



DPC: 24/30482239 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 19 August 2024

Origin: European

Latest date for receipt of comments: 12 October 2024

Project No. 2023/02579

Responsible committee: IST/33/3 Security Evaluation, Testing and Specification

Interested committees:

Title: Draft BS EN ISO/IEC 15408-2 BS EN ISO/IEC 15408-2 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. Part 2: Security functional components.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 12 October 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Responsible Committee Secretary: Ms Joy Tan (BSI)

Direct tel:

E-mail: joy.tan@bsigroup.com

Full document details: 24/30482239 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 15408-2

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components

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

Partie 2: Composants fonctionnels de sécurité

ICS: 35.030

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-08-19

Voting terminates on:
2024-11-11

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 15408-2:2024(en)

Full document details: 24/30482239 DC

© ISO/IEC 2024  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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

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

Published in Switzerland

Contents

Foreword	xxi
Legal notice	xxii
Introduction	xxiii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	3
5 Overview	4
5.1 General	4
5.2 Organization of this document	4
6 Functional requirements paradigm	5
7 Security functional components	9
7.1 Overview	9
7.2 Functional class structure	9
7.2.1 General	9
7.2.2 Class name	9
7.2.3 Class introduction	9
7.2.4 Class informative notes	9
7.2.5 Functional families	10
7.3 Functional family structure	10
7.3.1 General	10
7.3.2 Family name	10
7.3.3 Family behaviour	10
7.3.4 Component levelling and description	10
7.3.5 Component management	11
7.3.6 Component audit	11
7.3.7 Family application notes	11
7.3.8 Family evaluator notes	12
7.3.9 Functional components	12
7.4 Functional component structure	12
7.4.1 General	12
7.4.2 Component name	12
7.4.3 Component relationships	12
7.4.4 Component rationale	13
7.4.5 Functional elements	13
7.5 Functional elements	13
7.6 Component catalogue	14
7.6.1 Highlighting of component changes	15
8 Class FAU Security audit	15
8.1 Introduction	15
8.2 Notes on class FAU	17
8.2.1 General information about audit requirements	17
8.2.2 Audit requirements in a distributed environment	17
8.3 Security audit automatic response (FAU_ARP)	18
8.3.1 Family Behaviour	18
8.3.2 Component levelling and description	18

8.3.3	Management of FAU_ARP.1	18
8.3.4	Audit of FAU_ARP.1	18
8.3.5	Application notes.....	18
8.3.6	FAU_ARP.1 Security alarms.....	19
8.4	Security audit data generation (FAU_GEN).....	19
8.4.1	Family Behaviour	19
8.4.2	Component levelling and description.....	19
8.4.3	Management of FAU_GEN.1, FAU_GEN.2	19
8.4.4	Audit of FAU_GEN.1, FAU_GEN.2	19
8.4.5	Application notes.....	20
8.4.6	Evaluator notes	21
8.4.7	FAU_GEN.1 Audit data generation	21
8.4.8	FAU_GEN.2 User identity association	22
8.5	Security audit analysis (FAU_SAA)	23
8.5.1	Family Behaviour	23
8.5.2	Component levelling and description.....	23
8.5.3	Management of FAU_SAA.1.....	23
8.5.4	Management of FAU_SAA.2.....	24
8.5.5	Management of FAU_SAA.3.....	24
8.5.6	Management of FAU_SAA.4.....	24
8.5.7	Audit of FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4.....	24
8.5.8	Application notes.....	24
8.5.9	FAU_SAA.1 Potential violation analysis.....	24
8.5.10	FAU_SAA.2 Profile based anomaly detection.....	25
8.5.11	FAU_SAA.3 Simple attack heuristics	26
8.5.12	FAU_SAA.4 Complex attack heuristics.....	28
8.6	Security audit review (FAU_SAR).....	29
8.6.1	Family Behaviour	29
8.6.2	Component levelling and description.....	29
8.6.3	Management of FAU_SAR.1.....	30
8.6.4	Management of FAU_SAR.2, FAU_SAR.3	30
8.6.5	Audit of FAU_SAR.1.....	30
8.6.6	Audit of FAU_SAR.2.....	30
8.6.7	Audit of FAU_SAR.3.....	30
8.6.8	Application notes.....	30
8.6.9	FAU_SAR.1 Audit review.....	31
8.6.10	FAU_SAR.2 Restricted audit review	31
8.6.11	FAU_SAR.3 Selectable audit review.....	31
8.7	Security audit event selection (FAU_SEL)	32
8.7.1	Family Behaviour	32
8.7.2	Component levelling and description.....	32
8.7.3	Management of FAU_SEL.1	32
8.7.4	Audit of FAU_SEL.1	32
8.7.5	Application notes.....	32
8.7.6	FAU_SEL.1 Selective audit.....	33
8.8	Security audit data storage (FAU_STG)	33
8.8.1	Family Behaviour	33
8.8.2	Component levelling and description.....	34
8.8.3	Management of FAU_STG.1.....	34
8.8.4	Management of FAU_STG.2.....	34
8.8.5	Management of FAU_STG.3.....	34
8.8.6	Management of FAU_STG.4.....	34
8.8.7	Management of FAU_STG.5.....	35

8.8.8	Audit of FAU_STG.1.....	35
8.8.9	Audit of FAU_STG.2, FAU_STG.3	35
8.8.10	Audit of FAU_STG.4.....	35
8.8.11	Audit of FAU_STG.5.....	35
8.8.12	Application notes.....	35
8.8.13	FAU_STG.1 Audit data storage location	35
8.8.14	FAU_STG.2 Protected audit data storage.....	36
8.8.15	FAU_STG.3 Guarantees of audit data availability.....	36
8.8.16	FAU_STG.4 Action in case of possible audit data loss	37
8.8.17	FAU_STG.5 Prevention of audit data loss	38
9	Class FCO Communication	38
9.1	Introduction	38
9.2	Notes on class FCO.....	39
9.3	Non-repudiation of origin (FCO_NRO).....	39
9.3.1	Family Behaviour	39
9.3.2	Component levelling and description.....	39
9.3.3	Management of FCO_NRO.1, FCO_NRO.2.....	40
9.3.4	Audit of FCO_NRO.1.....	40
9.3.5	Audit of FCO_NRO.2	40
9.3.6	Application notes.....	40
9.3.7	FCO_NRO.1 Selective proof of origin.....	41
9.3.8	FCO_NRO.2 Enforced proof of origin.....	42
9.4	Non-repudiation of receipt (FCO_NRR).....	43
9.4.1	Family Behaviour	43
9.4.2	Component levelling and description.....	43
9.4.3	Management of FCO_NRR.1, FCO_NRR.2	43
9.4.4	Audit of FCO_NRR.1	43
9.4.5	Audit of FCO_NRR.2	43
9.4.6	Application notes.....	44
9.4.7	FCO_NRR.1 Selective proof of receipt.....	44
9.4.8	FCO_NRR.2 Enforced proof of receipt.....	45
10	Class FCS Cryptographic support.....	46
10.1	Introduction	46
10.2	Notes on class FCS.....	48
10.3	Cryptographic key management (FCS_CKM)	49
10.3.1	Family Behaviour	49
10.3.2	Component levelling and description.....	50
10.3.3	Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, FCS_CKM.6	50
10.3.4	Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, FCS_CKM.6	50
10.3.5	Application notes.....	51
10.3.6	Evaluator notes	51
10.3.7	FCS_CKM.1 Cryptographic key generation	52
10.3.8	FCS_CKM.2 Cryptographic key distribution	52
10.3.9	FCS_CKM.3 Cryptographic key access.....	53
10.3.10	FCS_CKM.5 Cryptographic key derivation.....	53
10.3.11	FCS_CKM.6 Timing and event of cryptographic key destruction	54
10.4	Cryptographic operation (FCS_COP).....	55
10.4.1	Family Behaviour	55
10.4.2	Component levelling and description.....	55
10.4.3	Management of FCS_COP.1	56
10.4.4	Audit of FCS_COP.1	56
10.4.5	Application notes.....	56

10.4.6	FCS_COP.1 Cryptographic operation.....	57
10.5	Random bit generation (FCS_RBG).....	58
10.5.1	Family Behaviour	58
10.5.2	Component levelling and description.....	58
10.5.3	Management of FCS_RBG.1, FCS_RBG.2, FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6.....	58
10.5.4	Audit of FCS_RBG.1, FCS_RBG.2	59
10.5.5	Audit of FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6	59
10.5.6	Application notes.....	59
10.5.7	FCS_RBG.1 Random bit generation (RBG).....	59
10.5.8	FCS_RBG.2 Random bit generation (external seeding).....	60
10.5.9	FCS_RBG.3 Random bit generation (internal seeding - single source).....	61
10.5.10	FCS_RBG.4 Random bit generation (internal seeding - multiple sources)	62
10.5.11	FCS_RBG.5 Random bit generation (combining entropy sources).....	62
10.5.12	FCS_RBG.6 Random bit generation service.....	63
10.6	Generation of random numbers (FCS_RNG)	63
10.6.1	Family Behaviour	63
10.6.2	Component levelling and description.....	63
10.6.3	Management of FCS_RNG.1	63
10.6.4	Audit of FCS_RNG.1	63
10.6.5	Application notes.....	64
10.6.6	FCS_RNG.1 Random number generation	64
11	Class FDP User data protection.....	66
11.1	Introduction	66
11.2	Notes on class FDP	69
11.3	Access control policy (FDP_ACC).....	72
11.3.1	Family Behaviour	72
11.3.2	Component levelling and description.....	72
11.3.3	Management of FDP_ACC.1, FDP_ACC.2	72
11.3.4	Audit of FDP_ACC.1, FDP_ACC.2	72
11.3.5	Application notes.....	72
11.3.6	FDP_ACC.1 Subset access control.....	73
11.3.7	FDP_ACC.2 Complete access control	74
11.4	Access control functions (FDP_ACF)	74
11.4.1	Family Behaviour	74
11.4.2	Component levelling and description.....	74
11.4.3	Management of FDP_ACF.1.....	74
11.4.4	Audit of FDP_ACF.1.....	75
11.4.5	Application notes.....	75
11.4.6	FDP_ACF.1 Security attribute-based access control.....	75
11.5	Data authentication (FDP_DAU).....	77
11.5.1	Family Behaviour	77
11.5.2	Component levelling and description.....	77
11.5.3	Management of FDP_DAU.1, FDP_DAU.2	77
11.5.4	Audit of FDP_DAU.1.....	77
11.5.5	Audit of FDP_DAU.2.....	77
11.5.6	Application notes.....	78
11.5.7	FDP_DAU.1 Basic Data Authentication.....	78
11.5.8	FDP_DAU.2 Data Authentication with Identity of Guarantor.....	78
11.6	Export from the TOE (FDP_ETC).....	79
11.6.1	Family Behaviour	79
11.6.2	Component levelling and description.....	79
11.6.3	Management of FDP_ETC.1.....	79

