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

**Part 2:
Security functional components**

*Technologies de l'information — Techniques de sécurité — Critères
d'évaluation pour la sécurité TI —*

Partie 2: Composants fonctionnels de sécurité

*ITeH STANDARD PREVIEW
(standards.iteh.ai)
Full standard available at <https://standards.iteh.ai/catalog/standards/sist/ah/2d166-1c55-4a55-b9b3-6aa75658af21/iec-15408-2-2008>*

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/ab53cd166-1c55-4a55-b9b3-6aa75658af21/iso-iec-15408-2-2008>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

1	Scope	1
2	Normative references	1
3	Terms and definitions, symbols and abbreviated terms	1
4	Overview	1
4.1	Organisation of this part of ISO/IEC 15408	1
5	Functional requirements paradigm	2
6	Security functional components	5
6.1	Overview	5
6.1.1	Class structure	5
6.1.2	Family structure	6
6.1.3	Component structure	7
6.2	Component catalogue	9
6.2.1	Component changes highlighting	10
7	Class FAU: Security audit	10
7.1	Security audit automatic response (FAU_ARP)	11
7.1.1	Family Behaviour	11
7.1.2	Component levelling	11
7.1.3	Management of FAU_ARP.1	11
7.1.4	Audit of FAU_ARP.1	11
7.1.5	FAU_ARP.1 Security alarms	11
7.2	Security audit data generation (FAU_GEN)	11
7.2.1	Family Behaviour	11
7.2.2	Component levelling	11
7.2.3	Management of FAU_GEN.1, FAU_GEN.2	11
7.2.4	Audit of FAU_GEN.1, FAU_GEN.2	11
7.2.5	FAU_GEN.1 Audit data generation	12
7.2.6	FAU_GEN.2 User identity association	12
7.3	Security audit analysis (FAU_SAA)	12
7.3.1	Family Behaviour	12
7.3.2	Component levelling	12
7.3.3	Management of FAU_SAA.1	13
7.3.4	Management of FAU_SAA.2	13
7.3.5	Management of FAU_SAA.3	13
7.3.6	Management of FAU_SAA.4	13
7.3.7	Audit of FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4	13
7.3.8	FAU_SAA.1 Potential violation analysis	13
7.3.9	FAU_SAA.2 Profile based anomaly detection	14
7.3.10	FAU_SAA.3 Simple attack heuristics	14
7.3.11	FAU_SAA.4 Complex attack heuristics	15
7.4	Security audit review (FAU_SAR)	15
7.4.1	Family Behaviour	15
7.4.2	Component levelling	15
7.4.3	Management of FAU_SAR.1	15
7.4.4	Management of FAU_SAR.2, FAU_SAR.3	15
7.4.5	Audit of FAU_SAR.1	15
7.4.6	Audit of FAU_SAR.2	16
7.4.7	Audit of FAU_SAR.3	16
7.4.8	FAU_SAR.1 Audit review	16
7.4.9	FAU_SAR.2 Restricted audit review	16
7.4.10	FAU_SAR.3 Selectable audit review	16
7.5	Security audit event selection (FAU_SEL)	17

