13 Inter-TSF user data integrity transfer protection (FDP_UIT) 68
10.13.1 Family Behaviour 68
10.13.2 Component levelling 68
10.13.3 Management of FDP_UIT.1, FDP_UIT.2, FDP_UIT.3 68
10.13.4 Audit of FDP_UIT.1 68
10.13.5 Audit of FDP_UIT.2, FDP_UIT.3 68
10.13.6 FDP_UIT.1 Data exchange integrity 69
10.13.7 FDP_UIT.2 Source data exchange recovery 69
10.13.8 FDP_UIT.3 Destination data exchange recovery 69

11 Class FIA: Identification and authentication 70
11.1 Authentication failures (FIA_AFL) 71
11.1.1 Family Behaviour 71
11.1.2 Component levelling 71
11.1.3 Management of FIA_AFL.1 72
11.1.4 Audit of FIA_AFL.1 72
11.1.5 FIA_AFL.1 Authentication failure handling 72
11.2 User attribute definition (FIA_ATD) 72
11.2.1 Family Behaviour 72
11.2.2 Component levelling 72
11.2.3 Management of FIA_ATD.1 72
11.2.4 Audit of FIA_ATD.1 72
11.2.5 FIA_ATD.1 User attribute definition 73
11.3 Specification of secrets (FIA_SOS) 73

11.3.1 Family Behaviour 73
11.3.2 Component levelling 73
11.3.3 Management of FIA_SOS.1 73
11.3.4 Management of FIA_SOS.2 73
11.3.5 Audit of FIA_SOS.1, FIA_SOS.2 73
11.3.6 FIA_SOS.1 Verification of secrets 73
11.3.7 FIA_SOS.2 TSF Generation of secrets 74
11.4 User authentication (FIA_UAU) 74
11.4.1 Family Behaviour 74
11.4.2 Component levelling 74
11.4.3 Management of FIA_UAU.1 74
11.4.4 Management of FIA_UAU.2 75
11.4.5 Management of FIA_UAU.3, FIA_UAU.4, FIA_UAU.7 75
11.4.6 Management of FIA_UAU.5 75
11.4.7 Management of FIA_UAU.6 75
11.4.8 Audit of FIA_UAU.1 75
11.4.9 Audit of FIA_UAU.2 75
11.4.10 Audit of FIA_UAU.3 75
11.4.11 Audit of FIA_UAU.4 76
11.4.12 Audit of FIA_UAU.5 76
11.4.13 Audit of FIA_UAU.6 76
11.4.14 Audit of FIA_UAU.7 76
11.4.15 FIA_UAU.1 Timing of authentication 76
11.4.16 FIA_UAU.2 User authentication before any action 76
11.4.17 FIA_UAU.3 Unforgeable authentication 77
11.4.18 FIA_UAU.4 Single-use authentication mechanisms 77
11.4.19 FIA_UAU.5 Multiple authentication mechanisms 77
11.4.20 FIA_UAU.6 Re-authenticating 77
11.4.21 FIA_UAU.7 Protected authentication feedback 77
11.5 User identification (FIA_UID) 78
11.5.1 Family Behaviour 78
11.5.2 Component levelling 78
11.5.3 Management of FIA_UID.1 78
11.5.4 Management of FIA_UID.2 78
11.5.5 Audit of FIA_UID.1, FIA_UID.2 78
11.5.6 FIA_UID.1 Timing of identification 78
11.5.7 FIA_UID.2 User identification before any action 79
11.6 User-subject binding (FIA_USB) 79
11.6.1 Family Behaviour 79
11.6.2 Component levelling 79
11.6.3 Management of FIA_USB.1 79
11.6.4 Audit of FIA_USB.1 79
11.6.5 FIA_USB.1 User-subject binding 79

12 Class FMT: Security management 80
12.1 Management of functions in TSF (FMT_MOF) 81
12.1.1 Family Behaviour 81
12.1.2 Component levelling 81
12.1.3 Management of FMT_MOF.1 81
12.1.4 Audit of FMT_MOF.1 82
12.1.5 FMT_MOF.1 Management of security functions behaviour 82
12.2 Management of security attributes (FMT_MSA) 82
12.2.1 Family Behaviour 82
12.2.2 Component levelling 82
12.2.3 Management of FMT_MSA.1 82
12.2.4 Management of FMT_MSA.2 82
12.2.5 Management of FMT_MSA.3 83
12.2.6 Management of FMT_MSA.4 83
12.2.7 Audit of FMT_MSA.1 83
12.2.8 Audit of FMT_MSA.2 83

