

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

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 15408-2:2023 sisaldab Euroopa standardi EN ISO/IEC 15408-2:2023 ingliskeelset teksti. Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas. Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 06.12.2023. Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	This Estonian standard EVS-EN ISO/IEC 15408-2:2023 consists of the English text of the European standard EN ISO/IEC 15408-2:2023. This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation. Date of Availability of the European standard is 06.12.2023. The standard is available from the Estonian Centre for Standardisation and Accreditation.
---	---

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele. Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis-ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardimis-ja Akrediteerimiskeskusega: Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation and Accreditation. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation and Accreditation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation and Accreditation: Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

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

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.

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

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

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

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

13.4.4	Management of FMT_MSA.2	82
13.4.5	Management of FMT_MSA.3	82
13.4.6	Management of FMT_MSA.4	82
13.4.7	Audit of FMT_MSA.1	82
13.4.8	Audit of FMT_MSA.2	82
13.4.9	Audit of FMT_MSA.3	82
13.4.10	Audit of FMT_MSA.4	83
13.4.11	FMT_MSA.1 Management of security attributes	83
13.4.12	FMT_MSA.2 Secure security attributes	83
13.4.13	FMT_MSA.3 Static attribute initialization	83
13.4.14	FMT_MSA.4 Security attribute value inheritance	84
13.5	Management of TSF data (FMT_MTD)	84
13.5.1	Family behaviour	84
13.5.2	Components leveling and description	84
13.5.3	Management of FMT_MTD.1	84
13.5.4	Management of FMT_MTD.2	84
13.5.5	Management of FMT_MTD.3	85
13.5.6	Audit of FMT_MTD.1	85
13.5.7	Audit of FMT_MTD.2	85
13.5.8	Audit of FMT_MTD.3	85
13.5.9	FMT_MTD.1 Management of TSF data	85
13.5.10	FMT_MTD.2 Management of limits on TSF data	85
13.5.11	FMT_MTD.3 Secure TSF data	86
13.6	Revocation (FMT_REV)	86
13.6.1	Family behaviour	86
13.6.2	Components leveling and description	86
13.6.3	Management of FMT_REV.1	86
13.6.4	Audit of FMT_REV.1	86
13.6.5	FMT_REV.1 Revocation	86
13.7	Security attribute expiration (FMT_SAE)	87
13.7.1	Family behaviour	87
13.7.2	Components leveling and description	87
13.7.3	Management of FMT_SAE.1	87
13.7.4	Audit of FMT_SAE.1	87
13.7.5	FMT_SAE.1 Time-limited authorization	87
13.8	Specification of Management Functions (FMT_SMF)	88
13.8.1	Family behaviour	88
13.8.2	Components leveling and description	88
13.8.3	Management of FMT_SMF.1	88
13.8.4	Audit of FMT_SMF.1	88
13.8.5	FMT_SMF.1 Specification of Management Functions	88
13.9	Security management roles (FMT_SMR)	89
13.9.1	Family behaviour	89
13.9.2	Components leveling and description	89
13.9.3	Management of FMT_SMR.1	89
13.9.4	Management of FMT_SMR.2	89
13.9.5	Management of FMT_SMR.3	89
13.9.6	Audit of FMT_SMR.1	89
13.9.7	Audit of FMT_SMR.2	89
13.9.8	Audit of FMT_SMR.3	90
13.9.9	FMT_SMR.1 Security roles	90
13.9.10	FMT_SMR.2 Restrictions on security roles	90
13.9.11	FMT_SMR.3 Assuming roles	90
14	Class FPR: Privacy	91
14.1	Class description	91
14.2	Anonymity (FPR_ANO)	91
14.2.1	Family behaviour	91
14.2.2	Components leveling and description	91

14.2.3	Management of FPR_ANO.1, FPR_ANO.2	92
14.2.4	Audit of FPR_ANO.1, FPR_ANO.2	92
14.2.5	FPR_ANO.1 Anonymity	92
14.2.6	FPR_ANO.2 Anonymity without soliciting information	92
14.3	Pseudonymity (FPR_PSE)	92
14.3.1	Family behaviour	92
14.3.2	Components leveling and description	92
14.3.3	Management of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3	93
14.3.4	Audit of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3	93
14.3.5	FPR_PSE.1 Pseudonymity	93
14.3.6	FPR_PSE.2 Reversible pseudonymity	93
14.3.7	FPR_PSE.3 Alias pseudonymity	94
14.4	Unlinkability (FPR_UNL)	94
14.4.1	Family behaviour	94
14.4.2	Components leveling and description	94
14.4.3	Management of FPR_UNL.1	95
14.4.4	Audit of FPR_UNL.1	95
14.4.5	FPR_UNL.1 Unlinkability of operations	95
14.5	Unobservability (FPR_UNO)	95
14.5.1	Family behaviour	95
14.5.2	Components leveling and description	95
14.5.3	Management of FPR_UNO.1, FPR_UNO.2	96
14.5.4	Management of FPR_UNO.3	96
14.5.5	Management of FPR_UNO.4	96
14.5.6	Audit of FPR_UNO.1, FPR_UNO.2	96
14.5.7	Audit of FPR_UNO.3	96
14.5.8	Audit of FPR_UNO.4	96
14.5.9	FPR_UNO.1 Unobservability	97
14.5.10	FPR_UNO.2 Allocation of information impacting unobservability	97
14.5.11	FPR_UNO.3 Unobservability without soliciting information	97
14.5.12	FPR_UNO.4 Authorized user observability	97
15	Class FPT: Protection of the TSF	98
15.1	Class description	98
15.2	TOE emanation (FPT_EMS)	100
15.2.1	Family behaviour	100
15.2.2	Components leveling and description	101
15.2.3	Management of FPT_EMS.1	101
15.2.4	Audit of FPT_EMS.1	101
15.2.5	FPT_EMS.1 Emanation of TSF and User data	101
15.3	Fail secure (FPT_FLS)	101
15.3.1	Family behaviour	101
15.3.2	Components leveling and description	102
15.3.3	Management of FPT_FLS.1	102
15.3.4	Audit of FPT_FLS.1	102
15.3.5	FPT_FLS.1 Failure with preservation of secure state	102
15.4	TSF initialization (FPT_INI)	102
15.4.1	Family behaviour	102
15.4.2	Components leveling and description	102
15.4.3	Management of FPT_INI.1	103
15.4.4	Audit of FPT_INI.1	103
15.4.5	FPT_INI.1 TSF initialization	103
15.5	Availability of exported TSF data (FPT_ITA)	103
15.5.1	Family behaviour	103
15.5.2	Components leveling and description	103
15.5.3	Management of FPT_ITA.1	104
15.5.4	Audit of FPT_ITA.1	104
15.5.5	FPT_ITA.1 Inter-TSF availability within a defined availability metric	104
15.6	Confidentiality of exported TSF data (FPT_ITC)	104