11.6.4	Management of FDP_ETC.2.....	79
11.6.5	Audit of FDP_ETC.1, FDP_ETC.2.....	80
11.6.6	Application notes.....	80
11.6.7	FDP_ETC.1 Export of user data without security attributes.....	80
11.6.8	FDP_ETC.2 Export of user data with security attributes	80
11.7	Information flow control policy (FDP_IFC)	81
11.7.1	Family Behaviour	81
11.7.2	Component levelling and description	82
11.7.3	Management of FDP_IFC.1, FDP_IFC.2	82
11.7.4	Audit of FDP_IFC.1, FDP_IFC.2	82
11.7.5	Application notes.....	82
11.7.6	FDP_IFC.1 Subset information flow control	83
11.7.7	FDP_IFC.2 Complete information flow control	84
11.8	Information flow control functions (FDP_IFF).....	84
11.8.1	Family Behaviour	84
11.8.2	Component levelling and description	85
11.8.3	Management of FDP_IFF.1, FDP_IFF.2.....	85
11.8.4	Management of FDP_IFF.3, FDP_IFF.4, FDP_IFF.5.....	85
11.8.5	Management of FDP_IFF.6	85
11.8.6	Audit of FDP_IFF.1, FDP_IFF.2, FDP_IFF.5.....	86
11.8.7	Audit of FDP_IFF.3, FDP_IFF.4, FDP_IFF.6.....	86
11.8.8	Application notes.....	86
11.8.9	FDP_IFF.1 Simple security attributes	87
11.8.10	FDP_IFF.2 Hierarchical security attributes	88
11.8.11	FDP_IFF.3 Limited illicit information flows.....	90
11.8.12	FDP_IFF.4 Partial elimination of illicit information flows	90
11.8.13	FDP_IFF.5 No illicit information flows.....	91
11.8.14	FDP_IFF.6 Illicit information flow monitoring	91
11.9	Information retention control (FDP_IRC).....	92
11.9.1	Family Behaviour	92
11.9.2	Component levelling and description	93
11.9.3	Management of FDP_IRC.1.....	93
11.9.4	Audit of FDP_IRC.1.....	93
11.9.5	Application notes.....	93
11.9.6	FDP_IRC.1 Information retention control.....	93
11.10	Import from outside of the TOE (FDP_ITC)	94
11.10.1	Family Behaviour.....	94
11.10.2	Component levelling and description	94
11.10.3	Management of FDP_ITC.1, FDP_ITC.2	95
11.10.4	Audit of FDP_ITC.1, FDP_ITC.2	95
11.10.5	Application notes.....	95
11.10.6	FDP_ITC.1 Import of user data without security attributes	96
11.10.7	FDP_ITC.2 Import of user data with security attributes	97
11.11	Internal TOE transfer (FDP_ITT)	97
11.11.1	Family Behaviour.....	97
11.11.2	Component levelling and description	98
11.11.3	Management of FDP_ITT.1, FDP_ITT.2	98
11.11.4	Management of FDP_ITT.3, FDP_ITT.4	98
11.11.5	Audit of FDP_ITT.1, FDP_ITT.2	98
11.11.6	Audit of FDP_ITT.3, FDP_ITT.4	98
11.11.7	Application notes.....	99
11.11.8	FDP_ITT.1 Basic internal transfer protection.....	99
11.11.9	FDP_ITT.2 Transmission separation by attribute.....	99

11.11.10	FDP_ITT.3 Integrity monitoring	100
11.11.11	FDP_ITT.4 Attribute-based integrity monitoring.....	101
11.12	Residual information protection (FDP_RIP).....	102
11.12.1	Family Behaviour.....	102
11.12.2	Component levelling and description	102
11.12.3	Management of FDP_RIP.1, FDP_RIP.2	102
11.12.4	Audit of FDP_RIP.1, FDP_RIP.2	103
11.12.5	Application notes.....	103
11.12.6	FDP_RIP.1 Subset residual information protection.....	104
11.12.7	FDP_RIP.2 Full residual information protection	104
11.13	Rollback (FDP_ROL).....	105
11.13.1	Family Behaviour.....	105
11.13.2	Component levelling and description	105
11.13.3	Management of FDP_ROL.1, FDP_ROL.2	105
11.13.4	Audit of FDP_ROL.1, FDP_ROL.2	105
11.13.5	Application notes.....	105
11.13.6	FDP_ROL.1 Basic rollback	106
11.13.7	FDP_ROL.2 Advanced rollback	106
11.14	Stored data confidentiality (FDP_SDC)	107
11.14.1	Family Behaviour.....	107
11.14.2	Component levelling and description	107
11.14.3	Management of FDP_SDC.1, FDP_SDC.2	107
11.14.4	Audit of FDP_SDC.1, FDP_SDC.2	108
11.14.5	Application notes.....	108
11.14.6	Evaluator notes.....	108
11.14.7	FDP_SDC.1 Stored data confidentiality.....	108
11.14.8	FDP_SDC.2 Stored data confidentiality with dedicated method	108
11.15	Stored data integrity (FDP_SDI)	109
11.15.1	Family Behaviour.....	109
11.15.2	Component levelling and description	109
11.15.3	Management of FDP_SDI.1	109
11.15.4	Management of FDP_SDI.2	109
11.15.5	Audit of FDP_SDI.1	110
11.15.6	Audit of FDP_SDI.2	110
11.15.7	Application notes.....	110
11.15.8	FDP_SDI.1 Stored data integrity monitoring.....	110
11.15.9	FDP_SDI.2 Stored data integrity monitoring and action.....	111
11.16	Inter-TSF user data confidentiality transfer protection (FDP_UCT).....	111
11.16.1	Family Behaviour.....	111
11.16.2	Component levelling and description	111
11.16.3	Management of FDP_UCT.1.....	111
11.16.4	Audit of FDP_UCT.1.....	112
11.16.5	Application notes.....	112
11.16.6	FDP_UCT.1 Basic data exchange confidentiality	112
11.17	Inter-TSF user data integrity transfer protection (FDP_UIT).....	112
11.17.1	Family Behaviour.....	112
11.17.2	Component levelling and description	113
11.17.3	Management of FDP_UIT.1, FDP_UIT.2, FDP_UIT.3	113
11.17.4	Audit of FDP_UIT.1.....	113
11.17.5	Audit of FDP_UIT.2, FDP_UIT.3	113
11.17.6	Application notes.....	114
11.17.7	FDP_UIT.1 Data exchange integrity	114
11.17.8	FDP_UIT.2 Source data exchange recovery.....	115

11.17.9	FDP_UIT.3 Destination data exchange recovery	115
12	Class FIA Identification and authentication	116
12.1	Introduction	116
12.2	Notes on class FIA	118
12.3	Authentication failures (FIA_AFL)	119
12.3.1	Family Behaviour	119
12.3.2	Component levelling and description	119
12.3.3	Management of FIA_AFL.1	119
12.3.4	Audit of FIA_AFL.1	119
12.3.5	Application notes	119
12.3.6	FIA_AFL.1 Authentication failure handling	119
12.4	Authentication proof of identity (FIA_API)	121
12.4.1	Family Behaviour	121
12.4.2	Component levelling and description	121
12.4.3	Management of FIA_API.1	121
12.4.4	Audit of FIA_API.1	121
12.4.5	Application notes	121
12.4.6	FIA_API.1 Authentication proof of identity	122
12.5	User attribute definition (FIA_ATD)	122
12.5.1	Family Behaviour	122
12.5.2	Component levelling and description	122
12.5.3	Management of FIA_ATD.1	122
12.5.4	Audit of FIA_ATD.1	123
12.5.5	Application notes	123
12.5.6	FIA_ATD.1 User attribute definition	123
12.6	Specification of secrets (FIA_SOS)	123
12.6.1	Family Behaviour	123
12.6.2	Component levelling and description	123
12.6.3	Management of FIA_SOS.1	124
12.6.4	Management of FIA_SOS.2	124
12.6.5	Audit of FIA_SOS.1, FIA_SOS.2	124
12.6.6	Application notes	124
12.6.7	FIA_SOS.1 Verification of secrets	124
12.6.8	FIA_SOS.2 TSF Generation of secrets	125
12.7	User authentication (FIA_UAU)	125
12.7.1	Family Behaviour	125
12.7.2	Component levelling and description	126
12.7.3	Management of FIA_UAU.1	126
12.7.4	Management of FIA_UAU.2	127
12.7.5	Management of FIA_UAU.3, FIA_UAU.4	127
12.7.6	Management of FIA_UAU.5	127
12.7.7	Management of FIA_UAU.6	127
12.7.8	Management of FIA_UAU.7	127
12.7.9	Audit of FIA_UAU.1	127
12.7.10	Audit of FIA_UAU.2	127
12.7.11	Audit of FIA_UAU.3	127
12.7.12	Audit of FIA_UAU.4	128
12.7.13	Audit of FIA_UAU.5	128
12.7.14	Audit of FIA_UAU.6	128
12.7.15	Audit of FIA_UAU.7	128
12.7.16	Application notes	128
12.7.17	FIA_UAU.1 Timing of authentication	128
12.7.18	FIA_UAU.2 User authentication before any action	129

12.7.19	FIA_UAU.3 Unforgeable authentication	129
12.7.20	FIA_UAU.4 Single-use authentication mechanisms	130
12.7.21	FIA_UAU.5 Multiple authentication mechanisms	130
12.7.22	FIA_UAU.6 Re-authenticating.....	131
12.7.23	FIA_UAU.7 Protected authentication feedback	131
12.8	User identification (FIA_UID)	132
12.8.1	Family Behaviour	132
12.8.2	Component levelling and description	132
12.8.3	Management of FIA_UID.1	132
12.8.4	Management of FIA_UID.2	132
12.8.5	Audit of FIA_UID.1, FIA_UID.2	132
12.8.6	Application notes.....	132
12.8.7	FIA_UID.1 Timing of identification	132
12.8.8	FIA_UID.2 User identification before any action	133
12.9	User-subject binding (FIA_USB)	133
12.9.1	Family Behaviour	133
12.9.2	Component levelling and description	133
12.9.3	Management of FIA_USB.1	134
12.9.4	Audit of FIA_USB.1	134
12.9.5	Application notes.....	134
12.9.6	FIA_USB.1 User-subject binding	134
13	Class FMT Security management	135
13.1	Introduction	135
13.2	Notes on class FMT.....	137
13.3	Limited capabilities and availability (FMT_LIM)	137
13.3.1	Family Behaviour	137
13.3.2	Component levelling and description	138
13.3.3	Management of FMT_LIM.1, FMT_LIM.2	138
13.3.4	Audit of FMT_LIM.1, FMT_LIM.2	138
13.3.5	Application notes.....	138
13.3.6	FMT_LIM.1 Limited capabilities	138
13.3.7	FMT_LIM.2 Limited availability	139
13.4	Management of functions in TSF (FMT_MOF).....	139
13.4.1	Family Behaviour	139
13.4.2	Component levelling and description	139
13.4.3	Management of FMT_MOF.1	139
13.4.4	Audit of FMT_MOF.1.....	139
13.4.5	Application notes.....	140
13.4.6	FMT_MOF.1 Management of security functions behaviour	140
13.5	Management of security attributes (FMT_MSA)	141
13.5.1	Family Behaviour	141
13.5.2	Component levelling and description	141
13.5.3	Management of FMT_MSA.1	142
13.5.4	Management of FMT_MSA.2	142
13.5.5	Management of FMT_MSA.3	142
13.5.6	Management of FMT_MSA.4	142
13.5.7	Audit of FMT_MSA.1	142
13.5.8	Audit of FMT_MSA.2	142
13.5.9	Audit of FMT_MSA.3	142
13.5.10	Audit of FMT_MSA.4	142
13.5.11	Application notes.....	143
13.5.12	FMT_MSA.1 Management of security attributes	143
13.5.13	FMT_MSA.2 Secure security attributes.....	144