12.2.9 Audit of FMT_MSA.3 83
12.2.10 Audit of FMT_MSA.4 83
12.2.11 FMT_MSA.1 Management of security attributes 83
12.2.12 FMT_MSA.2 Secure security attributes 84
12.2.13 FMT_MSA.3 Static attribute initialisation 84
12.2.14 FMT_MSA.4 Security attribute value inheritance 84
12.3 Management of TSF data (FMT_MTD) 85
12.3.1 Family Behaviour 85
12.3.2 Component levelling 85
12.3.3 Management of FMT_MTD.1 85
12.3.4 Management of FMT_MTD.2 85
12.3.5 Management of FMT_MTD.3 85
12.3.6 Audit of FMT_MTD.1 85
12.3.7 Audit of FMT_MTD.2 85
12.3.8 Audit of FMT_MTD.3 85
12.3.9 FMT_MTD.1 Management of TSF data 85
12.3.10 FMT_MTD.2 Management of limits on TSF data 86
12.3.11 FMT_MTD.3 Secure TSF data 86
12.4 Revocation (FMT_REV) 86
12.4.1 Family Behaviour 86
12.4.2 Component levelling 86
12.4.3 Management of FMT_REV.1 86
12.4.4 Audit of FMT_REV.1 87
12.4.5 FMT_REV.1 Revocation 87
12.5 Security attribute expiration (FMT_SAE) 87
12.5.1 Family Behaviour 87
12.5.2 Component levelling 87
12.5.3 Management of FMT_SAE.1 87
12.5.4 Audit of FMT_SAE.1 87
12.5.5 FMT_SAE.1 Time-limited authorisation 87
12.6 Specification of Management Functions (FMT_SMF) 88
12.6.1 Family Behaviour 88
12.6.2 Component levelling 88
12.6.3 Management of FMT_SMF.1 88
12.6.4 Audit of FMT_SMF.1 88
12.6.5 FMT_SMF.1 Specification of Management Functions 88
12.7 Security management roles (FMT_SMR) 88
12.7.1 Family Behaviour 88
12.7.2 Component levelling 89
12.7.3 Management of FMT_SMR.1 89
12.7.4 Management of FMT_SMR.2 89
12.7.5 Management of FMT_SMR.3 89
12.7.6 Audit of FMT_SMR.1 89
12.7.7 Audit of FMT_SMR.2 89
12.7.8 Audit of FMT_SMR.3 89
12.7.9 FMT_SMR.1 Security roles 89
12.7.10 FMT_SMR.2 Restrictions on security roles 90
12.7.11 FMT_SMR.3 Assuming roles 90

13 Class FPR: Privacy 91
13.1 Anonymity (FPR_ANO) 91
13.1.1 Family Behaviour 91
13.1.2 Component levelling 91
13.1.3 Management of FPR_ANO.1, FPR_ANO.2 91
13.1.4 Audit of FPR_ANO.1, FPR_ANO.2 91
13.1.5 FPR_ANO.1 Anonymity 92
13.1.6 FPR_ANO.2 Anonymity without soliciting information 92
13.2 Pseudonymity (FPR_PSE) 92
13.2.1 Family Behaviour 92
13.2.2 Component levelling 92

13.2.3 Management of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 92
13.2.4 Audit of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3 92
13.2.5 FPR_PSE.1 Pseudonymity 93
13.2.6 FPR_PSE.2 Reversible pseudonymity 93
13.2.7 FPR_PSE.3 Alias pseudonymity 93
13.3 Unlinkability (FPR_UNL) 94
13.3.1 Family Behaviour 94
13.3.2 Component levelling 94
13.3.3 Management of FPR_UNL.1 94
13.3.4 Audit of FPR_UNL.1 94
13.3.5 FPR_UNL.1 Unlinkability 94
13.4 Unobservability (FPR_UNO) 94
13.4.1 Family Behaviour 94
13.4.2 Component levelling 95
13.4.3 Management of FPR_UNO.1, FPR_UNO.2 95
13.4.4 Management of FPR_UNO.3 95
13.4.5 Management of FPR_UNO.4 95
13.4.6 Audit of FPR_UNO.1, FPR_UNO.2 95
13.4.7 Audit of FPR_UNO.3 95
13.4.8 Audit of FPR_UNO.4 95
13.4.9 FPR_UNO.1 Unobservability 95
13.4.10 FPR_UNO.2 Allocation of information impacting unobservability 96
13.4.11 FPR_UNO.3 Unobservability without soliciting information 96
13.4.12 FPR_UNO.4 Authorised user observability 96