7.5.1	Family Behaviour	17
7.5.2	Component levelling	17
7.5.3	Management of FAU_SEL.1	17
7.5.4	Audit of FAU_SEL.1	17
7.5.5	FAU_SEL.1 Selective audit	17
7.6	Security audit event storage (FAU_STG)	17
7.6.1	Family Behaviour	17
7.6.2	Component levelling	17
7.6.3	Management of FAU_STG.1	18
7.6.4	Management of FAU_STG.2	18
7.6.5	Management of FAU_STG.3	18
7.6.6	Management of FAU_STG.4	18
7.6.7	Audit of FAU_STG.1, FAU_STG.2	18
7.6.8	Audit of FAU_STG.3	18
7.6.9	Audit of FAU_STG.4	18
7.6.10	FAU_STG.1 Protected audit trail storage	18
7.6.11	FAU_STG.2 Guarantees of audit data availability	19
7.6.12	FAU_STG.3 Action in case of possible audit data loss	19
7.6.13	FAU_STG.4 Prevention of audit data loss	19
8	Class FCO: Communication	19
8.1	Non-repudiation of origin (FCO_NRO)	20
8.1.1	Family Behaviour	20
8.1.2	Component levelling	20
8.1.3	Management of FCO_NRO.1, FCO_NRO.2	20
8.1.4	Audit of FCO_NRO.1	20
8.1.5	Audit of FCO_NRO.2	20
8.1.6	FCO_NRO.1 Selective proof of origin	20
8.1.7	FCO_NRO.2 Enforced proof of origin	21
8.2	Non-repudiation of receipt (FCO_NRR)	21
8.2.1	Family Behaviour	21
8.2.2	Component levelling	21
8.2.3	Management of FCO_NRR.1, FCO_NRR.2	21
8.2.4	Audit of FCO_NRR.1	22
8.2.5	Audit of FCO_NRR.2	22
8.2.6	FCO_NRR.1 Selective proof of receipt	22
8.2.7	FCO_NRR.2 Enforced proof of receipt	22
9	Class FCS: Cryptographic support	23
9.1	Cryptographic key management (FCS_CKM)	23
9.1.1	Family Behaviour	23
9.1.2	Component levelling	23
9.1.3	Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4	24
9.1.4	Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4	24
9.1.5	FCS_CKM.1 Cryptographic key generation	24
9.1.6	FCS_CKM.2 Cryptographic key distribution	24
9.1.7	FCS_CKM.3 Cryptographic key access	25
9.1.8	FCS_CKM.4 Cryptographic key destruction	25
9.2	Cryptographic operation (FCS_COP)	25
9.2.1	Family Behaviour	25
9.2.2	Component levelling	25
9.2.3	Management of FCS_COP.1	25
9.2.4	Audit of FCS_COP.1	26
9.2.5	FCS_COP.1 Cryptographic operation	26
10	Class FDP: User data protection	26
10.1	Access control policy (FDP_ACC)	28
10.1.1	Family Behaviour	28
10.1.2	Component levelling	29
10.1.3	Management of FDP_ACC.1, FDP_ACC.2	29
10.1.4	Audit of FDP_ACC.1, FDP_ACC.2	29

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

10.8.8	FDP_ITT.2 Transmission separation by attribute	41
10.8.9	FDP_ITT.3 Integrity monitoring	42
10.8.10	FDP_ITT.4 Attribute-based integrity monitoring	42
10.9	Residual information protection (FDP_RIP)	42
10.9.1	Family Behaviour	42
10.9.2	Component levelling	42
10.9.3	Management of FDP_RIP.1, FDP_RIP.2	43
10.9.4	Audit of FDP_RIP.1, FDP_RIP.2	43
10.9.5	FDP_RIP.1 Subset residual information protection	43
10.9.6	FDP_RIP.2 Full residual information protection	43
10.10	Rollback (FDP_ROL)	43
10.10.1	Family Behaviour	43
10.10.2	Component levelling	43
10.10.3	Management of FDP_ROL.1, FDP_ROL.2	43
10.10.4	Audit of FDP_ROL.1, FDP_ROL.2	44
10.10.5	FDP_ROL.1 Basic rollback	44
10.10.6	FDP_ROL.2 Advanced rollback	44
10.11	Stored data integrity (FDP_SDI)	44
10.11.1	Family Behaviour	44
10.11.2	Component levelling	45
10.11.3	Management of FDP_SDI.1	45
10.11.4	Management of FDP_SDI.2	45
10.11.5	Audit of FDP_SDI.1	45
10.11.6	Audit of FDP_SDI.2	45
10.11.7	FDP_SDI.1 Stored data integrity monitoring	45
10.11.8	FDP_SDI.2 Stored data integrity monitoring and action	46
10.12	Inter-TSF user data confidentiality transfer protection (FDP_UCT)	46
10.12.1	Family Behaviour	46
10.12.2	Component levelling	46
10.12.3	Management of FDP_UCT.1	46
10.12.4	Audit of FDP_UCT.1	46
10.12.5	FDP_UCT.1 Basic data exchange confidentiality	46
10.13	Inter-TSF user data integrity transfer protection (FDP_UIT)	47
10.13.1	Family Behaviour	47
10.13.2	Component levelling	47
10.13.3	Management of FDP_UIT.1, FDP_UIT.2, FDP_UIT.3	47
10.13.4	Audit of FDP_UIT.1	47
10.13.5	Audit of FDP_UIT.2, FDP_UIT.3	47
10.13.6	FDP_UIT.1 Data exchange integrity	48
10.13.7	FDP_UIT.2 Source data exchange recovery	48
10.13.8	FDP_UIT.3 Destination data exchange recovery	48
11	Class FIA: Identification and authentication	49
11.1	Authentication failures (FIA_AFL)	50
11.1.1	Family Behaviour	50
11.1.2	Component levelling	50
11.1.3	Management of FIA_AFL.1	51
11.1.4	Audit of FIA_AFL.1	51
11.1.5	FIA_AFL.1 Authentication failure handling	51
11.2	User attribute definition (FIA_ATD)	51
11.2.1	Family Behaviour	51
11.2.2	Component levelling	51
11.2.3	Management of FIA_ATD.1	51
11.2.4	Audit of FIA_ATD.1	51
11.2.5	FIA_ATD.1 User attribute definition	52
11.3	Specification of secrets (FIA_SOS)	52
11.3.1	Family Behaviour	52
11.3.2	Component levelling	52
11.3.3	Management of FIA_SOS.1	52
11.3.4	Management of FIA_SOS.2	52