13.5.14	FMT_MSA.3 Static attribute initialization	144
13.5.15	FMT_MSA.4 Security attribute value inheritance.....	145
13.6	Management of TSF data (FMT_MTD)	145
13.6.1	Family Behaviour	145
13.6.2	Component levelling and description.....	146
13.6.3	Management of FMT_MTD.1	146
13.6.4	Management of FMT_MTD.2	146
13.6.5	Management of FMT_MTD.3	146
13.6.6	Audit of FMT_MTD.1	146
13.6.7	Audit of FMT_MTD.2	146
13.6.8	Audit of FMT_MTD.3	147
13.6.9	Application notes.....	147
13.6.10	FMT_MTD.1 Management of TSF data	147
13.6.11	FMT_MTD.2 Management of limits on TSF data.....	147
13.6.12	FMT_MTD.3 Secure TSF data.....	148
13.7	Revocation (FMT_REV)	148
13.7.1	Family Behaviour	148
13.7.2	Component levelling and description.....	149
13.7.3	Management of FMT_REV.1.....	149
13.7.4	Audit of FMT_REV.1.....	149
13.7.5	Application notes.....	149
13.7.6	FMT_REV.1 Revocation	149
13.8	Security attribute expiration (FMT_SAE).....	150
13.8.1	Family Behaviour	150
13.8.2	Component levelling and description.....	150
13.8.3	Management of FMT_SAE.1	150
13.8.4	Audit of FMT_SAE.1	150
13.8.5	Application notes.....	150
13.8.6	FMT_SAE.1 Time-limited authorization	151
13.9	Specification of Management Functions (FMT_SMF).....	151
13.9.1	Family Behaviour	151
13.9.2	Component levelling and description.....	151
13.9.3	Management of FMT_SMF.1	151
13.9.4	Audit of FMT_SMF.1	152
13.9.5	Application notes.....	152
13.9.6	FMT_SMF.1 Specification of Management Functions.....	152
13.10	Security management roles (FMT_SMR)	152
13.10.1	Family Behaviour.....	152
13.10.2	Component levelling and description	152
13.10.3	Management of FMT_SMR.1	153
13.10.4	Management of FMT_SMR.2	153
13.10.5	Management of FMT_SMR.3	153
13.10.6	Audit of FMT_SMR.1	153
13.10.7	Audit of FMT_SMR.2	153
13.10.8	Audit of FMT_SMR.3	153
13.10.9	Application notes.....	153
13.10.10	FMT_SMR.1 Security roles.....	154
13.10.11	FMT_SMR.2 Restrictions on security roles.....	154
13.10.12	FMT_SMR.3 Assuming roles.....	155
14	Class FPR Privacy.....	155
14.1	Introduction.....	155
14.2	Notes on class FPR.....	156
14.3	Anonymity (FPR_ANO).....	158

14.3.1	Family Behaviour	158
14.3.2	Component levelling and description	158
14.3.3	Management of FPR_ANO.1, FPR_ANO.2	158
14.3.4	Audit of FPR_ANO.1, FPR_ANO.2	158
14.3.5	Application notes.....	158
14.3.6	FPR_ANO.1 Anonymity.....	159
14.3.7	FPR_ANO.2 Anonymity without soliciting information	159
14.4	Pseudonymity (FPR_PSE)	160
14.4.1	Family Behaviour	160
14.4.2	Component levelling and description	160
14.4.3	Management of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3	160
14.4.4	Audit of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3	160
14.4.5	Application notes.....	161
14.4.6	FPR_PSE.1 Pseudonymity	162
14.4.7	FPR_PSE.2 Reversible pseudonymity	163
14.4.8	FPR_PSE.3 Alias pseudonymity.....	164
14.5	Unlinkability (FPR_UNL)	165
14.5.1	Family Behaviour	165
14.5.2	Component levelling and description	166
14.5.3	Management of FPR_UNL.1	166
14.5.4	Audit of FPR_UNL.1	166
14.5.5	Application notes.....	166
14.5.6	FPR_UNL.1 Unlinkability of operations	167
14.6	Unobservability (FPR_UNO)	168
14.6.1	Family Behaviour	168
14.6.2	Component levelling and description	168
14.6.3	Management of FPR_UNO.1, FPR_UNO.2.....	168
14.6.4	Management of FPR_UNO.3.....	168
14.6.5	Management of FPR_UNO.4.....	168
14.6.6	Audit of FPR_UNO.1, FPR_UNO.2	168
14.6.7	Audit of FPR_UNO.3.....	169
14.6.8	Audit of FPR_UNO.4.....	169
14.6.9	Application notes.....	169
14.6.10	FPR_UNO.1 Unobservability	170
14.6.11	FPR_UNO.2 Allocation of information impacting unobservability.....	170
14.6.12	FPR_UNO.3 Unobservability without soliciting information.....	172
14.6.13	FPR_UNO.4 Authorized user observability	172
15	Class FPT Protection of the TSF	173
15.1	Introduction	173
15.2	Notes on class FPT	175
15.3	TOE emanation (FPT_EMS)	176
15.3.1	Family Behaviour	176
15.3.2	Component levelling and description	176
15.3.3	Management of FPT_EMS.1	177
15.3.4	Audit of FPT_EMS.1	177
15.3.5	Application notes.....	177
15.3.6	FPT_EMS.1 Emanation of TSF and User data.....	177
15.4	Fail secure (FPT_FLS).....	178
15.4.1	Family Behaviour	178
15.4.2	Component levelling and description	178
15.4.3	Management of FPT_FLS.1.....	178
15.4.4	Audit of FPT_FLS.1.....	178
15.4.5	Application notes.....	178

15.4.6	FPT_FLS.1 Failure with preservation of secure state	178
15.5	TSF initialization (FPT_INI)	179
15.5.1	Family Behaviour	179
15.5.2	Component levelling and description	179
15.5.3	Management of FPT_INI.1	179
15.5.4	Audit of FPT_INI.1	179
15.5.5	Application notes	179
15.5.6	FPT_INI.1 TSF initialization	180
15.6	Availability of exported TSF data (FPT_ITA)	181
15.6.1	Family Behaviour	181
15.6.2	Component levelling and description	181
15.6.3	Management of FPT_ITA.1	181
15.6.4	Audit of FPT_ITA.1	181
15.6.5	Application notes	181
15.6.6	FPT_ITA.1 Inter-TSF availability within a defined availability metric	181
15.7	Confidentiality of exported TSF data (FPT_ITC)	182
15.7.1	Family Behaviour	182
15.7.2	Component levelling and description	182
15.7.3	Management of FPT_ITC.1	182
15.7.4	Audit of FPT_ITC.1	182
15.7.5	Application notes	182
15.7.6	Evaluator notes	182
15.7.7	FPT_ITC.1 Inter-TSF confidentiality during transmission	183
15.8	Integrity of exported TSF data (FPT_ITI)	183
15.8.1	Family Behaviour	183
15.8.2	Component levelling and description	183
15.8.3	Management of FPT_ITI.1	183
15.8.4	Management of FPT_ITI.2	183
15.8.5	Audit of FPT_ITI.1	183
15.8.6	Audit of FPT_ITI.2	184
15.8.7	Application notes	184
15.8.8	Evaluator notes	184
15.8.9	FPT_ITI.1 Inter-TSF detection of modification	184
15.8.10	FPT_ITI.2 Inter-TSF detection and correction of modification	185
15.9	Internal TOE TSF data transfer (FPT_ITT)	186
15.9.1	Family Behaviour	186
15.9.2	Component levelling and description	186
15.9.3	Management of FPT_ITT.1	186
15.9.4	Management of FPT_ITT.2	186
15.9.5	Management of FPT_ITT.3	186
15.9.6	Audit of FPT_ITT.1, FPT_ITT.2	187
15.9.7	Audit of FPT_ITT.3	187
15.9.8	Application notes	187
15.9.9	Evaluator notes	187
15.9.10	FPT_ITT.1 Basic internal TSF data transfer protection	187
15.9.11	FPT_ITT.2 TSF data transfer separation	187
15.9.12	FPT_ITT.3 TSF data integrity monitoring	188
15.10	TSF physical protection (FPT_PHP)	188
15.10.1	Family Behaviour	188
15.10.2	Component levelling and description	189
15.10.3	Management of FPT_PHP.1	189
15.10.4	Management of FPT_PHP.2	189
15.10.5	Management of FPT_PHP.3	189

15.10.6	Audit of FPT_PHP.1.....	189
15.10.7	Audit of FPT_PHP.2.....	189
15.10.8	Audit of FPT_PHP.3.....	190
15.10.9	Application notes.....	190
15.10.10	FPT_PHP.1 Passive detection of physical attack.....	190
15.10.11	FPT_PHP.2 Notification of physical attack.....	191
15.10.12	FPT_PHP.3 Resistance to physical attack.....	191
15.11	Trusted recovery (FPT_RCV).....	192
15.11.1	Family Behaviour.....	192
15.11.2	Component levelling and description	192
15.11.3	Management of FPT_RCV.1	193
15.11.4	Management of FPT_RCV.2, FPT_RCV.3	193
15.11.5	Management of FPT_RCV.4	193
15.11.6	Audit of FPT_RCV.1, FPT_RCV.2, FPT_RCV.3.....	193
15.11.7	Audit of FPT_RCV.4	193
15.11.8	Application notes.....	193
15.11.9	Evaluator notes.....	195
15.11.10	FPT_RCV.1 Manual recovery	195
15.11.11	FPT_RCV.2 Automated recovery.....	195
15.11.12	FPT_RCV.3 Automated recovery without undue loss.....	196
15.11.13	FPT_RCV.4 Function recovery	197
15.12	Replay detection (FPT_RPL)	197
15.12.1	Family Behaviour.....	197
15.12.2	Component levelling and description	197
15.12.3	Management of FPT_RPL.1	197
15.12.4	Audit of FPT_RPL.1	198
15.12.5	Application notes.....	198
15.12.6	FPT_RPL.1 Replay detection	198
15.13	State synchrony protocol (FPT_SSP)	198
15.13.1	Family Behaviour.....	198
15.13.2	Component levelling and description	199
15.13.3	Management of FPT_SSP.1, FPT_SSP.2	199
15.13.4	Audit of FPT_SSP.1, FPT_SSP.2	199
15.13.5	Application notes.....	199
15.13.6	FPT_SSP.1 Simple trusted acknowledgement.....	199
15.13.7	FPT_SSP.2 Mutual trusted acknowledgement	200
15.14	Time stamps (FPT_STM)	200
15.14.1	Family Behaviour.....	200
15.14.2	Component levelling and description	200
15.14.3	Management of FPT_STM.1.....	201
15.14.4	Management of FPT_STM.2.....	201
15.14.5	Audit of FPT_STM.1.....	201
15.14.6	Audit of FPT_STM.2.....	201
15.14.7	Application notes.....	201
15.14.8	FPT_STM.1 Reliable time stamps	201
15.14.9	FPT_STM.2 Time source.....	201
15.15	Inter-TSF TSF data consistency (FPT_TDC).....	202
15.15.1	Family Behaviour.....	202
15.15.2	Component levelling and description	202
15.15.3	Management of FPT_TDC.1	202
15.15.4	Audit of FPT_TDC.1	202
15.15.5	Application notes.....	202
15.15.6	FPT_TDC.1 Inter-TSF basic TSF data consistency	203