14 Class FPT: Protection of the TSF 96
14.1 Fail secure (FPT_FLS) 97
14.1.1 Family Behaviour 97
14.1.2 Component levelling 98
14.1.3 Management of FPT_FLS.1 98
14.1.4 Audit of FPT_FLS.1 98
14.1.5 FPT_FLS.1 Failure with preservation of secure state 98
14.2 Availability of exported TSF data (FPT_ITA) 98
14.2.1 Family Behaviour 98
14.2.2 Component levelling 98
14.2.3 Management of FPT_ITA.1 98
14.2.4 Audit of FPT_ITA.1 98
14.2.5 FPT_ITA.1 Inter-TSF availability within a defined availability metric 98
14.3 Confidentiality of exported TSF data (FPT_ITC) 99
14.3.1 Family Behaviour 99
14.3.2 Component levelling 99
14.3.3 Management of FPT_ITC.1 99
14.3.4 Audit of FPT_ITC.1 99
14.3.5 FPT_ITC.1 Inter-TSF confidentiality during transmission 99
14.4 Integrity of exported TSF data (FPT_ITI) 99
14.4.1 Family Behaviour 99
14.4.2 Component levelling 99
14.4.3 Management of FPT_ITI.1 100
14.4.4 Management of FPT_ITI.2 100
14.4.5 Audit of FPT_ITI.1 100
14.4.6 Audit of FPT_ITI.2 100
14.4.7 FPT_ITI.1 Inter-TSF detection of modification 100
14.4.8 FPT_ITI.2 Inter-TSF detection and correction of modification 100
14.5 Internal TOE TSF data transfer (FPT_ITT) 101
14.5.1 Family Behaviour 101
14.5.2 Component levelling 101
14.5.3 Management of FPT_ITT.1 101
14.5.4 Management of FPT_ITT.2 101
14.5.5 Management of FPT_ITT.3 101
14.5.6 Audit of FPT_ITT.1, FPT_ITT.2 102

14.5.7 Audit of FPT_ITT.3 102
14.5.8 FPT_ITT.1 Basic internal TSF data transfer protection 102
14.5.9 FPT_ITT.2 TSF data transfer separation 102
14.5.10 FPT_ITT.3 TSF data integrity monitoring 102
14.6 TSF physical protection (FPT_PHP) 103
14.6.1 Family Behaviour 103
14.6.2 Component levelling 103
14.6.3 Management of FPT_PHP.1 103
14.6.4 Management of FPT_PHP.2 103
14.6.5 Management of FPT_PHP.3 103
14.6.6 Audit of FPT_PHP.1 103
14.6.7 Audit of FPT_PHP.2 104
14.6.8 Audit of FPT_PHP.3 104
14.6.9 FPT_PHP.1 Passive detection of physical attack 104
14.6.10 FPT_PHP.2 Notification of physical attack 104
14.6.11 FPT_PHP.3 Resistance to physical attack 104
14.7 Trusted recovery (FPT_RCV) 105
14.7.1 Family Behaviour 105
14.7.2 Component levelling 105
14.7.3 Management of FPT_RCV.1 105
14.7.4 Management of FPT_RCV.2, FPT_RCV.3 105
14.7.5 Management of FPT_RCV.4 105
14.7.6 Audit of FPT_RCV.1, FPT_RCV.2, FPT_RCV.3 105
14.7.7 Audit of FPT_RCV.4 105
14.7.8 FPT_RCV.1 Manual recovery 106
14.7.9 FPT_RCV.2 Automated recovery 106
14.7.10 FPT_RCV.3 Automated recovery without undue loss 106
14.7.11 FPT_RCV.4 Function recovery 107
14.8 Replay detection (FPT_RPL) 107
14.8.1 Family Behaviour 107
14.8.2 Component levelling 107
14.8.3 Management of FPT_RPL.1 107
14.8.4 Audit of FPT_RPL.1 107
14.8.5 FPT_RPL.1 Replay detection 107
14.9 State synchrony protocol (FPT_SSP) 108
14.9.1 Family Behaviour 108
14.9.2 Component levelling 108
14.9.3 Management of FPT_SSP.1, FPT_SSP.2 108
14.9.4 Audit of FPT_SSP.1, FPT_SSP.2 108
14.9.5 FPT_SSP.1 Simple trusted acknowledgement 108
14.9.6 FPT_SSP.2 Mutual trusted acknowledgement 108
14.10 Time stamps (FPT_STM) 109
14.10.1 Family Behaviour 109
14.10.2 Component levelling 109
14.10.3 Management of FPT_STM.1 109
14.10.4 Audit of FPT_STM.1 109
14.10.5 FPT_STM.1 Reliable time stamps 109
14.11 Inter-TSF TSF data consistency (FPT_TDC) 109
14.11.1 Family Behaviour 109
14.11.2 Component levelling 109
14.11.3 Management of FPT_TDC.1 109
14.11.4 Audit of FPT_TDC.1 109
14.11.5 FPT_TDC.1 Inter-TSF basic TSF data consistency 110
14.12 Testing of external entities (FPT_TEE) 110
14.12.1 Family Behaviour 110
14.12.2 Component levelling 110
14.12.3 Management of FPT_TEE.1 110
14.12.4 Audit of FPT_TEE.1 110
14.12.5 FPT_TEE.1 Testing of external entities 110
14.13 Internal TOE TSF data replication consistency (FPT_TRC) 111