11.3.5	Audit of FIA_SOS.1, FIA_SOS.2	52
11.3.6	FIA_SOS.1 Verification of secrets	52
11.3.7	FIA_SOS.2 TSF Generation of secrets	53
11.4	User authentication (FIA_UAU)	53
11.4.1	Family Behaviour	53
11.4.2	Component levelling	53
11.4.3	Management of FIA_UAU.1	53
11.4.4	Management of FIA_UAU.2	53
11.4.5	Management of FIA_UAU.3, FIA_UAU.4, FIA_UAU.7	54
11.4.6	Management of FIA_UAU.5	54
11.4.7	Management of FIA_UAU.6	54
11.4.8	Audit of FIA_UAU.1	54
11.4.9	Audit of FIA_UAU.2	54
11.4.10	Audit of FIA_UAU.3	54
11.4.11	Audit of FIA_UAU.4	54
11.4.12	Audit of FIA_UAU.5	55
11.4.13	Audit of FIA_UAU.6	55
11.4.14	Audit of FIA_UAU.7	55
11.4.15	FIA_UAU.1 Timing of authentication	55
11.4.16	FIA_UAU.2 User authentication before any action	55
11.4.17	FIA_UAU.3 Unforgeable authentication	55
11.4.18	FIA_UAU.4 Single-use authentication mechanisms	56
11.4.19	FIA_UAU.5 Multiple authentication mechanisms	56
11.4.20	FIA_UAU.6 Re-authenticating	56
11.4.21	FIA_UAU.7 Protected authentication feedback	56
11.5	User identification (FIA_UID)	57
11.5.1	Family Behaviour	57
11.5.2	Component levelling	57
11.5.3	Management of FIA_UID.1	57
11.5.4	Management of FIA_UID.2	57
11.5.5	Audit of FIA_UID.1, FIA_UID.2	57
11.5.6	FIA_UID.1 Timing of identification	57
11.5.7	FIA_UID.2 User identification before any action	57
11.6	User-subject binding (FIA_USB)	58
11.6.1	Family Behaviour	58
11.6.2	Component levelling	58
11.6.3	Management of FIA_USB.1	58
11.6.4	Audit of FIA_USB.1	58
11.6.5	FIA_USB.1 User-subject binding	58
12	Class FMT: Security management	59
12.1	Management of functions in TSF (FMT_MOF)	60
12.1.1	Family Behaviour	60
12.1.2	Component levelling	60
12.1.3	Management of FMT_MOF.1	61
12.1.4	Audit of FMT_MOF.1	61
12.1.5	FMT_MOF.1 Management of security functions behaviour	61
12.2	Management of security attributes (FMT_MSA)	61
12.2.1	Family Behaviour	61
12.2.2	Component levelling	61
12.2.3	Management of FMT_MSA.1	61
12.2.4	Management of FMT_MSA.2	61
12.2.5	Management of FMT_MSA.3	62
12.2.6	Management of FMT_MSA.4	62
12.2.7	Audit of FMT_MSA.1	62
12.2.8	Audit of FMT_MSA.2	62
12.2.9	Audit of FMT_MSA.3	62
12.2.10	Audit of FMT_MSA.4	62
12.2.11	FMT_MSA.1 Management of security attributes	62
12.2.12	FMT_MSA.2 Secure security attributes	63