15.16	Testing of external entities (FPT_TEE)	203
15.16.1	Family Behaviour	203
15.16.2	Component levelling and description	204
15.16.3	Management of FPT_TEE.1	204
15.16.4	Audit of FPT_TEE.1	204
15.16.5	Application notes	204
15.16.6	Evaluator notes	204
15.16.7	FPT_TEE.1 Testing of external entities	205
15.17	Internal TOE TSF data replication consistency (FPT_TRC)	206
15.17.1	Family Behaviour	206
15.17.2	Component levelling and description	206
15.17.3	Management of FPT_TRC.1	206
15.17.4	Audit of FPT_TRC.1	206
15.17.5	Application notes	206
15.17.6	FPT_TRC.1 Internal TSF consistency	206
15.18	TSF self-test (FPT_TST)	207
15.18.1	Family Behaviour	207
15.18.2	Component levelling and description	207
15.18.3	Management of FPT_TST.1	207
15.18.4	Audit of FPT_TST.1	207
15.18.5	Application notes	208
15.18.6	Evaluator notes	208
15.18.7	FPT_TST.1 TSF self-testing	208
16	Class FRU Resource utilization	209
16.1	Introduction	209
16.2	Notes on class FRU	210
16.3	Fault tolerance (FRU_FLT)	210
16.3.1	Family Behaviour	210
16.3.2	Component levelling and description	210
16.3.3	Management of FRU_FLT.1, FRU_FLT.2	211
16.3.4	Audit of FRU_FLT.1	211
16.3.5	Audit of FRU_FLT.2	211
16.3.6	Application notes	211
16.3.7	FRU_FLT.1 Degraded fault tolerance	211
16.3.8	FRU_FLT.2 Limited fault tolerance	212
16.4	Priority of service (FRU_PRS)	212
16.4.1	Family Behaviour	212
16.4.2	Component levelling and description	212
16.4.3	Management of FRU_PRS.1, FRU_PRS.2	213
16.4.4	Audit of FRU_PRS.1, FRU_PRS.2	213
16.4.5	Application notes	213
16.4.6	FRU_PRS.1 Limited priority of service	213
16.4.7	FRU_PRS.2 Full priority of service	214
16.5	Resource allocation (FRU_RSA)	214
16.5.1	Family Behaviour	214
16.5.2	Component levelling and description	214
16.5.3	Management of FRU_RSA.1	214
16.5.4	Management of FRU_RSA.2	215
16.5.5	Audit of FRU_RSA.1, FRU_RSA.2	215
16.5.6	Application notes	215
16.5.7	FRU_RSA.1 Maximum quotas	215
16.5.8	FRU_RSA.2 Minimum and maximum quotas	216

17	Class FTA TOE access.....	217
17.1	Introduction.....	217
17.2	Notes on class FTA.....	219
17.3	Limitation on scope of selectable attributes (FTA_LSA).....	219
17.3.1	Family Behaviour.....	219
17.3.2	Component levelling and description.....	219
17.3.3	Management of FTA_LSA.1.....	219
17.3.4	Audit of FTA_LSA.1.....	219
17.3.5	Application notes.....	220
17.3.6	FTA_LSA.1 Limitation on scope of selectable attributes.....	220
17.4	Limitation on multiple concurrent sessions (FTA_MCS).....	221
17.4.1	Family Behaviour.....	221
17.4.2	Component levelling and description.....	221
17.4.3	Management of FTA_MCS.1.....	221
17.4.4	Management of FTA_MCS.2.....	221
17.4.5	Audit of FTA_MCS.1, FTA_MCS.2.....	221
17.4.6	Application notes.....	221
17.4.7	FTA_MCS.1 Basic limitation on multiple concurrent sessions.....	221
17.4.8	FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions.....	222
17.5	Session locking and termination (FTA_SSL).....	222
17.5.1	Family Behaviour.....	222
17.5.2	Component levelling and description.....	223
17.5.3	Management of FTA_SSL.1.....	223
17.5.4	Management of FTA_SSL.2.....	223
17.5.5	Management of FTA_SSL.3.....	223
17.5.6	Management of FTA_SSL.4.....	224
17.5.7	Audit of FTA_SSL.1, FTA_SSL.2.....	224
17.5.8	Audit of FTA_SSL.3.....	224
17.5.9	Audit of FTA_SSL.4.....	224
17.5.10	Application notes.....	224
17.5.11	FTA_SSL.1 TSF-initiated session locking.....	224
17.5.12	FTA_SSL.2 User-initiated locking.....	225
17.5.13	FTA_SSL.3 TSF-initiated termination.....	226
17.5.14	FTA_SSL.4 User-initiated termination.....	226
17.6	TOE access banners (FTA_TAB).....	227
17.6.1	Family Behaviour.....	227
17.6.2	Component levelling and description.....	227
17.6.3	Management of FTA_TAB.1.....	227
17.6.4	Audit of FTA_TAB.1.....	227
17.6.5	Application notes.....	227
17.6.6	FTA_TAB.1 Default TOE access banners.....	227
17.7	TOE access history (FTA_TAH).....	228
17.7.1	Family Behaviour.....	228
17.7.2	Component levelling and description.....	228
17.7.3	Management of FTA_TAH.1.....	228
17.7.4	Audit of FTA_TAH.1.....	228
17.7.5	Application notes.....	228
17.7.6	FTA_TAH.1 TOE access history.....	228
17.8	TOE session establishment (FTA_TSE).....	229
17.8.1	Family Behaviour.....	229
17.8.2	Component levelling and description.....	229
17.8.3	Management of FTA_TSE.1.....	229
17.8.4	Audit of FTA_TSE.1.....	229

17.8.5 Application notes.....	229
17.8.6 FTA_TSE.1 TOE session establishment	230
18 Class FTP Trusted path/channels	230
18.1 Introduction	230
18.2 Notes on class FTP	232
18.3 Inter-TSF trusted channel (FTP_ITC)	232
18.3.1 Family Behaviour	232
18.3.2 Component levelling and description	232
18.3.3 Management of FTP_ITC.1	232
18.3.4 Audit of FTP_ITC.1	232
18.3.5 Application notes.....	233
18.3.6 FTP_ITC.1 Inter-TSF trusted channel	233
18.4 Trusted channel protocol (FTP_PRO)	233
18.4.1 Family Behaviour	233
18.4.2 Component levelling and description	234
18.4.3 Management of FTP_PRO.1	234
18.4.4 Management of FTP_PRO.2	234
18.4.5 Management of FTP_PRO.3	234
18.4.6 Audit of FTP_PRO.1	234
18.4.7 Audit of FTP_PRO.2	235
18.4.8 Audit of FTP_PRO.3	235
18.4.9 Application notes.....	235
18.4.10 FTP_PRO.1 Trusted channel protocol.....	235
18.4.11 FTP_PRO.2 Trusted channel establishment	237
18.4.12 FTP_PRO.3 Trusted channel data protection.....	237
18.5 Trusted path (FTP_TRP)	238
18.5.1 Family Behaviour	238
18.5.2 Component levelling and description	238
18.5.3 Management of FTP_TRP.1	238
18.5.4 Audit of FTP_TRP.1	239
18.5.5 Application notes.....	239
18.5.6 FTP_TRP.1 Trusted path	239
Bibliography.....	241

List of figures

Figure 1 — Relationship between user data and TSF data.....	8
Figure 2 — Relationship between authentication data and secrets	8
Figure 3 — Functional class structure	9
Figure 4 — Functional family structure.....	10
Figure 5 — Functional component structure	12
Figure 6 — Functional element structure.....	14
Figure 7 — Sample class decomposition diagram.....	15
Figure 8 — FAU: Security audit, class decomposition	16
Figure 9 — FAU_ARP: Component levelling.....	18
Figure 10 — FAU_GEN: Component levelling.....	19
Figure 11 — FAU_SAA: Component levelling	23
Figure 12 — FAU_SAR: Component levelling	29
Figure 13 — FAU_SEL: Component levelling.....	32
Figure 14 — FAU_STG: Component levelling.....	34
Figure 15 — FCO: Communication, class decomposition.....	39
Figure 16 — FCO_NRO: Component levelling.....	39
Figure 17 — FCO_NRR: Component levelling.....	43
Figure 18 — FCS: Cryptographic support, class decomposition	47
Figure 19 — FCS_CKM: Component levelling.....	50
Figure 20 — FCS_COP: Component levelling	55
Figure 21 — FCS_RBG: Component levelling.....	58
Figure 22 — FCS_RNG: Component levelling.....	63
Figure 23 — FDP: User data protection, class decomposition	68
Figure 24 — FDP_ACC: Component levelling	72
Figure 25 — FDP_ACF: Component levelling.....	74
Figure 26 — FDP_DAU: Component levelling.....	77
Figure 27 — FDP_ETC: Component levelling.....	79
Figure 28 — FDP_IFC: Component levelling.....	82
Figure 29 — FDP_IFF: Component levelling.....	85
Figure 30 — FDP_IRC: Component levelling.....	93
Figure 31 — FDP_ITC: Component levelling.....	94
Figure 32 — FDP_ITT: Component levelling.....	98
Figure 33 — FDP_RIP: Component levelling.....	102
Figure 34 — FDP_ROL: Component levelling	105
Figure 35 — FDP_SDC: Component levelling.....	107
Figure 36 — FDP_SDI: Component levelling.....	109
Figure 37 — FDP_UCT: Component levelling	111
Figure 38 — FDP_UIT: Component levelling	113
Figure 39 — FIA: Identification and authentication, class decomposition	117
Figure 40 — FIA_AFL: Component levelling.....	119
Figure 41 — FIA_API: Component levelling.....	121
Figure 42 — FIA_ATD: Component levelling	122
Figure 43 — FIA_SOS: Component levelling	123
Figure 44 — FIA_UAU: Component levelling.....	126
Figure 45 — FIA_UID: Component levelling	132
Figure 46 — FIA_USB: Component levelling.....	133
Figure 47 — FMT: Security management, class decomposition.....	136
Figure 48 — FMT_LIM: Component levelling.....	138
Figure 49 — FMT_MOF: Component levelling	139
Figure 50 — FMT_MSA: Component levelling.....	141
Figure 51 — FMT_MTD: Component levelling.....	146

Figure 52 — FMT_REV: Component levelling	149
Figure 53 — FMT_SAE: Component levelling.....	150
Figure 54 — FMT_SMF: Component levelling	151
Figure 55 — FMT_SMR: Component levelling.....	152
Figure 56 — FPR: Privacy, class decomposition	156
Figure 57 — FPR_ANO: Component levelling.....	158
Figure 58 — FPR_PSE: Component levelling	160
Figure 59 — FPR_UNL: Component levelling.....	166
Figure 60 — FPR_UNO: Component levelling.....	168
Figure 61 — FPT: Protection of the TSF, class decomposition	174
Figure 62 — FPT_EMS: Component levelling.....	176
Figure 63 — FPT_FLS: Component levelling.....	178
Figure 64 — FPT_INI: Component levelling.....	179
Figure 65 — FPT_ITA: Component levelling.....	181
Figure 66 — FPT_ITC: Component levelling.....	182
Figure 67 — FPT_ITI: Component levelling	183
Figure 68 — FPT_ITT: Component levelling.....	186
Figure 69 — FPT_PHP: Component levelling	189
Figure 70 — FPT_RCV: Component levelling.....	192
Figure 71 — FPT_RPL: Component levelling.....	197
Figure 72 — FPT_SSP: Component levelling.....	199
Figure 73 — FPT_STM: Component levelling.....	200
Figure 74 — FPT_TDC: Component levelling	202
Figure 75 — FPT_TEE: Component levelling.....	204
Figure 76 — FPT_TRC: Component levelling.....	206
Figure 77 — FPT_TST: Component levelling	207
Figure 78 — FRU: Resource utilization, class decomposition.....	210
Figure 79 — FRU_FLT: Component levelling.....	210
Figure 80 — FRU_PRS: Component levelling.....	212
Figure 81 — FRU_RSA: Component levelling	214
Figure 82 — FTA: TOE access, class decomposition.....	218
Figure 83 — FTA_LSA: Component levelling.....	219
Figure 84 — FTA_MCS: Component levelling.....	221
Figure 85 — FTA_SSL: Component levelling.....	223
Figure 86 — FTA_TAB: Component levelling.....	227
Figure 87 — FTA_TAH: Component levelling.....	228
Figure 88 — FTA_TSE: Component levelling.....	229
Figure 89 — FTP: Trusted path/channels, class decomposition.....	231
Figure 90 — FTP_ITC: Component levelling.....	232
Figure 91 — FTP_PRO: Component levelling	234
Figure 92 — FTP_TRP: Component levelling.....	238