14.13.1 Family Behaviour 111
14.13.2 Component levelling 111
14.13.3 Management of FPT_TRC.1 111
14.13.4 Audit of FPT_TRC.1 111
14.13.5 FPT_TRC.1 Internal TSF consistency 111
14.14 TSF self test (FPT_TST) 112
14.14.1 Family Behaviour 112
14.14.2 Component levelling 112
14.14.3 Management of FPT_TST.1 112
14.14.4 Audit of FPT_TST.1 112
14.14.5 FPT_TST.1 TSF testing 112

15 Class FRU: Resource utilisation 113
15.1 Fault tolerance (FRU_FLT) 113
15.1.1 Family Behaviour 113
15.1.2 Component levelling 113
15.1.3 Management of FRU_FLT.1, FRU_FLT.2 113
15.1.4 Audit of FRU_FLT.1 113
15.1.5 Audit of FRU_FLT.2 113
15.1.6 FRU_FLT.1 Degraded fault tolerance 114
15.1.7 FRU_FLT.2 Limited fault tolerance 114
15.2 Priority of service (FRU_PRS) 114
15.2.1 Family Behaviour 114
15.2.2 Component levelling 114
15.2.3 Management of FRU_PRS.1, FRU_PRS.2 114
15.2.4 Audit of FRU_PRS.1, FRU_PRS.2 114
15.2.5 FRU_PRS.1 Limited priority of service 114
15.2.6 FRU_PRS.2 Full priority of service 115
15.3 Resource allocation (FRU_RSA) 115
15.3.1 Family Behaviour 115
15.3.2 Component levelling 115
15.3.3 Management of FRU_RSA.1 115
15.3.4 Management of FRU_RSA.2 115
15.3.5 Audit of FRU_RSA.1, FRU_RSA.2 116
15.3.6 FRU_RSA.1 Maximum quotas 116
15.3.7 FRU_RSA.2 Minimum and maximum quotas 116

16 Class FTA: TOE access 117
16.1 Limitation on scope of selectable attributes (FTA_LSA) 117
16.1.1 Family Behaviour 117
16.1.2 Component levelling 117
16.1.3 Management of FTA_LSA.1 117
16.1.4 Audit of FTA_LSA.1 117
16.1.5 FTA_LSA.1 Limitation on scope of selectable attributes 118
16.2 Limitation on multiple concurrent sessions (FTA_MCS) 118
16.2.1 Family Behaviour 118
16.2.2 Component levelling 118
16.2.3 Management of FTA_MCS.1 118
16.2.4 Management of FTA_MCS.2 118
16.2.5 Audit of FTA_MCS.1, FTA_MCS.2 118
16.2.6 FTA_MCS.1 Basic limitation on multiple concurrent sessions 118
16.2.7 FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions 119
16.3 Session locking and termination (FTA_SSL) 119
16.3.1 Family Behaviour 119
16.3.2 Component levelling 119
16.3.3 Management of FTA_SSL.1 119
16.3.4 Management of FTA_SSL.2 119
16.3.5 Management of FTA_SSL.3 119
16.3.6 Management of FTA_SSL.4 120
16.3.7 Audit of FTA_SSL.1, FTA_SSL.2 120
16.3.8 Audit of FTA_SSL.3 120