12.2.13	FMT_MSA.3 Static attribute initialisation	63
12.2.14	FMT_MSA.4 Security attribute value inheritance	63
12.3	Management of TSF data (FMT_MTD).....	64
12.3.1	Family Behaviour.....	64
12.3.2	Component levelling	64
12.3.3	Management of FMT_MTD.1	64
12.3.4	Management of FMT_MTD.2	64
12.3.5	Management of FMT_MTD.3	64
12.3.6	Audit of FMT_MTD.1	64
12.3.7	Audit of FMT_MTD.2	64
12.3.8	Audit of FMT_MTD.3	64
12.3.9	FMT_MTD.1 Management of TSF data.....	64
12.3.10	FMT_MTD.2 Management of limits on TSF data	65
12.3.11	FMT_MTD.3 Secure TSF data	65
12.4	Revocation (FMT_REV)	65
12.4.1	Family Behaviour.....	65
12.4.2	Component levelling	65
12.4.3	Management of FMT_REV.1.....	65
12.4.4	Audit of FMT_REV.1.....	66
12.4.5	FMT_REV.1 Revocation.....	66
12.5	Security attribute expiration (FMT_SAE).....	66
12.5.1	Family Behaviour	66
12.5.2	Component levelling	66
12.5.3	Management of FMT_SAE.1.....	66
12.5.4	Audit of FMT_SAE.1.....	66
12.5.5	FMT_SAE.1 Time-limited authorisation	66
12.6	Specification of Management Functions (FMT_SMF)	67
12.6.1	Family Behaviour.....	67
12.6.2	Component levelling	67
12.6.3	Management of FMT_SMF.1	67
12.6.4	Audit of FMT_SMF.1	67
12.6.5	FMT_SMF.1 Specification of Management Functions.....	67
12.7	Security management roles (FMT_SMR).....	67
12.7.1	Family Behaviour.....	67
12.7.2	Component levelling	68
12.7.3	Management of FMT_SMR.1	68
12.7.4	Management of FMT_SMR.2	68
12.7.5	Management of FMT_SMR.3	68
12.7.6	Audit of FMT_SMR.1	68
12.7.7	Audit of FMT_SMR.2.....	68
12.7.8	Audit of FMT_SMR.3.....	68
12.7.9	FMT_SMR.1 Security roles.....	68
12.7.10	FMT_SMR.2 Restrictions on security roles.....	69
12.7.11	FMT_SMR.3 Assuming roles	69
13	Class FPR: Privacy	69
13.1	Anonymity (FPR_ANO).....	70
13.1.1	Family Behaviour.....	70
13.1.2	Component levelling	70
13.1.3	Management of FPR_ANO.1, FPR_ANO.2.....	70
13.1.4	Audit of FPR_ANO.1, FPR_ANO.2.....	70
13.1.5	FPR_ANO.1 Anonymity	70
13.1.6	FPR_ANO.2 Anonymity without soliciting information	71
13.2	Pseudonymity (FPR_PSE)	71
13.2.1	Family Behaviour	71
13.2.2	Component levelling	71
13.2.3	Management of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3	71
13.2.4	Audit of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3	71
13.2.5	FPR_PSE.1 Pseudonymity	71
13.2.6	FPR_PSE.2 Reversible pseudonymity.....	72