List of tables

Table 1 — Dependency table for Class FAU: Security audit	17
Table 2 — Dependency table for Class FCO: Communication	39
Table 3 — Dependency table for Class FCS: Cryptographic support.....	48
Table 4 — Dependency table for Class FDP: User data protection.....	69
Table 5 — Dependency table for Class FIA: Identification and authentication.....	118
Table 6 — Dependency table for Class FMT: Security management	137
Table 7 — Dependency table for Class FPR: Privacy.....	156
Table 8 — Dependency table for Class FPT: Protection of the TSF	175
Table 9 — Limit of Emissions	177
Table 10 — Initialization	180
Table 11 — Dependency table for Class FRU: Resource utilization.....	210
Table 12 — Dependency table for Class FTA: TOE access	219
Table 13 — Dependency table for Class FTP: Trusted path/channels	232

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

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

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

This fifth edition cancels and replaces the fourth edition (ISO/IEC 15408-2:2022), which has been technically revised.

The main changes are as follows:

- the document has been restructured;
- technical changes have been introduced:
 - the terminology has been reviewed and updated;
 - the dependency and hierarchy for each component have been reviewed and updated;
 - the new notes for operations have been introduced.

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

The catalogue of security functional requirements defined in this document is provided in machine readable format (XML) at: <https://standards.iso.org/iso-iec/TBD>.

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

Legal notice

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

Australia	The Australian Signals Directorate
Canada	Communications Security Establishment
France	Agence Nationale de la Sécurité des Systèmes d'Information
Germany	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Netherlands	Netherlands National Communications Security Agency
New Zealand	Government Communications Security Bureau
Republic of Korea	National Security Research Institute
Spain	Centro Criptológico Nacional
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency and the National Institute of Standards and Technology

Introduction

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

Security functional components allow for the expression of SFRs intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organizational security policies.

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

- consumers, who use this document when selecting components to express functional requirements which satisfy the security objectives expressed in a PP, PP-Module, functional package or ST. ISO/IEC 15408-1 provides more detailed information on the relationship between security objectives and security requirements;
- developers, who respond to actual or perceived consumer security requirements in constructing a TOE, will find a standardized method to understand those requirements in this document. They also use the contents of this document as a basis for further defining the TOE security functionality and mechanisms that conform with those requirements;
- evaluators, who use the SFRs defined in this document in verifying that the TOE functional requirements expressed in the PP, PP-Module, functional package or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators use this document to assist in determining whether a given TOE satisfies stated requirements.

NOTE 1 This document uses bold type to highlight hierarchical relationships between requirements. This convention calls for the use of bold type for all new requirements.

NOTE 2 For security functional requirements, the use of italics denotes assignment and selection items.

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components

1 Scope

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

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

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

3 Terms and definitions

For the purposes of this document, the terms, definitions, and abbreviated terms given in ISO/IEC 15408-1, ISO/IEC 15408-3, ISO/IEC 15408-4, ISO/IEC 15408-5, ISO/IEC 18045 and the following apply.

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

- ISO Online browsing platform: available at www.iso.org/obp;
- IEC Electropedia: available at www.electropedia.org.

3.1

identity

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

Note 1 to entry: Entities can be diverse such as a user, process, or disk. For a human user, the representation can be the full or abbreviated name or a unique pseudonym. An entity can have more than one identity.

EXAMPLE 1

An example of such a representation is a string.

3.2

inter TSF transfer

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

3.3

internal communication channel

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

3.4

internal TOE transfer

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

3.5

operation

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

3.6

secret

information that is known only to authorized users and/or the TOE security functionality (TSF) in order to enforce a specific [security function policy \(3.8\)](#)

3.7

secure state

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

3.8

security function policy

SFP

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

3.9

TOE resource

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

3.10

transfer outside of the TOE

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

3.11

trusted channel

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

3.12

trusted path

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

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

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

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

3.13

TSF data

data for the operation of the target of evaluation (TOE) upon which the enforcement of the security functional requirement (SFR) relies

3.14

user data

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

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

4 Abbreviated terms

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

PP	protection profile
RAM	random access memory
RBG	random bit generator
RNG	random number generator
RPC	remote procedure call
SEMA	simple electromagnetic analysis
SPA	simple power analysis
SFP	security function policy
SFR	security functional requirement
SSH	secure shell
ST	security target
TCP	transmission control protocol
TLS	transport layer security
TOE	target of evaluation
TSF	TOE security functionality
TSFI	TSF interface
USB	universal serial bus
VPN	virtual private network

5 Overview

5.1 General

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

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

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

5.2 Organization of this document

[Clause 6](#) describes the paradigm used in the SFRs of this document.

[Clause 7](#) introduces the catalogue of functional components, followed by their definition, from [Class FAU Security audit \(see Clause 8\)](#) through [Class FTP Trusted path/channels \(see Clause 18\)](#).

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

- ISO/IEC 15408-1, Clause 3 defines the terms and definitions used in the ISO/IEC 15408 series;
- ISO/IEC 15408-1, Clause 7 describes how SFRs can be specified using the security functional components;
- ISO/IEC 15408-1, Clause 8 describes how security functional components are organized, and the operations that may be applied to them;
- ISO/IEC 15408-1, Clause 9 provides further information on the structure for security functional packages;
- ISO/IEC 15408-1, Annex B provides further information on the structure for PPs;
- ISO/IEC 15408-1, Annex C provides further information on the structure of PP-Modules and PP-Configurations;
- ISO/IEC 15408-1, Annex D provides further information on the structure for STs.

6 Functional requirements paradigm

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

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

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

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

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

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

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

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

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

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

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

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

EXAMPLE 1

An example of a TOE device is a workstation.

A period of interaction between users and the TSF is referred to as a user session. Establishment of user sessions can be controlled based on a variety of considerations.

EXAMPLE 2

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

This document uses the term authorized to signify a user who possesses either the rights or privileges, or both that are necessary to perform an operation. The term authorized user, therefore, indicates that it is allowable for a user to perform a specific operation or a set of operations as defined by the SFRs.

To express requirements that call for the separation of administrator duties, the relevant security functional components (from family [Security management roles \(FMT_SMR\)](#) (see 13.10)) explicitly state that administrative roles are required. A role is a pre-defined set of rules establishing the allowed interactions between a user operating in that role and the TOE. A TOE may support the definition of any number of roles.

EXAMPLE 3

Roles related to the secure operation of a TOE may include “Audit Administrator” and “User Accounts Administrator”.

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

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

Active entities in the TOE that perform operations on objects are referred to as subjects.

EXAMPLE 4

Several types of subjects may exist within a TOE:

- those acting on behalf of an authorized user: UNIX processes.

- those acting as a specific functional process that may in turn act on behalf of multiple users: functions as can be found in client/server architectures.
- those acting as part of the TOE itself: processes not acting on behalf of a user.

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

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

EXAMPLE 5

An example of an operation is an inter-process communication.

Objects can contain information. This concept is required to specify information flow control policies as addressed in [Class FDP User data protection \(see Clause 11\)](#).

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

Data in a TOE is categorized as either user data or TSF data. Figure 1 depicts this relationship. User data is information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning. TSF Data is information used by the TSF in making decisions as required by the SFRs. TSF Data may be influenced by users if allowed by the SFRs.

EXAMPLE 6

User data:

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

EXAMPLE 7

TSF data:

- Security attributes, authentication data, TSF internal status variables used by the rules defined in the SFRs or used for the protection of the TSF and access control list entries are examples of TSF data.

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

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

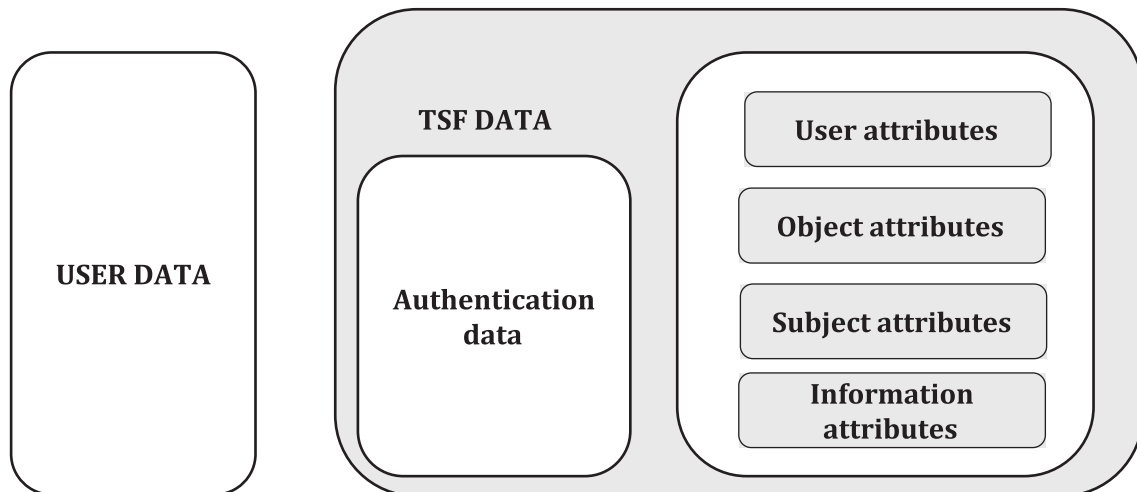


Figure 1 — Relationship between user data and TSF data

Two specific types of TSF data addressed by this document can be, but are not necessarily, the same. These are authentication data and secrets.

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

EXAMPLE 8

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

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

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

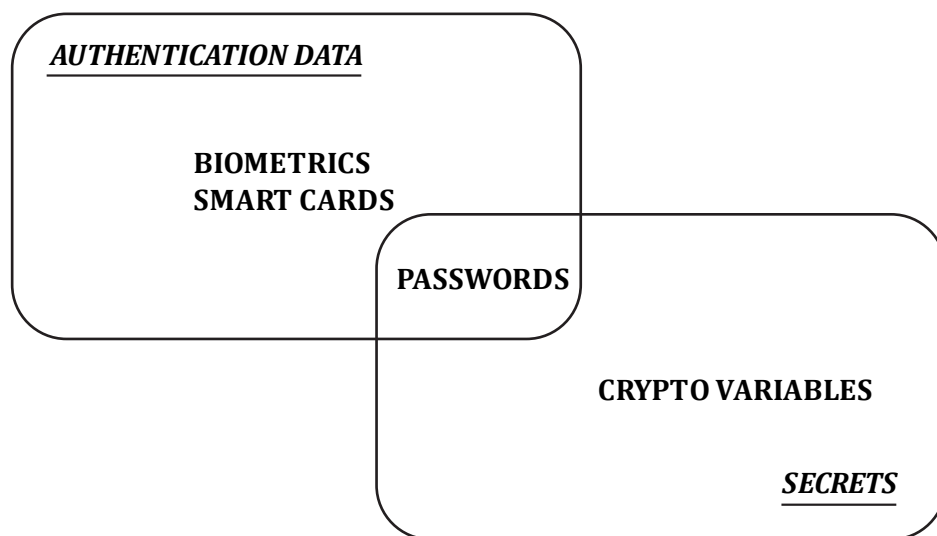


Figure 2 — Relationship between authentication data and secrets

7 Security functional components

7.1 Overview

This clause describes the constructs used in representing the functional classes, families, and components that define the security functional requirements (SFRs) defined in this document.