16.3.9 Audit of FTA_SSL.4 120
16.3.10 FTA_SSL.1 TSF-initiated session locking 120
16.3.11 FTA_SSL.2 User-initiated locking 120
16.3.12 FTA_SSL.3 TSF-initiated termination 121
16.3.13 FTA_SSL.4 User-initiated termination 121
16.4 TOE access banners (FTA_TAB) 121
16.4.1 Family Behaviour 121
16.4.2 Component levelling 121
16.4.3 Management of FTA_TAB.1 121
16.4.4 Audit of FTA_TAB.1 121
16.4.5 FTA_TAB.1 Default TOE access banners 121
16.5 TOE access history (FTA_TAH) 122
16.5.1 Family Behaviour 122
16.5.2 Component levelling 122
16.5.3 Management of FTA_TAH.1 122
16.5.4 Audit of FTA_TAH.1 122
16.5.5 FTA_TAH.1 TOE access history 122
16.6 TOE session establishment (FTA_TSE) 122
16.6.1 Family Behaviour 122
16.6.2 Component levelling 122
16.6.3 Management of FTA_TSE.1 123
16.6.4 Audit of FTA_TSE.1 123
16.6.5 FTA_TSE.1 TOE session establishment 123

17 Class FTP: Trusted path/channels 123
17.1 Inter-TSF trusted channel (FTP_ITC) 124
17.1.1 Family Behaviour 124
17.1.2 Component levelling 124
17.1.3 Management of FTP_ITC.1 124
17.1.4 Audit of FTP_ITC.1 124
17.1.5 FTP_ITC.1 Inter-TSF trusted channel 124
17.2 Trusted path (FTP_TRP) 125
17.2.1 Family Behaviour 125
17.2.2 Component levelling 125
17.2.3 Management of FTP_TRP.1 125
17.2.4 Audit of FTP_TRP.1 125
17.2.5 FTP_TRP.1 Trusted path 125

Annex A (normative) Security functional requirements application notes 127
A.1 Structure of the notes 127
A.1.1 Class structure 127
A.1.2 Family structure 128
A.1.3 Component structure 129
A.2 Dependency tables 129

Annex B (normative) Functional classes, families, and components 135

Annex C (normative) Class FAU: Security audit 136
C.1 Audit requirements in a distributed environment 136
C.2 Security audit automatic response (FAU_ARP) 137
C.2.1 User notes 137
C.2.2 FAU_ARP.1 Security alarms 137
C.3 Security audit data generation (FAU_GEN) 138
C.3.1 User notes 138
C.3.2 FAU_GEN.1 Audit data generation 139
C.3.3 FAU_GEN.2 User identity association 140
C.4 Security audit analysis (FAU_SAA) 140
C.4.1 User notes 140
C.4.2 FAU_SAA.1 Potential violation analysis 140
C.4.3 FAU_SAA.2 Profile based anomaly detection 141
C.4.4 FAU_SAA.3 Simple attack heuristics 142
C.4.5 FAU_SAA.4 Complex attack heuristics 142

C.5 Security audit review (FAU_SAR) **143**
C.5.1 User notes **143**
C.5.2 FAU_SAR.1 Audit review **144**
C.5.3 FAU_SAR.2 Restricted audit review **144**
C.5.4 FAU_SAR.3 Selectable audit review **144**
C.6 Security audit event selection (FAU_SEL) **145**
C.6.1 User notes **145**
C.6.2 FAU_SEL.1 Selective audit **145**
C.7 Security audit event storage (FAU_STG) **145**
C.7.1 User notes **145**
C.7.2 FAU_STG.1 Protected audit trail storage **146**
C.7.3 FAU_STG.2 Guarantees of audit data availability **146**
C.7.4 FAU_STG.3 Action in case of possible audit data loss **146**
C.7.5 FAU_STG.4 Prevention of audit data loss **147**

Annex D (normative) **Class FCO: Communication** **148**
D.1 Non-repudiation of origin (FCO_NRO) **148**
D.1.1 User notes **148**
D.1.2 FCO_NRO.1 Selective proof of origin **149**
D.1.3 FCO_NRO.2 Enforced proof of origin **149**
D.2 Non-repudiation of receipt (FCO_NRR) **150**
D.2.1 User notes **150**
D.2.2 FCO_NRR.1 Selective proof of receipt **150**
D.2.3 FCO_NRR.2 Enforced proof of receipt **151**

Annex E (normative) **Class FCS: Cryptographic support** **152**
E.1 Cryptographic key management (FCS_CKM) **153**
E.1.1 User notes **153**
E.1.2 FCS_CKM.1 Cryptographic key generation **154**
E.1.3 FCS_CKM.2 Cryptographic key distribution **154**
E.1.4 FCS_CKM.3 Cryptographic key access **154**
E.1.5 FCS_CKM.4 Cryptographic key destruction **155**
E.2 Cryptographic operation (FCS_COP) **155**
E.2.1 User notes **155**
E.2.2 FCS_COP.1 Cryptographic operation **156**