13.2.7	FPR_PSE.3 Alias pseudonymity	72
13.3	Unlinkability (FPR_UNL)	73
13.3.1	Family Behaviour.....	73
13.3.2	Component levelling	73
13.3.3	Management of FPR_UNL.1	73
13.3.4	Audit of FPR_UNL.1	73
13.3.5	FPR_UNL.1 Unlinkability.....	73
13.4	Unobservability (FPR_UNO).....	73
13.4.1	Family Behaviour.....	73
13.4.2	Component levelling	73
13.4.3	Management of FPR_UNO.1, FPR_UNO.2.....	74
13.4.4	Management of FPR_UNO.3.....	74
13.4.5	Management of FPR_UNO.4.....	74
13.4.6	Audit of FPR_UNO.1, FPR_UNO.2	74
13.4.7	Audit of FPR_UNO.3.....	74
13.4.8	Audit of FPR_UNO.4.....	74
13.4.9	FPR_UNO.1 Unobservability	74
13.4.10	FPR_UNO.2 Allocation of information impacting unobservability.....	74
13.4.11	FPR_UNO.3 Unobservability without soliciting information.....	75
13.4.12	FPR_UNO.4 Authorised user observability	75
14	Class FPT: Protection of the TSF	75
14.1	Fail secure (FPT_FLS).....	76
14.1.1	Family Behaviour.....	76
14.1.2	Component levelling	77
14.1.3	Management of FPT_FLS.1.....	77
14.1.4	Audit of FPT_FLS.1	77
14.1.5	FPT_FLS.1 Failure with preservation of secure state.....	77
14.2	Availability of exported TSF data (FPT_ITA).....	77
14.2.1	Family Behaviour.....	77
14.2.2	Component levelling	77
14.2.3	Management of FPT_ITA.1.....	77
14.2.4	Audit of FPT_ITA.1	77
14.2.5	FPT_ITA.1 Inter-TSF availability within a defined availability metric.....	77
14.3	Confidentiality of exported TSF data (FPT_ITC)	78
14.3.1	Family Behaviour.....	78
14.3.2	Component levelling	78
14.3.3	Management of FPT_ITC.1.....	78
14.3.4	Audit of FPT_ITC.1	78
14.3.5	FPT_ITC.1 Inter-TSF confidentiality during transmission.....	78
14.4	Integrity of exported TSF data (FPT_ITI).....	78
14.4.1	Family Behaviour.....	78
14.4.2	Component levelling	78
14.4.3	Management of FPT_ITI.1	79
14.4.4	Management of FPT_ITI.2	79
14.4.5	Audit of FPT_ITI.1	79
14.4.6	Audit of FPT_ITI.2	79
14.4.7	FPT_ITI.1 Inter-TSF detection of modification.....	79
14.4.8	FPT_ITI.2 Inter-TSF detection and correction of modification.....	79
14.5	Internal TOE TSF data transfer (FPT_ITT).....	80
14.5.1	Family Behaviour.....	80
14.5.2	Component levelling	80
14.5.3	Management of FPT_ITT.1	80
14.5.4	Management of FPT_ITT.2	80
14.5.5	Management of FPT_ITT.3	80
14.5.6	Audit of FPT_ITT.1, FPT_ITT.2.....	81
14.5.7	Audit of FPT_ITT.3.....	81
14.5.8	FPT_ITT.1 Basic internal TSF data transfer protection	81
14.5.9	FPT_ITT.2 TSF data transfer separation	81
14.5.10	FPT_ITT.3 TSF data integrity monitoring.....	81

