



SLOVENSKI STANDARD SIST EN ISO/IEC 15408-2:2024

01-maj-2024

Nadomešča:

SIST EN ISO/IEC 15408-2:2020

Informacijska varnost, kibernetika varnost in varstvo zasebnosti - Merila za vrednotenje varnosti IT - 2. del: Funkcionalne varnostne komponente (ISO/IEC 15408-2:2022)

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components (ISO/IEC 15408-2:2022)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Evaluationskriterien für IT-Sicherheit - Teil 2: Sicherheit funktionale Komponenten (ISO/IEC 15408-2:2022)

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 (ISO/IEC 15408-2:2022)

Ta slovenski standard je istoveten z: EN ISO/IEC 15408-2:2023

ICS:

35.030	Informacijska varnost	IT Security
--------	-----------------------	-------------

SIST EN ISO/IEC 15408-2:2024	en,fr,de
-------------------------------------	-----------------

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 15408-2

December 2023

ICS 35.030

Supersedes EN ISO/IEC 15408-2:2020

English version

Information security, cybersecurity and privacy protection
- Evaluation criteria for IT security - Part 2: Security
functional components (ISO/IEC 15408-2:2022)

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 (ISO/IEC 15408-
2:2022)

Informationssicherheit, Cybersicherheit und Schutz
der Privatsphäre - Evaluationskriterien für IT-
Sicherheit - Teil 2: Sicherheit funktionale
Komponenten (ISO/IEC 15408-2:2022)

This European Standard was approved by CEN on 20 November 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

EN ISO/IEC 15408-2:2023 (E)

Contents	Page
European foreword.....	3

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[SIST EN ISO/IEC 15408-2:2024](https://standards.iteh.ai/catalog/standards/sist/4757cf07-870a-44a5-a8d9-8d36022f4859/sist-en-iso-iec-15408-2-2024)

<https://standards.iteh.ai/catalog/standards/sist/4757cf07-870a-44a5-a8d9-8d36022f4859/sist-en-iso-iec-15408-2-2024>

European foreword

The text of ISO/IEC 15408-2:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 15408-2:2023 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2024, and conflicting national standards shall be withdrawn at the latest by June 2024.

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

This document supersedes EN ISO/IEC 15408-2:2020.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 15408-2:2022 has been approved by CEN-CENELEC as EN ISO/IEC 15408-2:2023 without any modification.

INTERNATIONAL STANDARD

**ISO/IEC
15408-2**

Fourth edition
2022-08

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

Part 2: Security functional components

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

Partie 2: Composants fonctionnels de sécurité

SIST EN ISO/IEC 15408-2:2024

<https://standards.iteh.ai/catalog/standards/sist/4757cf07-870a-44a5-a8d9-8d36022f4859/sist-en-iso-iec-15408-2-2024>



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

© ISO/IEC 2022

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

SIST EN ISO/IEC 15408-2:2024

<https://standards.iteh.ai/catalog/standards/sist/4757cf07-870a-44a5-a8d9-8d36022f4859/sist-en-iso-iec-15408-2-2024>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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

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

Published in Switzerland

Contents

Page

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

ISO/IEC 15408-2:2022(E)