Annex F (normative) **Class FDP: User data protection** **157**
F.1 Access control policy (FDP_ACC) **160**
F.1.1 User notes **160**
F.1.2 FDP_ACC.1 Subset access control **160**
F.1.3 FDP_ACC.2 Complete access control **161**
F.2 Access control functions (FDP_ACF) **161**
F.2.1 User notes **161**
F.2.2 FDP_ACF.1 Security attribute based access control **161**
F.3 Data authentication (FDP_DAU) **163**
F.3.1 User notes **163**
F.3.2 FDP_DAU.1 Basic Data Authentication **163**
F.3.3 FDP_DAU.2 Data Authentication with Identity of Guarantor **163**
F.4 Export from the TOE (FDP_ETC) **163**
F.4.1 User notes **163**
F.4.2 FDP_ETC.1 Export of user data without security attributes **164**
F.4.3 FDP_ETC.2 Export of user data with security attributes **164**
F.5 Information flow control policy (FDP_IFC) **165**
F.5.1 User notes **165**
F.5.2 FDP_IFC.1 Subset information flow control **166**
F.5.3 FDP_IFC.2 Complete information flow control **166**
F.6 Information flow control functions (FDP_IFF) **166**
F.6.1 User notes **166**
F.6.2 FDP_IFF.1 Simple security attributes **167**
F.6.3 FDP_IFF.2 Hierarchical security attributes **168**
F.6.4 FDP_IFF.3 Limited illicit information flows **169**

F.6.5 FDP_IFF.4 Partial elimination of illicit information flows 169
F.6.6 FDP_IFF.5 No illicit information flows 170
F.6.7 FDP_IFF.6 Illicit information flow monitoring 170
F.7 Import from outside of the TOE (FDP_ITC) 171
F.7.1 User notes 171
F.7.2 FDP_ITC.1 Import of user data without security attributes 172
F.7.3 FDP_ITC.2 Import of user data with security attributes 172
F.8 Internal TOE transfer (FDP_ITT) 172
F.8.1 User notes 172
F.8.2 FDP_ITT.1 Basic internal transfer protection 173
F.8.3 FDP_ITT.2 Transmission separation by attribute 173
F.8.4 FDP_ITT.3 Integrity monitoring 173
F.8.5 FDP_ITT.4 Attribute-based integrity monitoring 174
F.9 Residual information protection (FDP_RIP) 175
F.9.1 User notes 175
F.9.2 FDP_RIP.1 Subset residual information protection 176
F.9.3 FDP_RIP.2 Full residual information protection 176
F.10 Rollback (FDP_ROL) 176
F.10.1 User notes 176
F.10.2 FDP_ROL.1 Basic rollback 177
F.10.3 FDP_ROL.2 Advanced rollback 177
F.11 Stored data integrity (FDP_SDI) 178
F.11.1 User notes 178
F.11.2 FDP_SDI.1 Stored data integrity monitoring 178
F.11.3 FDP_SDI.2 Stored data integrity monitoring and action 178
F.12 Inter-TSF user data confidentiality transfer protection (FDP_UCT) 178
F.12.1 User notes 178
F.12.2 FDP_UCT.1 Basic data exchange confidentiality 179
F.13 Inter-TSF user data integrity transfer protection (FDP_UIT) 179
F.13.1 User notes 179
F.13.2 FDP_UIT.1 Data exchange integrity 179
F.13.3 FDP_UIT.2 Source data exchange recovery 180
F.13.4 FDP_UIT.3 Destination data exchange recovery 180

Annex G (normative) **Class FIA: Identification and authentication** 181
G.1 Authentication failures (FIA_AFL) 182
G.1.1 User notes 182
G.1.2 FIA_AFL.1 Authentication failure handling 183
G.2 User attribute definition (FIA_ATD) 184
G.2.1 User notes 184
G.2.2 FIA_ATD.1 User attribute definition 184
G.3 Specification of secrets (FIA_SOS) 184
G.3.1 User notes 184
G.3.2 FIA_SOS.1 Verification of secrets 185
G.3.3 FIA_SOS.2 TSF Generation of secrets 185
G.4 User authentication (FIA_UAU) 185
G.4.1 User notes 185
G.4.2 FIA_UAU.1 Timing of authentication 185
G.4.3 FIA_UAU.2 User authentication before any action 186
G.4.4 FIA_UAU.3 Unforgeable authentication 186
G.4.5 FIA_UAU.4 Single-use authentication mechanisms 186
G.4.6 FIA_UAU.5 Multiple authentication mechanisms 187
G.4.7 FIA_UAU.6 Re-authenticating 187
G.4.8 FIA_UAU.7 Protected authentication feedback 188
G.5 User identification (FIA_UID) 188
G.5.1 User notes 188
G.5.2 FIA_UID.1 Timing of identification 188
G.5.3 FIA_UID.2 User identification before any action 188
G.6 User-subject binding (FIA_USB) 189
G.6.1 User notes 189