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

14.13.5	FPT_TRC.1 Internal TSF consistency.....	90
14.14	TSF self test (FPT_TST).....	90
14.14.1	Family Behaviour.....	90
14.14.2	Component levelling.....	91
14.14.3	Management of FPT_TST.1.....	91
14.14.4	Audit of FPT_TST.1.....	91
14.14.5	FPT_TST.1 TSF testing.....	91
15	Class FRU: Resource utilisation.....	92
15.1	Fault tolerance (FRU_FLT).....	92
15.1.1	Family Behaviour.....	92
15.1.2	Component levelling.....	92
15.1.3	Management of FRU_FLT.1, FRU_FLT.2.....	92
15.1.4	Audit of FRU_FLT.1.....	92
15.1.5	Audit of FRU_FLT.2.....	92
15.1.6	FRU_FLT.1 Degraded fault tolerance.....	93
15.1.7	FRU_FLT.2 Limited fault tolerance.....	93
15.2	Priority of service (FRU_PRS).....	93
15.2.1	Family Behaviour.....	93
15.2.2	Component levelling.....	93
15.2.3	Management of FRU_PRS.1, FRU_PRS.2.....	93
15.2.4	Audit of FRU_PRS.1, FRU_PRS.2.....	93
15.2.5	FRU_PRS.1 Limited priority of service.....	93
15.2.6	FRU_PRS.2 Full priority of service.....	94
15.3	Resource allocation (FRU_RSA).....	94
15.3.1	Family Behaviour.....	94
15.3.2	Component levelling.....	94
15.3.3	Management of FRU_RSA.1.....	94
15.3.4	Management of FRU_RSA.2.....	94
15.3.5	Audit of FRU_RSA.1, FRU_RSA.2.....	94
15.3.6	FRU_RSA.1 Maximum quotas.....	95
15.3.7	FRU_RSA.2 Minimum and maximum quotas.....	95
16	Class FTA: TOE access.....	95
16.1	Limitation on scope of selectable attributes (FTA_LSA).....	96
16.1.1	Family Behaviour.....	96
16.1.2	Component levelling.....	96
16.1.3	Management of FTA_LSA.1.....	96
16.1.4	Audit of FTA_LSA.1.....	96
16.1.5	FTA_LSA.1 Limitation on scope of selectable attributes.....	97
16.2	Limitation on multiple concurrent sessions (FTA_MCS).....	97
16.2.1	Family Behaviour.....	97
16.2.2	Component levelling.....	97
16.2.3	Management of FTA_MCS.1.....	97
16.2.4	Management of FTA_MCS.2.....	97
16.2.5	Audit of FTA_MCS.1, FTA_MCS.2.....	97
16.2.6	FTA_MCS.1 Basic limitation on multiple concurrent sessions.....	97
16.2.7	FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions.....	98
16.3	Session locking and termination (FTA_SSL).....	98
16.3.1	Family Behaviour.....	98
16.3.2	Component levelling.....	98
16.3.3	Management of FTA_SSL.1.....	98
16.3.4	Management of FTA_SSL.2.....	98
16.3.5	Management of FTA_SSL.3.....	99
16.3.6	Management of FTA_SSL.4.....	99
16.3.7	Audit of FTA_SSL.1, FTA_SSL.2.....	99
16.3.8	Audit of FTA_SSL.3.....	99
16.3.9	Audit of FTA_SSL.4.....	99
16.3.10	FTA_SSL.1 TSF-initiated session locking.....	99
16.3.11	FTA_SSL.2 User-initiated locking.....	100
16.3.12	FTA_SSL.3 TSF-initiated termination.....	100

16.3.13	FTA_SSL.4 User-initiated termination	100
16.4	TOE access banners (FTA_TAB).....	100
16.4.1	Family Behaviour	100
16.4.2	Component levelling	100
16.4.3	Management of FTA_TAB.1	100
16.4.4	Audit of FTA_TAB.1	101
16.4.5	FTA_TAB.1 Default TOE access banners.....	101
16.5	TOE access history (FTA_TAH).....	101
16.5.1	Family Behaviour	101
16.5.2	Component levelling	101
16.5.3	Management of FTA_TAH.1	101
16.5.4	Audit of FTA_TAH.1	101
16.5.5	FTA_TAH.1 TOE access history	101
16.6	TOE session establishment (FTA_TSE)	102
16.6.1	Family Behaviour	102
16.6.2	Component levelling	102
16.6.3	Management of FTA_TSE.1	102
16.6.4	Audit of FTA_TSE.1	102
16.6.5	FTA_TSE.1 TOE session establishment.....	102
17	Class FTP: Trusted path/channels.....	102
17.1	Inter-TSF trusted channel (FTP_ITC)	103
17.1.1	Family Behaviour	103
17.1.2	Component levelling	103
17.1.3	Management of FTP_ITC.1	103
17.1.4	Audit of FTP_ITC.1	103
17.1.5	FTP_ITC.1 Inter-TSF trusted channel.....	103
17.2	Trusted path (FTP_TRP).....	104
17.2.1	Family Behaviour	104
17.2.2	Component levelling	104
17.2.3	Management of FTP_TRP.1	104
17.2.4	Audit of FTP_TRP.1	104
17.2.5	FTP_TRP.1 Trusted path	104
Annex A	(normative) Security functional requirements application notes.....	106
A.1	Structure of the notes	106
A.1.1	Class structure.....	106
A.1.2	Family structure	106
A.1.3	Component structure	107
A.2	Dependency tables	108
Annex B	(normative) Functional classes, families, and components	114
Annex C	(normative) Class FAU: Security audit.....	115
C.1	Audit requirements in a distributed environment	115
C.2	Security audit automatic response (FAU_ARP)	116
C.2.1	User notes	116
C.2.2	FAU_ARP.1 Security alarms	117
C.3	Security audit data generation (FAU_GEN)	117
C.3.1	User notes	117
C.3.2	FAU_GEN.1 Audit data generation.....	118
C.3.3	FAU_GEN.2 User identity association	119
C.4	Security audit analysis (FAU_SAA)	119
C.4.1	User notes	119
C.4.2	FAU_SAA.1 Potential violation analysis	119
C.4.3	FAU_SAA.2 Profile based anomaly detection	120
C.4.4	FAU_SAA.3 Simple attack heuristics.....	121
C.4.5	FAU_SAA.4 Complex attack heuristics	122
C.5	Security audit review (FAU_SAR)	122
C.5.1	User notes	122
C.5.2	FAU_SAR.1 Audit review	123
C.5.3	FAU_SAR.2 Restricted audit review	123