Note that the most abstract collection of SFRs is referred to as a class. Each class contains functional families, which then contain functional components, which in turn contain functional elements. Classes and families are used to provide a taxonomy for classifying SFRs, while components are used to specify SFRs in a PP, PP-Module, functional package or ST.

7.2 Functional class structure

7.2.1 General

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

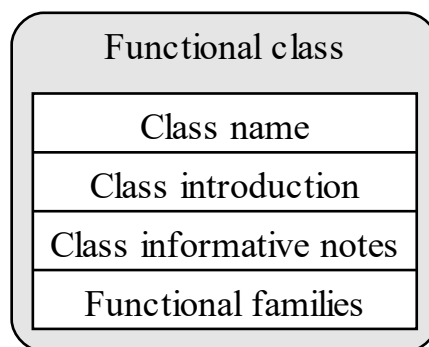


Figure 3 — Functional class structure

7.2.2 Class name

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

7.2.3 Class introduction

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

The class introduction provides a figure describing the families in this class and the hierarchy of the components in each family, as explained in [subclause 7.6](#).

The class introduction includes a class decomposition diagram, showing the families and components of the class. It also provides a dependency table that shows the hierarchical, direct, indirect, and optional dependencies among functional components, as explained in [subclause 7.4.3](#).

7.2.4 Class informative notes

The informative notes contain additional information that supports the interpretation and understanding of the concepts, structure and usage of the functional class.

7.2.5 Functional families

Each functional class contains at least one functional family. The structure of the functional families is described in the following subclause.

7.3 Functional family structure

7.3.1 General

Figure 4 illustrates the functional family structure in diagrammatic form.

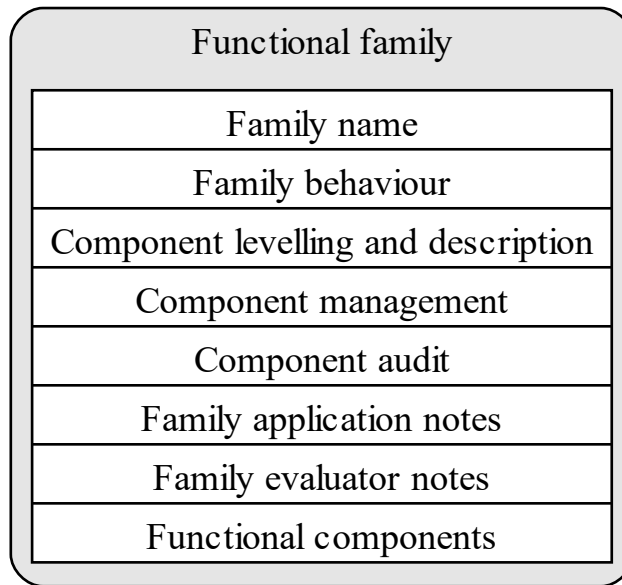


Figure 4 — Functional family structure

7.3.2 Family name

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

7.3.3 Family behaviour

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

- the security objectives of the family address a security problem that may be solved with the help of a TOE that incorporates SFRs derived from a component of this family;
- the description of the functional requirements summarizes all the requirements that are included in the component(s). The description is aimed at authors of STs, PPs, PP-Modules or security functional packages who wish to assess whether the family is relevant to their specific requirements.

7.3.4 Component levelling and description

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

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

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

The relationships between components within a functional family may be hierarchical. A component is hierarchical to another if it offers more security.

As explained in [subclause 7.6](#), the descriptions of the families provide a graphical overview of the hierarchy of the components in a family.

7.3.5 Component management

The management subclauses contain information for ST, PP, PP-Module, or security functional package authors to consider as management activities for a given component. The clauses reference components of [Class FMT Security management \(see Clause 13\)](#) and provide guidance regarding potential management activities that may be applied via operations to those components.

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

7.3.6 Component audit

The audit requirements subclauses contain auditable events for the authors to select, if requirements from [Class FAU Security audit \(see Clause 8\)](#) are included in the ST, PP, PP-Module, or security functional package. These requirements include security relevant events in terms of the various levels of detail supported by the components of the [Security audit data generation \(FAU_GEN\) \(see 8.4\)](#) family.

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

EXAMPLE 1

An audit note can include actions that are:

- Minimal: successful use of the security mechanism;
- Basic: any use of the security mechanism as well as relevant information regarding the security attributes involved;
- Detailed: any configuration changes made to the mechanism, including the actual configuration values before and after the change.

EXAMPLE 2

When Basic Audit Generation is needed, all auditable events identified as being both Minimal and Basic are included in the PP, PP-Module, functional package or ST through the use of the appropriate assignment operation, except when the higher-level event simply provides more detail than the lower level event. When Detailed Audit Generation is needed, all identified auditable events (Minimal, Basic and Detailed) are included in the PP, PP-Module, functional package or ST.

In [Class FAU Security audit \(see Clause 8\)](#) the rules governing the audit are explained in more detail.

7.3.7 Family application notes

The application notes contain additional information that is of interest to potential users of the family, that is PP, PP-Module, ST and functional package authors, and developers of TOEs incorporating the functional components. The presentation is informative and can cover warnings about limitations of use and areas where specific attention can be required when using the components.

NOTE 1 The term PP, PP-Module, functional package or ST author includes authors of documents used to formulate a PP or ST, this includes PP-Modules and functional packages.

7.3.8 Family evaluator notes

The evaluator notes contain any information that is of interest to developers and evaluators of TOEs that claim conformance with a component of the family. The presentation provides information and can cover a variety of areas where specific attention can be needed when evaluating the TOE. This can include clarifications of meaning and specification of the way to interpret requirements, as well as caveats and warnings of specific interest to evaluators.

The family application and evaluator notes are not mandatory and appear only if appropriate.

7.3.9 Functional components

Each functional family has at least one functional component. The structure of the functional components is provided in the following subclause.

7.4 Functional component structure

7.4.1 General

Figure 5 illustrates the functional component structure.

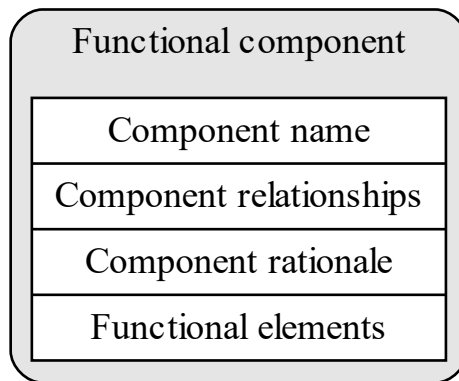


Figure 5 — Functional component structure

7.4.2 Component name

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

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

7.4.3 Component relationships

These subclause(s) define the relationships of each component with the rest of components defined in ISO/IEC 15408-2:

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

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

Each functional component provides a complete list of dependencies to other functional and assurance components. Some components may list “No dependencies”. The components depended upon may in turn have dependencies on other components. The list provided in the components will be the direct dependencies, i.e. only references to the other functional components that are required for this component to perform its job properly. The indirect dependencies, i.e. the dependencies that result from the depended upon components, can be found in the tables included in the functional class introduction. It is noted that in some cases the dependency is optional in that a number of functional components are provided, where each one of them would be sufficient to satisfy the dependency.

Some dependencies are optional and are indicated as such.

EXAMPLE 1

An example of a component with optional dependencies is [FDP_ETC.1, Export of user data without security attributes](#), which requires either [FDP_ACC.1, Subset access control](#) or [FDP_IFC.1, Subset information flow control](#) to be present. So, if [FDP_ACC.1, Subset access control](#) is present, [FDP_IFC.1, Subset information flow control](#) is not necessary and vice versa.

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

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

Where a dependency is given for security assurance requirements, ISO/IEC 15408-3 shall be referred to.

The dependencies of functional components are shown in a table at the class introduction clause, where each of the components that is a dependency of some other functional component is allocated a column. Each functional component is allocated a row. The value in the table cell indicates whether the column label component is a hierarchical requirement (indicated by an “H”), directly required (indicated by a cross “X”), indirectly required (indicated by a dash “-”), or optionally required (indicated by a “O”) by the row label component. Sets of optional requirements are indicated by using an entry of type O^x (e.g. O¹) whereby an SFR with such entry requires at minimum only one of the SFRs contained in that O^x-set.

7.4.4 Component rationale

Any specific information related to the component is found in the component rationale subclause.

The component rationale contains information that refines the general statements on rationale for the specific component level and is used if level-specific amplification is needed.

The component rationale subclause appears only if appropriate.

7.4.5 Functional elements

A set of functional elements is provided for each functional component. An functional element is a security requirement which, if further divided, would not yield a meaningful expression of a functional requirement. It is the smallest security requirement recognized in the ISO/IEC 15408 series.

7.5 Functional elements

Figure 6 illustrates the functional element structure.

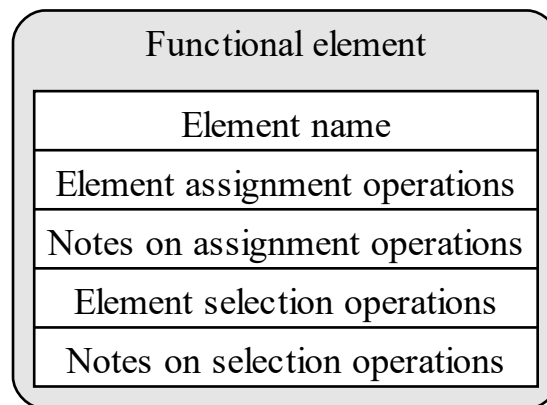


Figure 6 — Functional element structure

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

The content of the functional element may include assignment and/or selection operations. Where considered useful, these have been complemented by notes on the text.

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

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

EXAMPLE 1

The element name **FDP_IFF.4.2** reads as follows:

- F: functional requirement;
- DP: class “User data protection”;
- _IFF: family “Information flow control functions”;
- .4: 4th component named “Partial elimination of illicit information flows”;
- .2: 2nd element of the component.

7.6 Component catalogue

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

This document contains classes of families and components, which are rough groupings on the basis of related function or purpose, presented in alphabetical order. At the start of each class is an informative figure that indicates the taxonomy of each class, indicating the families in each class and the components in each family. Figure 7 is a useful indicator of the hierarchical relationship that can exist between components.

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

In each class, a figure describing the family hierarchy similarly to Figure 7 is provided. In Figure 7, the first family, Family 1, contains three hierarchical components, where component 2 and component 3 can both be used to satisfy dependencies on component 1. Component 3 is hierarchical to component 2 and can also be used to satisfy dependencies on component 2.