8.5.7	Audit of FAU_SAR.3	21
8.5.8	FAU_SAR.1 Audit review	21
8.5.9	FAU_SAR.2 Restricted audit review	21
8.5.10	FAU_SAR.3 Selectable audit review	21
8.6	Security audit event selection (FAU_SEL)	22
8.6.1	Family behaviour	22
8.6.2	Components leveling and description	22
8.6.3	Management of FAU_SEL.1	22
8.6.4	Audit of FAU_SEL.1	22
8.6.5	FAU_SEL.1 Selective audit	22
8.7	Security audit data storage (FAU_STG)	22
8.7.1	Family behaviour	22
8.7.2	Components leveling and description	23
8.7.3	Management of FAU_STG.1	23
8.7.4	Management of FAU_STG.2	23
8.7.5	Management of FAU_STG.3	23
8.7.6	Management of FAU_STG.4	23
8.7.7	Management of FAU_STG.5	23
8.7.8	Audit of FAU_STG.1	24
8.7.9	Audit of FAU_STG.2, FAU_STG.3	24
8.7.10	Audit of FAU_STG.4	24
8.7.11	Audit of FAU_STG.5	24
8.7.12	FAU_STG.1 Audit data storage location	24
8.7.13	FAU_STG.2 Protected audit data storage	24
8.7.14	FAU_STG.3 Guarantees of audit data availability	25
8.7.15	FAU_STG.4 Action in case of possible audit data loss	25
8.7.16	FAU_STG.5 Prevention of audit data loss	25
9	Class FCO: Communication	25
9.1	Class description	25
9.2	Non-repudiation of origin (FCO_NRO)	26
9.2.1	Family behaviour	26
9.2.2	Components leveling and description	26
9.2.3	Management of FCO_NRO.1, FCO_NRO.2	26
9.2.4	Audit of FCO_NRO.1	26
9.2.5	Audit of FCO_NRO.2	27
9.2.6	FCO_NRO.1 Selective proof of origin	27
9.2.7	FCO_NRO.2 Enforced proof of origin	27
9.3	Non-repudiation of receipt (FCO_NRR)	28
9.3.1	Family behaviour	28
9.3.2	Components leveling and description	28
9.3.3	Management of FCO_NRR.1, FCO_NRR.2	28
9.3.4	Audit of FCO_NRR.1	28
9.3.5	Audit of FCO_NRR.2	28
9.3.6	FCO_NRR.1 Selective proof of receipt	29
9.3.7	FCO_NRR.2 Enforced proof of receipt	29
10	Class FCS: Cryptographic support	29
10.1	Class description	29
10.2	Cryptographic key management (FCS_CKM)	30
10.2.1	Family behaviour	30
10.2.2	Components leveling and description	30
10.2.3	Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6	31
10.2.4	Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.5, CKM.6	31
10.2.5	FCS_CKM.1 Cryptographic key generation	31
10.2.6	FCS_CKM.2 Cryptographic key distribution	32
10.2.7	FCS_CKM.3 Cryptographic key access	32
10.2.8	FCS_CKM.4 Cryptographic key destruction	32
10.2.9	FCS_CKM.5 Cryptographic key derivation	33

10.2.10	FCS_CKM.6 Timing and event of cryptographic key destruction	33
10.3	Cryptographic operation (FCS_COP)	33
10.3.1	Family behaviour	33
10.3.2	Components leveling and description	33
10.3.3	Management of FCS_COP.1	34
10.3.4	Audit of FCS_COP.1	34
10.3.5	FCS_COP.1 Cryptographic operation	34
10.4	Random bit generation (FCS_RBG)	34
10.4.1	Family behaviour	34
10.4.2	Components leveling and description	34
10.4.3	Management of FCS_RBG.1, FCS_RBG.2, FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6	35
10.4.4	Audit of FCS_RBG.1, FCS_RBG.2	35
10.4.5	Audit of FCS_RBG.3, FCS_RBG.4, FCS_RBG.5, FCS_RBG.6	35
10.4.6	FCS_RBG.1 Random bit generation (RBG)	35
10.4.7	FCS_RBG.2 Random bit generation (external seeding)	36
10.4.8	FCS_RBG.3 Random bit generation (internal seeding – single source)	36
10.4.9	FCS_RBG.4 Random bit generation (internal seeding – multiple sources)	37
10.4.10	FCS_RBG.5 Random bit generation (combining noise sources)	37
10.4.11	FCS_RBG.6 Random bit generation service	37
10.5	Generation of random numbers (FCS_RNG)	37
10.5.1	Family behaviour	37
10.5.2	Components leveling and description	38
10.5.3	Management of FCS_RNG.1	38
10.5.4	Audit of FCS_RNG.1	38
10.5.5	FCS_RNG.1 Random number generation	38
11	Class FDP: User data protection	38
11.1	Class description	38
11.2	Access control policy (FDP_ACC)	40
11.2.1	Family behaviour	40
11.2.2	Components leveling and description	41
11.2.3	Management of FDP_ACC.1, FDP_ACC.2	41
11.2.4	Audit of FDP_ACC.1, FDP_ACC.2	41
11.2.5	FDP_ACC.1 Subset access control	41
11.2.6	FDP_ACC.2 Complete access control	41
11.3	Access control functions (FDP_ACF)	42
11.3.1	Family behaviour	42
11.3.2	Components leveling and description	42
11.3.3	Management of FDP_ACF.1	42
11.3.4	Audit of FDP_ACF.1	42
11.3.5	FDP_ACF.1 Security attribute-based access control	42
11.4	Data authentication (FDP_DAU)	43
11.4.1	Family behaviour	43
11.4.2	Components leveling and description	43
11.4.3	Management of FDP_DAU.1, FDP_DAU.2	43
11.4.4	Audit of FDP_DAU.1	43
11.4.5	Audit of FDP_DAU.2	44
11.4.6	FDP_DAU.1 Basic Data Authentication	44
11.4.7	FDP_DAU.2 Data Authentication with Identity of Guarantor	44
11.5	Export from the TOE (FDP_ETC)	44
11.5.1	Family behaviour	44
11.5.2	Components leveling and description	45
11.5.3	Management of FDP_ETC.1	45
11.5.4	Management of FDP_ETC.2	45
11.5.5	Audit of FDP_ETC.1, FDP_ETC.2	45
11.5.6	FDP_ETC.1 Export of user data without security attributes	45
11.5.7	FDP_ETC.2 Export of user data with security attributes	45
11.6	Information flow control policy (FDP_IFC)	46