C.5.4	FAU_SAR.3 Selectable audit review	123
C.6	Security audit event selection (FAU_SEL)	124
C.6.1	User notes	124
C.6.2	FAU_SEL.1 Selective audit	124
C.7	Security audit event storage (FAU_STG)	125
C.7.1	User notes	125
C.7.2	FAU_STG.1 Protected audit trail storage	125
C.7.3	FAU_STG.2 Guarantees of audit data availability	125
C.7.4	FAU_STG.3 Action in case of possible audit data loss	126
C.7.5	FAU_STG.4 Prevention of audit data loss	126
Annex D	(normative) Class FCO: Communication	127
D.1	Non-repudiation of origin (FCO_NRO)	127
D.1.1	User notes	127
D.1.2	FCO_NRO.1 Selective proof of origin	128
D.1.3	FCO_NRO.2 Enforced proof of origin	128
D.2	Non-repudiation of receipt (FCO_NRR)	129
D.2.1	User notes	129
D.2.2	FCO_NRR.1 Selective proof of receipt	129
D.2.3	FCO_NRR.2 Enforced proof of receipt	130
Annex E	(normative) Class FCS: Cryptographic support	131
E.1	Cryptographic key management (FCS_CKM)	132
E.1.1	User notes	132
E.1.2	FCS_CKM.1 Cryptographic key generation	133
E.1.3	FCS_CKM.2 Cryptographic key distribution	133
E.1.4	FCS_CKM.3 Cryptographic key access	133
E.1.5	FCS_CKM.4 Cryptographic key destruction	134
E.2	Cryptographic operation (FCS_COP)	134
E.2.1	User notes	134
E.2.2	FCS_COP.1 Cryptographic operation	135
Annex F	(normative) Class FDP: User data protection	136
F.1	Access control policy (FDP_ACC)	139
F.1.1	User notes	139
F.1.2	FDP_ACC.1 Subset access control	139
F.1.3	FDP_ACC.2 Complete access control	140
F.2	Access control functions (FDP_ACF)	140
F.2.1	User notes	140
F.2.2	FDP_ACF.1 Security attribute based access control	140
F.3	Data authentication (FDP_DAU)	142
F.3.1	User notes	142
F.3.2	FDP_DAU.1 Basic Data Authentication	142
F.3.3	FDP_DAU.2 Data Authentication with Identity of Guarantor	142
F.4	Export from the TOE (FDP_ETC)	142
F.4.1	User notes	142
F.4.2	FDP_ETC.1 Export of user data without security attributes	143
F.4.3	FDP_ETC.2 Export of user data with security attributes	143
F.5	Information flow control policy (FDP_IFC)	144
F.5.1	User notes	144
F.5.2	FDP_IFC.1 Subset information flow control	145
F.5.3	FDP_IFC.2 Complete information flow control	145
F.6	Information flow control functions (FDP_IFF)	145
F.6.1	User notes	145
F.6.2	FDP_IFF.1 Simple security attributes	146
F.6.3	FDP_IFF.2 Hierarchical security attributes	147
F.6.4	FDP_IFF.3 Limited illicit information flows	148
F.6.5	FDP_IFF.4 Partial elimination of illicit information flows	148
F.6.6	FDP_IFF.5 No illicit information flows	149
F.6.7	FDP_IFF.6 Illicit information flow monitoring	149
F.7	Import from outside of the TOE (FDP_ITC)	150