G.6.2 FIA_USB.1 User-subject binding 189

Annex H (normative) **Class FMT: Security management 190**
H.1 Management of functions in TSF (FMT_MOF) 191
H.1.1 User notes 191
H.1.2 FMT_MOF.1 Management of security functions behaviour 192
H.2 Management of security attributes (FMT_MSA) 192
H.2.1 User notes 192
H.2.2 FMT_MSA.1 Management of security attributes 193
H.2.3 FMT_MSA.2 Secure security attributes 193
H.2.4 FMT_MSA.3 Static attribute initialisation 194
H.2.5 FMT_MSA.4 Security attribute value inheritance 194
H.3 Management of TSF data (FMT_MTD) 194
H.3.1 User notes 194
H.3.2 FMT_MTD.1 Management of TSF data 194
H.3.3 FMT_MTD.2 Management of limits on TSF data 195
H.3.4 FMT_MTD.3 Secure TSF data 195
H.4 Revocation (FMT_REV) 196
H.4.1 User notes 196
H.4.2 FMT_REV.1 Revocation 196
H.5 Security attribute expiration (FMT_SAE) 196
H.5.1 User notes 196
H.5.2 FMT_SAE.1 Time-limited authorisation 197
H.6 Specification of Management Functions (FMT_SMF) 197
H.6.1 User notes 197
H.6.2 FMT_SMF.1 Specification of Management Functions 197
H.7 Security management roles (FMT_SMR) 197
H.7.1 User notes 197
H.7.2 FMT_SMR.1 Security roles 198
H.7.3 FMT_SMR.2 Restrictions on security roles 198
H.7.4 FMT_SMR.3 Assuming roles 198

Annex I (normative) **Class FPR: Privacy 199**
I.1 Anonymity (FPR_ANO) 200
I.1.1 User notes 200
I.1.2 FPR_ANO.1 Anonymity 201
I.1.3 FPR_ANO.2 Anonymity without soliciting information 201
I.2 Pseudonymity (FPR_PSE) 202
I.2.1 User notes 202
I.2.2 FPR_PSE.1 Pseudonymity 203
I.2.3 FPR_PSE.2 Reversible pseudonymity 203
I.2.4 FPR_PSE.3 Alias pseudonymity 204
I.3 Unlinkability (FPR_UNL) 205
I.3.1 User notes 205
I.3.2 FPR_UNL.1 Unlinkability 206
I.4 Unobservability (FPR_UNO) 206
I.4.1 User notes 206
I.4.2 FPR_UNO.1 Unobservability 207
I.4.3 FPR_UNO.2 Allocation of information impacting unobservability 207
I.4.4 FPR_UNO.3 Unobservability without soliciting information 208
I.4.5 FPR_UNO.4 Authorised user observability 209

Annex J (normative) **Class FPT: Protection of the TSF 210**
J.1 Fail secure (FPT_FLS) 212
J.1.1 User notes 212
J.1.2 FPT_FLS.1 Failure with preservation of secure state 212
J.2 Availability of exported TSF data (FPT_ITA) 212
J.2.1 User notes 212
J.2.2 FPT_ITA.1 Inter-TSF availability within a defined availability metric 212
J.3 Confidentiality of exported TSF data (FPT_ITC) 213
J.3.1 User notes 213