ISO/IEC 15408-2:2022(E)

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

11.12.6	FDP_ROL.2 Advanced rollback	60
11.13	Stored data confidentiality (FDP_SDC)	60
11.13.1	Family behaviour	60
11.13.2	Components leveling and description	60
11.13.3	Management of FDP_SDC.1, FDP_SDC.2	60
11.13.4	Audit of FDP_SDC.1, FDP_SDC.2	61
11.13.5	FDP_SDC.1 Stored data confidentiality	61
11.13.6	FDP_SDC.2 Stored data confidentiality with dedicated method	61
11.14	Stored data integrity (FDP_SDI)	61
11.14.1	Family behaviour	61
11.14.2	Components leveling and description	61
11.14.3	Management of FDP_SDI.1	62
11.14.4	Management of FDP_SDI.2	62
11.14.5	Audit of FDP_SDI.1	62
11.14.6	Audit of FDP_SDI.2	62
11.14.7	FDP_SDI.1 Stored data integrity monitoring	62
11.14.8	FDP_SDI.2 Stored data integrity monitoring and action	62
11.15	Inter-TSF user data confidentiality transfer protection (FDP_UCT)	63
11.15.1	Family behaviour	63
11.15.2	Components leveling and description	63
11.15.3	Management of FDP_UCT.1	63
11.15.4	Audit of FDP_UCT.1	63
11.15.5	FDP_UCT.1 Basic data exchange confidentiality	63
11.16	Inter-TSF user data integrity transfer protection (FDP_UIT)	64
11.16.1	Family behaviour	64
11.16.2	Components leveling and description	64
11.16.3	Management of FDP_UIT.1, FDP_UIT.2, FDP_UIT.3	64
11.16.4	Audit of FDP_UIT.1	64
11.16.5	Audit of FDP_UIT.2, FDP_UIT.3	65
11.16.6	FDP_UIT.1 Data exchange integrity	65
11.16.7	FDP_UIT.2 Source data exchange recovery	65
11.16.8	FDP_UIT.3 Destination data exchange recovery	66
12	Class FIA: Identification and authentication	66
12.1	Class description	66
12.2	Authentication failures (FIA_AFL)	67
12.2.1	Family behaviour	67
12.2.2	Components leveling and description	67
12.2.3	Management of FIA_AFL.1	68
12.2.4	Audit of FIA_AFL.1	68
12.2.5	FIA_AFL.1 Authentication failure handling	68
12.3	Authentication proof of identity (FIA_API)	68
12.3.1	Family behaviour	68
12.3.2	Components leveling and description	68
12.3.3	Management of FIA_API.1	68
12.3.4	Audit of FIA_API.1	69
12.3.5	FIA_API.1 Authentication proof of identity	69
12.4	User attribute definition (FIA_ATD)	69
12.4.1	Family behaviour	69
12.4.2	Components leveling and description	69
12.4.3	Management of FIA_ATD.1	69
12.4.4	Audit of FIA_ATD.1	69
12.4.5	FIA_ATD.1 User attribute definition	69
12.5	Specification of secrets (FIA_SOS)	70
12.5.1	Family behaviour	70
12.5.2	Components leveling and description	70
12.5.3	Management of FIA_SOS.1	70
12.5.4	Management of FIA_SOS.2	70
12.5.5	Audit of FIA_SOS.1, FIA_SOS.2	70

