
**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

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.

This document is a preview generated by EVS



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_IFT)	34
10.6.1	Family Behaviour	34
10.6.2	Component levelling	35
10.6.3	Management of FDP_IFT.1, FDP_IFT.2	35
10.6.4	Management of FDP_IFT.3, FDP_IFT.4, FDP_IFT.5	35
10.6.5	Management of FDP_IFT.6	35
10.6.6	Audit of FDP_IFT.1, FDP_IFT.2, FDP_IFT.5	35
10.6.7	Audit of FDP_IFT.3, FDP_IFT.4, FDP_IFT.6	36
10.6.8	FDP_IFT.1 Simple security attributes	36
10.6.9	FDP_IFT.2 Hierarchical security attributes	36
10.6.10	FDP_IFT.3 Limited illicit information flows	37
10.6.11	FDP_IFT.4 Partial elimination of illicit information flows	38
10.6.12	FDP_IFT.5 No illicit information flows	38
10.6.13	FDP_IFT.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 authorisations.....	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

F.7.1	User notes	150
F.7.2	FDP_ITC.1 Import of user data without security attributes	151
F.7.3	FDP_ITC.2 Import of user data with security attributes	151
F.8	Internal TOE transfer (FDP_ITT)	151
F.8.1	User notes	151
F.8.2	FDP_ITT.1 Basic internal transfer protection	152
F.8.3	FDP_ITT.2 Transmission separation by attribute	152
F.8.4	FDP_ITT.3 Integrity monitoring	152
F.8.5	FDP_ITT.4 Attribute-based integrity monitoring	153
F.9	Residual information protection (FDP_RIP)	154
F.9.1	User notes	154
F.9.2	FDP_RIP.1 Subset residual information protection	155
F.9.3	FDP_RIP.2 Full residual information protection	155
F.10	Rollback (FDP_ROL)	155
F.10.1	User notes	155
F.10.2	FDP_ROL.1 Basic rollback	156
F.10.3	FDP_ROL.2 Advanced rollback	156
F.11	Stored data integrity (FDP_SDI)	157
F.11.1	User notes	157
F.11.2	FDP_SDI.1 Stored data integrity monitoring	157
F.11.3	FDP_SDI.2 Stored data integrity monitoring and action	157
F.12	Inter-TSF user data confidentiality transfer protection (FDP_UCT)	157
F.12.1	User notes	157
F.12.2	FDP_UCT.1 Basic data exchange confidentiality	158
F.13	Inter-TSF user data integrity transfer protection (FDP_UIT)	158
F.13.1	User notes	158
F.13.2	FDP_UIT.1 Data exchange integrity	158
F.13.3	FDP_UIT.2 Source data exchange recovery	159
F.13.4	FDP_UIT.3 Destination data exchange recovery	159
Annex G	(normative) Class FIA: Identification and authentication	160
G.1	Authentication failures (FIA_AFL)	161
G.1.1	User notes	161
G.1.2	FIA_AFL.1 Authentication failure handling	162
G.2	User attribute definition (FIA_ATD)	163
G.2.1	User notes	163
G.2.2	FIA_ATD.1 User attribute definition	163
G.3	Specification of secrets (FIA_SOS)	163
G.3.1	User notes	163
G.3.2	FIA_SOS.1 Verification of secrets	164
G.3.3	FIA_SOS.2 TSF Generation of secrets	164
G.4	User authentication (FIA_UAU)	164
G.4.1	User notes	164
G.4.2	FIA_UAU.1 Timing of authentication	164
G.4.3	FIA_UAU.2 User authentication before any action	165
G.4.4	FIA_UAU.3 Unforgeable authentication	165
G.4.5	FIA_UAU.4 Single-use authentication mechanisms	165
G.4.6	FIA_UAU.5 Multiple authentication mechanisms	166
G.4.7	FIA_UAU.6 Re-authenticating	166
G.4.8	FIA_UAU.7 Protected authentication feedback	167
G.5	User identification (FIA_UID)	167
G.5.1	User notes	167
G.5.2	FIA_UID.1 Timing of identification	167
G.5.3	FIA_UID.2 User identification before any action	167
G.6	User-subject binding (FIA_USB)	168
G.6.1	User notes	168
G.6.2	FIA_USB.1 User-subject binding	168
Annex H	(normative) Class FMT: Security management	169
H.1	Management of functions in TSF (FMT_MOF)	170
H.1.1	User notes	170