J.3.2 FPT_ITC.1 Inter-TSF confidentiality during transmission 213
J.4 Integrity of exported TSF data (FPT_ITI) 213
J.4.1 User notes 213
J.4.2 FPT_ITI.1 Inter-TSF detection of modification 213
J.4.3 FPT_ITI.2 Inter-TSF detection and correction of modification 214
J.5 Internal TOE TSF data transfer (FPT_ITT) 214
J.5.1 User notes 214
J.5.2 Evaluator notes 214
J.5.3 FPT_ITT.1 Basic internal TSF data transfer protection 215
J.5.4 FPT_ITT.2 TSF data transfer separation 215
J.5.5 FPT_ITT.3 TSF data integrity monitoring 215
J.6 TSF physical protection (FPT_PHP) 215
J.6.1 User notes 215
J.6.2 FPT_PHP.1 Passive detection of physical attack 216
J.6.3 FPT_PHP.2 Notification of physical attack 216
J.6.4 FPT_PHP.3 Resistance to physical attack 216
J.7 Trusted recovery (FPT_RCV) 217
J.7.1 User notes 217
J.7.2 FPT_RCV.1 Manual recovery 218
J.7.3 FPT_RCV.2 Automated recovery 219
J.7.4 FPT_RCV.3 Automated recovery without undue loss 219
J.7.5 FPT_RCV.4 Function recovery 220
J.8 Replay detection (FPT_RPL) 220
J.8.1 User notes 220
J.8.2 FPT_RPL.1 Replay detection 220
J.9 State synchrony protocol (FPT_SSP) 221
J.9.1 User notes 221
J.9.2 FPT_SSP.1 Simple trusted acknowledgement 221
J.9.3 FPT_SSP.2 Mutual trusted acknowledgement 221
J.10 Time stamps (FPT_STM) 221
J.10.1 User notes 221
J.10.2 FPT_STM.1 Reliable time stamps 221
J.11 Inter-TSF TSF data consistency (FPT_TDC) 222
J.11.1 User notes 222
J.11.2 FPT_TDC.1 Inter-TSF basic TSF data consistency 222
J.12 Testing of external entities (FPT_TEE) 222
J.12.1 User notes 222
J.12.2 Evaluator notes 223
J.12.3 FPT_TEE.1 Testing of external entities 223
J.13 Internal TOE TSF data replication consistency (FPT_TRC) 224
J.13.1 User notes 224
J.13.2 FPT_TRC.1 Internal TSF consistency 224
J.14 TSF self test (FPT_TST) 224
J.14.1 User notes 224
J.14.2 FPT_TST.1 TSF testing 224

Annex K (normative) **Class FRU: Resource utilisation** 226
K.1 Fault tolerance (FRU_FLT) 226
K.1.1 User notes 226
K.1.2 FRU_FLT.1 Degraded fault tolerance 227
K.1.3 FRU_FLT.2 Limited fault tolerance 227
K.2 Priority of service (FRU_PRS) 227
K.2.1 User notes 227
K.2.2 FRU_PRS.1 Limited priority of service 228
K.2.3 FRU_PRS.2 Full priority of service 228
K.3 Resource allocation (FRU_RSA) 228
K.3.1 User notes 228
K.3.2 FRU_RSA.1 Maximum quotas 229
K.3.3 FRU_RSA.2 Minimum and maximum quotas 229

Annex L (normative) **Class FTA: TOE access** 231

L.1 Limitation on scope of selectable attributes (FTA_LSA) 231
L.1.1 User notes 231
L.1.2 FTA_LSA.1 Limitation on scope of selectable attributes 232
L.2 Limitation on multiple concurrent sessions (FTA_MCS) 232
L.2.1 User notes 232
L.2.2 FTA_MCS.1 Basic limitation on multiple concurrent sessions 232
L.2.3 FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions 232
L.3 Session locking and termination (FTA_SSL) 233
L.3.1 User notes 233
L.3.2 FTA_SSL.1 TSF-initiated session locking 233
L.3.3 FTA_SSL.2 User-initiated locking 234
L.3.4 FTA_SSL.3 TSF-initiated termination 234
L.3.5 FTA_SSL.4 User-initiated termination 234
L.4 TOE access banners (FTA_TAB) 234
L.4.1 User notes 234
L.4.2 FTA_TAB.1 Default TOE access banners 235
L.5 TOE access history (FTA_TAH) 235
L.5.1 User notes 235
L.5.2 FTA_TAH.1 TOE access history 235
L.6 TOE session establishment (FTA_TSE) 235
L.6.1 User notes 235
L.6.2 FTA_TSE.1 TOE session establishment 236

Annex M (normative) **Class FTP: Trusted path/channels 237**
M.1 Inter-TSF trusted channel (FTP_ITC) 237
M.1.1 User notes 237
M.1.2 FTP_ITC.1 Inter-TSF trusted channel 237
M.2 Trusted path (FTP_TRP) 238
M.2.1 User notes 238
M.2.2 FTP_TRP.1 Trusted path 238