ISO/IEC 15408-2:2022(E)

12.5.6	FIA_SOS.1 Verification of secrets	70
12.5.7	FIA_SOS.2 TSF Generation of secrets	71
12.6	User authentication (FIA_UAU)	71
12.6.1	Family behaviour	71
12.6.2	Components leveling and description	71
12.6.3	Management of FIA_UAU.1	72
12.6.4	Management of FIA_UAU.2	72
12.6.5	Management of FIA_UAU.3, FIA_UAU.4, FIA_UAU.7	72
12.6.6	Management of FIA_UAU.5	72
12.6.7	Management of FIA_UAU.6	72
12.6.8	Management of FIA_UAU.7	72
12.6.9	Audit of FIA_UAU.1	72
12.6.10	Audit of FIA_UAU.2	73
12.6.11	Audit of FIA_UAU.3	73
12.6.12	Audit of FIA_UAU.4	73
12.6.13	Audit of FIA_UAU.5	73
12.6.14	Audit of FIA_UAU.6	73
12.6.15	Audit of FIA_UAU.7	73
12.6.16	FIA_UAU.1 Timing of authentication	73
12.6.17	FIA_UAU.2 User authentication before any action	74
12.6.18	FIA_UAU.3 Unforgeable authentication	74
12.6.19	FIA_UAU.4 Single-use authentication mechanisms	74
12.6.20	FIA_UAU.5 Multiple authentication mechanisms	74
12.6.21	FIA_UAU.6 Re-authenticating	75
12.6.22	FIA_UAU.7 Protected authentication feedback	75
12.7	User identification (FIA_UID)	75
12.7.1	Family behaviour	75
12.7.2	Components leveling and description	75
12.7.3	Management of FIA_UID.1	76
12.7.4	Management of FIA_UID.2	76
12.7.5	Audit of FIA_UID.1, FIA_UID.2	76
12.7.6	FIA_UID.1 Timing of identification	76
12.7.7	FIA_UID.2 User identification before any action	76
12.8	User-subject binding (FIA_USB)	77
12.8.1	Family behaviour	77
12.8.2	Components leveling and description	77
12.8.3	Management of FIA_USB.1	77
12.8.4	Audit of FIA_USB.1	77
12.8.5	FIA_USB.1 User-subject binding	77
13	Class FMT: Security management	78
13.1	Class description	78
13.2	Limited capabilities and availability (FMT_LIM)	79
13.2.1	Family behaviour	79
13.2.2	Components leveling and description	79
13.2.3	Management of FMT_LIM.1, FMT_LIM.2	80
13.2.4	Audit of FMT_LIM.1	80
13.2.5	FMT_LIM.1 Limited capabilities	80
13.2.6	FMT_LIM.2 Limited availability	80
13.3	Management of functions in TSF (FMT_MOF)	80
13.3.1	Family behaviour	80
13.3.2	Components leveling and description	80
13.3.3	Management of FMT_MOF.1	81
13.3.4	Audit of FMT_MOF.1	81
13.3.5	FMT_MOF.1 Management of security functions behaviour	81
13.4	Management of security attributes (FMT_MSA)	81
13.4.1	Family behaviour	81
13.4.2	Components leveling and description	81
13.4.3	Management of FMT_MSA.1	82