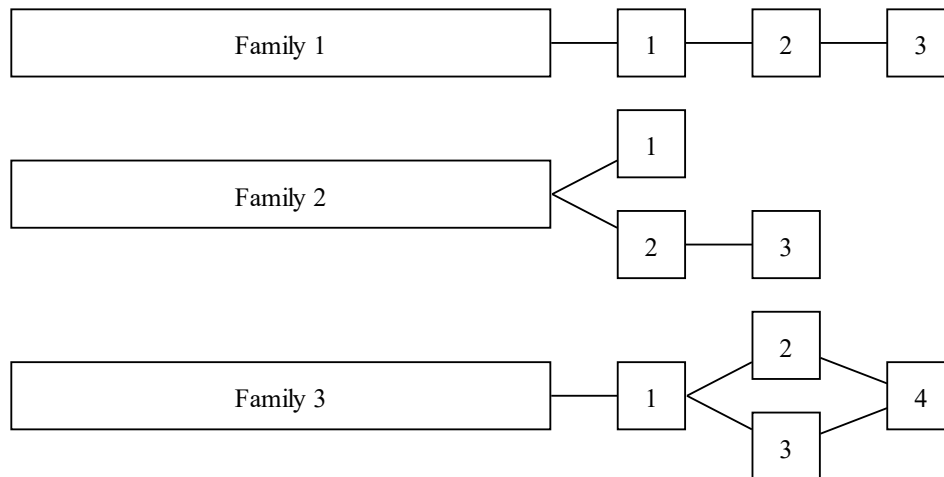


Figure 7 — Sample class decomposition diagram

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

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

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

7.6.1 Highlighting of component changes

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

8 Class FAU Security audit

8.1 Introduction

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

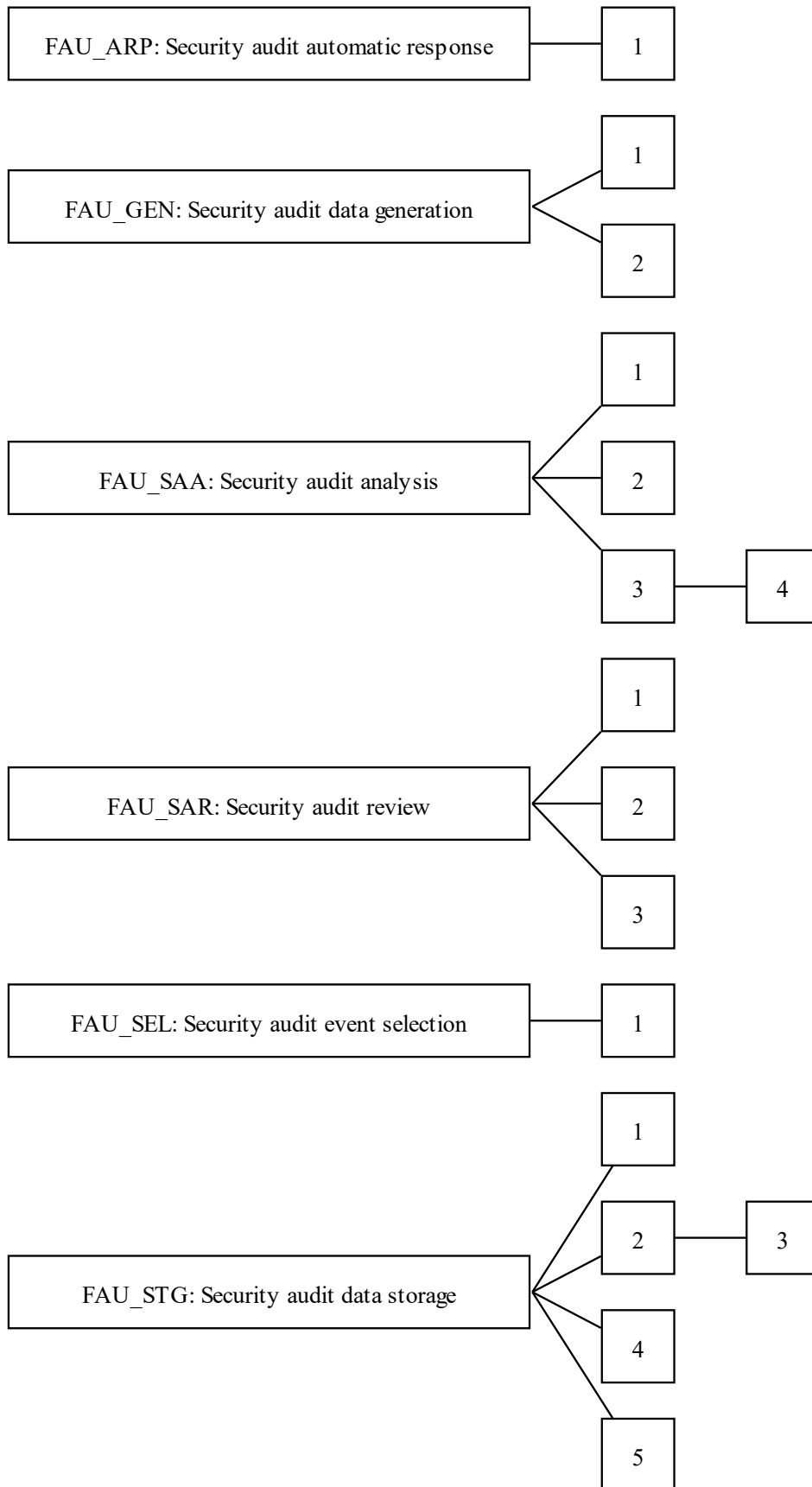


Figure 8 — FAU: Security audit, class decomposition

	FAU_GEN.1	FAU_SAA.1	FAU_SAA.3	FAU_SAR.1	FAU_STG.2	FIA_UID.1	FMT_MTD.1	FPT_STM.1	FTP_ITC.1
FAU_ARP.1	-	X						-	
FAU_GEN.1								X	
FAU_GEN.2	X					X		-	
FAU_SAA.1	X							-	
FAU_SAA.2						X			
FAU_SAA.3									
FAU_SAA.4			H						
FAU_SAR.1	X							-	
FAU_SAR.2	-			X				-	
FAU_SAR.3	-			X				-	
FAU_SEL.1	X						X	-	
FAU_STG.1	X							-	X
FAU_STG.2	X							-	
FAU_STG.3	X				H			-	
FAU_STG.4	-				X			-	
FAU_STG.5	X				X			-	

Table 1 — Dependency table for Class FAU: Security audit

8.2 Notes on class FAU

8.2.1 General information about audit requirements

The audit families allow PP, PP-Module, functional package or ST authors the ability to define requirements for monitoring user activities and, in some cases, detecting real, possible, or imminent violations of the enforcement of the SFRs. The TOE's security audit functions are defined to help monitor security-relevant events, and act as a deterrent against security violations. The requirements of the audit families refer to functions that include audit data protection, record format, and event selection, as well as analysis tools, violation alarms, and real-time analysis. The audit records may be presented in human-readable format either directly or indirectly or both.

EXAMPLE 1

An example of direct presentation is storing the audit records in human-readable format.

EXAMPLE 2

An example of indirect presentation is by using audit reduction tools.

While developing the security audit requirements, the author of a PP, PP-Module, functional package or ST should take note of the inter-relationships among the audit families and components. The potential exists to specify a set of audit requirements that conform with the family/component dependencies lists, while at the same time resulting in a deficient audit function.

EXAMPLE 3

An audit function that requires all security relevant events to be audited but without the selectivity to control them on any reasonable basis such as individual user or object.

8.2.2 Audit requirements in a distributed environment

The implementation of audit requirements for networks and other large systems can differ significantly from those needed for stand-alone systems. Larger, more complex, and active systems require more thought concerning which audit data to collect and how this can be managed, due to the lowered

feasibility of interpreting (or even storing) what gets collected. The traditional notion of a time-ordered list, set of records or “trail” of audited events is not always applicable in a global asynchronous network with many arbitrary events occurring at once.

Also, different hosts and servers on a distributed TOE can have differing naming policies and values. Further, the use of symbolic names for audit review requires a net-wide convention to avoid redundancies and “name clashes”.

A multi-object audit repository, portions of which are accessible by a potentially wide variety of authorized users, are usually required if audit repositories are to serve a useful function in distributed systems.

Finally, misuse of authority by authorized users can be addressed by systematically avoiding local storage of audit data pertaining to administrator actions.

8.3 Security audit automatic response (FAU_ARP)

8.3.1 Family Behaviour

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

8.3.2 Component levelling and description

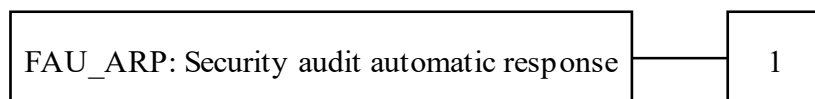


Figure 9 — FAU_ARP: Component levelling

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

8.3.3 Management of [FAU_ARP.1](#)

The following actions could be considered for the management functions in [Class FMT Security management \(see Clause 13\)](#):

- The management (addition, removal, or modification) of actions.

8.3.4 Audit of [FAU_ARP.1](#)

The following actions should be auditable if [Security audit data generation \(FAU_GEN\) \(see 8.4\)](#) is included in the PP, PP-Module, functional package or ST:

- Minimal: Actions taken due to potential security violations.

8.3.5 Application notes

The security audit automatic response family describes requirements for the handling of audit events. The requirement can include requirements for alarms or TSF action (automatic response).

EXAMPLE 1

The TSF can include the generation of real time alarms, termination of the offending process, disabling of a service, or disconnection or invalidation of a user account.

An audit event is defined to be an “potential security violation” when indicated by the [Security audit analysis \(FAU_SAA\) \(see 8.5\)](#) components.

8.3.6 FAU_ARP.1 Security alarms

8.3.6.1 Component relationships

Hierarchical to: No other components.

Dependencies: [FAU_SAA.1, Potential violation analysis](#)

8.3.6.2 Component rationale

One or more actions should be taken for follow up action in the event of an alarm.

These actions can include informing the authorized user of the alarm, presenting the authorized user with a set of possible containment actions, or options for the authorized user to take corrective actions.

The timing of the actions should be carefully considered by the PP, PP-Module, functional package or ST author.

8.3.6.3 Element FAU_ARP.1.1

The TSF shall take [assignment ^(a1): *list of actions*] upon detection of a potential security violation.

NOTE 1 In [FAU_ARP.1.1](#) (a1), the author of a PP, PP-Module, functional package or ST specifies the actions to be taken in case of a potential security violation.

8.4 Security audit data generation (FAU_GEN)

8.4.1 Family Behaviour

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

8.4.2 Component levelling and description

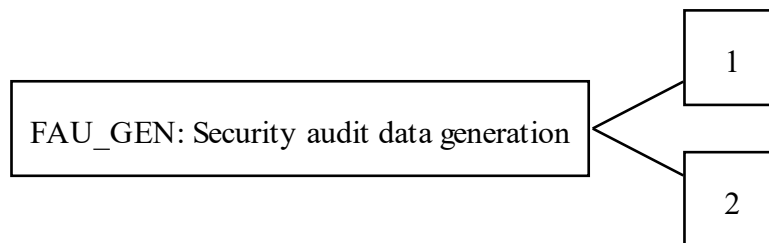


Figure 10 — FAU_GEN: Component levelling

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

In [FAU_GEN.2, User identity association](#), the TSF shall associate auditable events to individual user identities.