H.1.2	FMT_MOF.1 Management of security functions behaviour	171
H.2	Management of security attributes (FMT_MSA)	171
H.2.1	User notes	171
H.2.2	FMT_MSA.1 Management of security attributes	172
H.2.3	FMT_MSA.2 Secure security attributes	172
H.2.4	FMT_MSA.3 Static attribute initialisation	173
H.2.5	FMT_MSA.4 Security attribute value inheritance	173
H.3	Management of TSF data (FMT_MTD)	173
H.3.1	User notes	173
H.3.2	FMT_MTD.1 Management of TSF data	174
H.3.3	FMT_MTD.2 Management of limits on TSF data	174
H.3.4	FMT_MTD.3 Secure TSF data	175
H.4	Revocation (FMT_REV)	175
H.4.1	User notes	175
H.4.2	FMT_REV.1 Revocation	175
H.5	Security attribute expiration (FMT_SAE)	176
H.5.1	User notes	176
H.5.2	FMT_SAE.1 Time-limited authorisation	176
H.6	Specification of Management Functions (FMT_SMF)	176
H.6.1	User notes	176
H.6.2	FMT_SMF.1 Specification of Management Functions	176
H.7	Security management roles (FMT_SMR)	176
H.7.1	User notes	176
H.7.2	FMT_SMR.1 Security roles	177
H.7.3	FMT_SMR.2 Restrictions on security roles	177
H.7.4	FMT_SMR.3 Assuming roles	177
Annex I	(normative) Class FPR: Privacy	179
I.1	Anonymity (FPR_ANO)	180
I.1.1	User notes	180
I.1.2	FPR_ANO.1 Anonymity	181
I.1.3	FPR_ANO.2 Anonymity without soliciting information	181
I.2	Pseudonymity (FPR_PSE)	182
I.2.1	User notes	182
I.2.2	FPR_PSE.1 Pseudonymity	183
I.2.3	FPR_PSE.2 Reversible pseudonymity	183
I.2.4	FPR_PSE.3 Alias pseudonymity	184
I.3	Unlinkability (FPR_UNL)	185
I.3.1	User notes	185
I.3.2	FPR_UNL.1 Unlinkability	186
I.4	Unobservability (FPR_UNO)	186
I.4.1	User notes	186
I.4.2	FPR_UNO.1 Unobservability	187
I.4.3	FPR_UNO.2 Allocation of information impacting unobservability	187
I.4.4	FPR_UNO.3 Unobservability without soliciting information	188
I.4.5	FPR_UNO.4 Authorised user observability	189
Annex J	(normative) Class FPT: Protection of the TSF	190
J.1	Fail secure (FPT_FLS)	191
J.1.1	User notes	191
J.1.2	FPT_FLS.1 Failure with preservation of secure state	192
J.2	Availability of exported TSF data (FPT_ITA)	192
J.2.1	User notes	192
J.2.2	FPT_ITA.1 Inter-TSF availability within a defined availability metric	192
J.3	Confidentiality of exported TSF data (FPT_ITC)	192
J.3.1	User notes	192
J.3.2	FPT_ITC.1 Inter-TSF confidentiality during transmission	193
J.4	Integrity of exported TSF data (FPT_ITI)	193
J.4.1	User notes	193
J.4.2	FPT_ITI.1 Inter-TSF detection of modification	193
J.4.3	FPT_ITI.2 Inter-TSF detection and correction of modification	193