8.4.3 Management of [FAU_GEN.1](#), [FAU_GEN.2](#)

The following actions could be considered for the management functions in [Class FMT Security management](#) (see [Clause 13](#)):

- There are no management activities foreseen.

8.4.4 Audit of [FAU_GEN.1](#), [FAU_GEN.2](#)

The following actions should be auditable if [Security audit data generation \(FAU_GEN\)](#) (see [8.4](#)) is included in the PP, PP-Module, functional package or ST:

- There are no auditable events foreseen.

8.4.5 Application notes

The security audit data generation family includes requirements to specify the audit events that shall be generated by the TSF for security-relevant events.

This family is presented in a manner that avoids a dependency on all components requiring audit support. Each component has an audit subclause developed in which the events to be audited for that functional area are listed. When the PP, PP-Module, functional package or ST is written, the items in the audit area are used to complete the variable in these components. Thus, the specification of what can be audited for a functional area is localized in that functional area.

The list of auditable events is entirely dependent on the other functional families within the PP, PP-Module, functional package or ST. Each family definition should therefore include a list of its family-specific auditable events. Each auditable event in the list of auditable events specified in the functional family should correspond to one of the levels of audit event generation specified in this family (i.e. minimal, basic, detailed). This provides the author of a PP, PP-Module, functional package or ST with the information necessary to ensure that all appropriate auditable events are specified in the PP, PP-Module, functional package or ST. The following example shows how auditable events are to be specified in appropriate functional families:

EXAMPLE 1

The following actions should be auditable if [Security audit data generation \(FAU_GEN\) \(see 8.4\)](#) is included in the PP, PP-Module, functional package or ST:

- Minimal: Successful use of the user security attribute administration functions;
- Basic: All attempted uses of the user security attribute administration functions;
- Basic: Identification of which user security attributes have been modified;
- Detailed: With the exception of specific sensitive attribute data items, the new values of the attributes should be captured.

NOTE 1 Sensitive attribute data items include passwords and cryptographic keys.

For each functional component that is chosen, the auditable events that are indicated in that component, at and below the level indicated in [Security audit data generation \(FAU_GEN\) \(see 8.4\)](#) should be auditable. So, in the previous example “Basic” would be selected in [Security audit data generation \(FAU_GEN\) \(see 8.4\)](#), the auditable events mentioned in a), b) and c) should be auditable.

Observe that the categorization of auditable events (minimal, basic, detailed) is hierarchical in that order.

This means that:

- when minimal audit generation is desired, all auditable events identified as being minimal should be included in the PP, PP-Module, functional package or ST through the use of the appropriate assignment operation;
- when basic audit generation is desired, all auditable events identified as being either minimal or basic, should also be included in the PP, PP-Module, functional package or ST through the use of the appropriate assignment operation, except when the higher-level event simply provides more detail than the lower level event;
- when detailed audit generation is desired, all identified auditable events (minimal, basic, and detailed) should be included in the PP, PP-Module, functional package or ST.

A PP, PP-Module, functional package or ST author may decide to include other auditable events beyond those required for a given audit level.

EXAMPLE 2

The PP, PP-Module, functional package or ST may claim only minimal audit capabilities while including most of the basic capabilities because the few excluded capabilities conflict with other PP, PP-Module, functional package or ST constraints (perhaps because they require the collection of unavailable data).

The functionality that creates the auditable event should be specified in the PP, PP-Module, functional package or ST as a functional requirement.

EXAMPLE 3

The following are examples of the types of the events that can be defined as auditable within each PP, PP-Module, functional package or ST functional component:

- introduction of objects within the control of the TSF into a subject's address space;
- deletion of objects;
- distribution or revocation of access rights or capabilities;
- changes to subject or object security attributes;
- policy checks performed by the TSF as a result of a request by a subject;
- the use of access rights to bypass a policy check;
- use of Identification and Authentication functions;
- actions taken by an operator, and/or authorized user (such as suppression of a TSF protection mechanism as human-readable labels);
- import/export of data from/to removable media (such as printed output, tapes, USB sticks).

8.4.6 Evaluator notes

[FAU_GEN.1, Audit data generation](#) has a dependency on [FPT_STM.1, Reliable time stamps](#). If correctness of time is not an issue for this TOE, elimination of this dependency can be justified by the author of a PP, PP-Module, functional package or ST.

8.4.7 FAU_GEN.1 Audit data generation

8.4.7.1 Component relationships

Hierarchical to: No other components.

Dependencies: [FPT_STM.1, Reliable time stamps](#)

8.4.7.2 Component rationale

This component defines requirements to identify the auditable events for which audit records should be generated, and the information to be provided in the audit records.

[FAU_GEN.1, Audit data generation](#) by itself can be used when the SFRs do not require that individual user identities be associated with audit events. This can be appropriate when the PP, PP-Module, functional package or ST also contains privacy requirements. If the user identity needs to be incorporated [FAU_GEN.2, User identity association](#) can be used in addition to [FAU_GEN.1, Audit data generation](#).

If the subject is a user, the user identity may be recorded as the subject identity. The identity of the user may not yet have been verified if [User authentication \(FIA_UAU\)](#) (see 12.7) has not been applied. Therefore, in the instance of an invalid login the claimed user identity should be recorded. It should also be considered whether to indicate when a recorded identity has not been authenticated.

8.4.7.3 Element FAU_GEN.1.1

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

- **Start-up and shutdown of the audit functions;**
- **All auditable events for the [selection, choose one of ^(s1): *minimum, basic, detailed, not specified*] level of audit;**
- **[assignment ^(a1): *other specifically defined auditable events*].**

NOTE 1 In [FAU_GEN.1.1](#) (s1), the author of a PP, PP-Module, functional package or ST should select the level of auditable events called out in the audit subclause of other functional components included in the PP, PP-Module, functional package or ST. This level is one of the following: “minimum”, “basic”, “detailed” or “not specified”.

NOTE 2 In [FAU_GEN.1.1](#) (a1), the author of a PP, PP-Module, functional package or ST should select the level of auditable events called out in the audit subclause of other functional components included in the PP, PP-Module, functional package or ST. This level is one of the following: “minimum”, “basic”, “detailed” or “not specified”.

8.4.7.4 Element FAU_GEN.1.2

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

- **Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;**
- **For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [assignment ^(a1): *other audit relevant information*].**

NOTE 1 In [FAU_GEN.1.2](#) (a1), the author of a PP, PP-Module, functional package or ST should assign, for each of the auditable events included in the PP, PP-Module, functional package or ST, either a list of other audit relevant information to be included in audit events records or none.

8.4.8 FAU_GEN.2 User identity association

8.4.8.1 Component relationships

Hierarchical to: No other components.

Dependencies: [FAU_GEN.1, Audit data generation](#)
[FIA_UID.1, Timing of identification](#)

8.4.8.2 Component rationale

This component addresses the requirement of accountability of auditable events at the level of individual user identity. This component should be used in addition to [FAU_GEN.1, Audit data generation](#).

There is a potential conflict between the audit and privacy requirements. For audit purposes, it can be desirable to know who performed an action. It is possible that a user wants to keep his/her actions to himself/herself and not be identified by other persons such as a site with job offers. Alternatively, it can be required in the Organizational Security Policy that the identity of the users must be protected. In those cases, the objectives for audit and privacy can contradict each other. Therefore, if this requirement is selected and privacy is important, inclusion of the component user pseudonymity should be considered. Requirements on determining the real user name based on its pseudonym are specified in the privacy class.

If the identity of the user has not yet been verified through authentication, in the instance of an invalid login the claimed user identity should be recorded. It should be considered to indicate when a recorded identity has not been authenticated.

8.4.8.3 Element FAU_GEN.2.1

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

8.5 Security audit analysis (FAU_SAA)

8.5.1 Family Behaviour

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

The actions to be taken based on the detection can be specified using the [Security audit automatic response \(FAU_ARP\)](#) (see 8.3) family as desired.

8.5.2 Component levelling and description

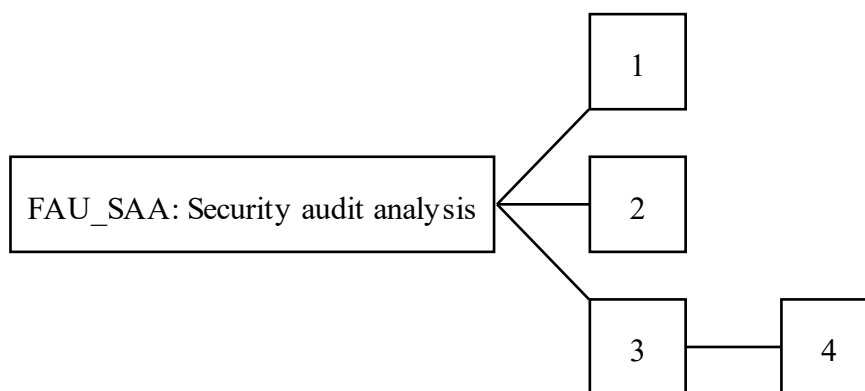


Figure 11 — FAU_SAA: Component levelling

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

In [FAU_SAA.2, Profile based anomaly detection](#), the TSF maintains individual profiles of system usage, where a profile represents the historical patterns of usage performed by members of the profile target group. A profile target group refers to a group of one or more individuals who interact with the TSF. Each member of a profile target group is assigned an individual suspicion rating that represents how well that member's current activity corresponds to the established patterns of usage represented in the profile. This analysis can be performed at runtime or during a post-collection batch-mode analysis.

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

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

8.5.3 Management of [FAU_SAA.1](#)

The following actions could be considered for the management functions in [Class FMT Security management](#) (see Clause 13):

- Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.

8.5.4 Management of FAU_SAA.2

The following actions could be considered for the management functions in [Class FMT Security management \(see Clause 13\)](#):

- Maintenance (deletion, modification, addition) of the group of users in the profile target group.

8.5.5 Management of FAU_SAA.3

The following actions could be considered for the management functions in [Class FMT Security management \(see Clause 13\)](#):

- Maintenance (deletion, modification, addition) of the subset of system events.

8.5.6 Management of FAU_SAA.4

The following actions could be considered for the management functions in [Class FMT Security management \(see Clause 13\)](#):

- Maintenance (deletion, modification, addition) of the subset of system events;
- Maintenance (deletion, modification, addition) of the set of sequences of system events.

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

The following actions should be auditable if [Security audit data generation \(FAU_GEN\) \(see 8.4\)](#) is included in the PP, PP-Module, functional package or ST:

- Minimal: Enabling and disabling of any of the analysis mechanisms;
- Minimal: Automated responses performed by the tool.

8.5.8 Application notes

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

The action to be performed by the TSF on detection of a potential violation is defined in [Security audit automatic response \(FAU_ARP\) \(see 8.3\)](#) components.

For real-time analysis, audit data can be transformed into a useful format for automated treatment, but into a different useful format for delivery to authorized users for review.

8.5.9 FAU_SAA.1 Potential violation analysis**8.5.9.1 Component relationships**

Hierarchical to: No other components.

Dependencies: [FAU_GEN.1, Audit data generation](#)

8.5.9.2 Component rationale

This component is used to specify the set of auditable events whose occurrence or accumulated occurrence held to indicate a potential violation of the enforcement of the SFRs, and any rules to be used to perform the violation analysis.

8.5.9.3 Element FAU_SAA.1.1

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

8.5.9.4 Element FAU_SAA.1.2

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