J.5	Internal TOE TSF data transfer (FPT_ITT)	194
J.5.1	User notes	194
J.5.2	Evaluator notes	194
J.5.3	FPT_ITT.1 Basic internal TSF data transfer protection.....	194
J.5.4	FPT_ITT.2 TSF data transfer separation.....	194
J.5.5	FPT_ITT.3 TSF data integrity monitoring	195
J.6	TSF physical protection (FPT_PHP)	195
J.6.1	User notes	195
J.6.2	FPT_PHP.1 Passive detection of physical attack.....	196
J.6.3	FPT_PHP.2 Notification of physical attack	196
J.6.4	FPT_PHP.3 Resistance to physical attack	196
J.7	Trusted recovery (FPT_RCV).....	197
J.7.1	User notes	197
J.7.2	FPT_RCV.1 Manual recovery	198
J.7.3	FPT_RCV.2 Automated recovery.....	198
J.7.4	FPT_RCV.3 Automated recovery without undue loss.....	199
J.7.5	FPT_RCV.4 Function recovery	199
J.8	Replay detection (FPT_RPL).....	200
J.8.1	User notes	200
J.8.2	FPT_RPL.1 Replay detection.....	200
J.9	State synchrony protocol (FPT_SSP)	200
J.9.1	User notes	200
J.9.2	FPT_SSP.1 Simple trusted acknowledgement	201
J.9.3	FPT_SSP.2 Mutual trusted acknowledgement.....	201
J.10	Time stamps (FPT_STM)	201
J.10.1	User notes	201
J.10.2	FPT_STM.1 Reliable time stamps.....	201
J.11	Inter-TSF TSF data consistency (FPT_TDC).....	201
J.11.1	User notes	201
J.11.2	FPT_TDC.1 Inter-TSF basic TSF data consistency.....	202
J.12	Testing of external entities (FPT_TEE).....	202
J.12.1	User notes	202
J.12.2	Evaluator notes	202
J.12.3	FPT_TEE.1 Testing of external entities	202
J.13	Internal TOE TSF data replication consistency (FPT_TRC).....	203
J.13.1	User notes	203
J.13.2	FPT_TRC.1 Internal TSF consistency.....	203
J.14	TSF self test (FPT_TST)	204
J.14.1	User notes	204
J.14.2	FPT_TST.1 TSF testing.....	204
Annex K	(normative) Class FRU: Resource utilisation	206
K.1	Fault tolerance (FRU_FLT).....	206
K.1.1	User notes	206
K.1.2	FRU_FLT.1 Degraded fault tolerance.....	207
K.1.3	FRU_FLT.2 Limited fault tolerance	207
K.2	Priority of service (FRU_PRS)	207
K.2.1	User notes	207
K.2.2	FRU_PRS.1 Limited priority of service.....	208
K.2.3	FRU_PRS.2 Full priority of service	208
K.3	Resource allocation (FRU_RSA)	208
K.3.1	User notes	208
K.3.2	FRU_RSA.1 Maximum quotas	209
K.3.3	FRU_RSA.2 Minimum and maximum quotas	209
Annex L	(normative) Class FTA: TOE access	211
L.1	Limitation on scope of selectable attributes (FTA_LSA).....	212
L.1.1	User notes	212
L.1.2	FTA_LSA.1 Limitation on scope of selectable attributes	212
L.2	Limitation on multiple concurrent sessions (FTA_MCS).....	212
L.2.1	User notes	212

L.2.2	FTA_MCS.1 Basic limitation on multiple concurrent sessions	212
L.2.3	FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions	213
L.3	Session locking and termination (FTA_SSL)	213
L.3.1	User notes	213
L.3.2	FTA_SSL.1 TSF-initiated session locking	213
L.3.3	FTA_SSL.2 User-initiated locking	214
L.3.4	FTA_SSL.3 TSF-initiated termination	214
L.3.5	FTA_SSL.4 User-initiated termination	214
L.4	TOE access banners (FTA_TAB)	215
L.4.1	User notes	215
L.4.2	FTA_TAB.1 Default TOE access banners	215
L.5	TOE access history (FTA_TAH)	215
L.5.1	User notes	215
L.5.2	FTA_TAH.1 TOE access history	215
L.6	TOE session establishment (FTA_TSE)	215
L.6.1	User notes	215
L.6.2	FTA_TSE.1 TOE session establishment	216
Annex M	(normative) Class FTP: Trusted path/channels	217
M.1	Inter-TSF trusted channel (FTP_ITC)	217
M.1.1	User notes	217
M.1.2	FTP_ITC.1 Inter-TSF trusted channel	217
M.2	Trusted path (FTP_TRP)	218
M.2.1	User notes	218
M.2.2	FTP_TRP.1 Trusted path	218

Foreword

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

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

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

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

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

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

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

- *Part 1: Introduction and general model*
- *Part 2: Security functional components*
- *Part 3: Security assurance components*

Legal Notice

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

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;
France:	Direction Centrale de la Sécurité des Systèmes d'Information;
Germany:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;

Netherlands:	Netherlands National Communications Security Agency;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

This document is a preview generated by EVS

Introduction

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

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

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

- a) Consumers, who use this part of ISO/IEC 15408 when selecting components to express functional requirements to satisfy the security objectives expressed in a PP or ST. ISO/IEC 15408-1 provides more detailed information on the relationship between security objectives and security requirements.
- b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, may find a standardised method to understand those requirements in this part of ISO/IEC 15408. They can also use the contents of this part of ISO/IEC 15408 as a basis for further defining the TOE security functionality and mechanisms that comply with those requirements.
- c) Evaluators, who use the functional requirements defined in this part of ISO/IEC 15408 in verifying that the TOE functional requirements expressed in the PP or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators also should use this part of ISO/IEC 15408 to assist in determining whether a given TOE satisfies stated requirements.

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

Part 2: Security functional components

1 Scope

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

2 Normative references

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

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

3 Terms and definitions, symbols and abbreviated terms

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

4 Overview

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

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

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

4.1 Organisation of this part of ISO/IEC 15408

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

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

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