15.6.1	Family behaviour	104
15.6.2	Components leveling and description	104
15.6.3	Management of FPT_ITC.1	105
15.6.4	Audit of FPT_ITC.1	105
15.6.5	FPT_ITC.1 Inter-TSF confidentiality during transmission	105
15.7	Integrity of exported TSF data (FPT_ITI)	105
15.7.1	Family behaviour	105
15.7.2	Components leveling and description	105
15.7.3	Management of FPT_ITI.1	105
15.7.4	Management of FPT_ITI.2	106
15.7.5	Audit of FPT_ITI.1	106
15.7.6	Audit of FPT_ITI.2	106
15.7.7	FPT_ITI.1 Inter-TSF detection of modification	106
15.7.8	FPT_ITI.2 Inter-TSF detection and correction of modification	106
15.8	Internal TOE TSF data transfer (FPT_ITT)	107
15.8.1	Family behaviour	107
15.8.2	Components leveling and description	107
15.8.3	Management of FPT_ITT.1	107
15.8.4	Management of FPT_ITT.2	107
15.8.5	Management of FPT_ITT.3	108
15.8.6	Audit of FPT_ITT.1, FPT_ITT.2	108
15.8.7	Audit of FPT_ITT.3	108
15.8.8	FPT_ITT.1 Basic internal TSF data transfer protection	108
15.8.9	FPT_ITT.2 TSF data transfer separation	108
15.8.10	FPT_ITT.3 TSF data integrity monitoring	109
15.9	TSF physical protection (FPT_PHP)	109
15.9.1	Family behaviour	109
15.9.2	Components leveling and description	109
15.9.3	Management of FPT_PHP.1	110
15.9.4	Management of FPT_PHP.2	110
15.9.5	Management of FPT_PHP.3	110
15.9.6	Audit of FPT_PHP.1	110
15.9.7	Audit of FPT_PHP.2	110
15.9.8	Audit of FPT_PHP.3	110
15.9.9	FPT_PHP.1 Passive detection of physical attack	110
15.9.10	FPT_PHP.2 Notification of physical attack	111
15.9.11	FPT_PHP.3 Resistance to physical attack	111
15.10	Trusted recovery (FPT_RCV)	111
15.10.1	Family behaviour	111
15.10.2	Components leveling and description	111
15.10.3	Management of FPT_RCV.1	112
15.10.4	Management of FPT_RCV.2, FPT_RCV.3	112
15.10.5	Management of FPT_RCV.4	112
15.10.6	Audit of FPT_RCV.1, FPT_RCV.2, FPT_RCV.3	112
15.10.7	Audit of FPT_RCV.4	112
15.10.8	FPT_RCV.1 Manual recovery	112
15.10.9	FPT_RCV.2 Automated recovery	113
15.10.10		
	FPT_RCV.3 Automated recovery without undue loss	113
15.10.11		
	FPT_RCV.4 Function recovery	113
15.11	Replay detection (FPT_RPL)	114
15.11.1	Family behaviour	114
15.11.2	Components leveling and description	114
15.11.3	Management of FPT_RPL.1	114
15.11.4	Audit of FPT_RPL.1	114
15.11.5	FPT_RPL.1 Replay detection	114
15.12	State synchrony protocol (FPT_SSP)	115

15.12.1	Family behaviour	115
15.12.2	Components leveling and description	115
15.12.3	Management of FPT_SSP.1, FPT_SSP.2	115
15.12.4	Audit of FPT_SSP.1, FPT_SSP.2	115
15.12.5	FPT_SSP.1 Simple trusted acknowledgement	115
15.12.6	FPT_SSP.2 Mutual trusted acknowledgement	115
15.13	Time stamps (FPT_STM)	116
15.13.1	Family behaviour	116
15.13.2	Components leveling and description	116
15.13.3	Management of FPT_STM.1	116
15.13.4	Management of FPT_STM.2	116
15.13.5	Audit of FPT_STM.1	116
15.13.6	Audit of FPT_STM.2	116
15.13.7	FPT_STM.1 Reliable time stamps	117
15.13.8	FPT_STM.2 Time source	117
15.14	Inter-TSF TSF data consistency (FPT_TDC)	117
15.14.1	Family behaviour	117
15.14.2	Components leveling and description	117
15.14.3	Management of FPT_TDC.1	117
15.14.4	Audit of FPT_TDC.1	118
15.14.5	FPT_TDC.1 Inter-TSF basic TSF data consistency	118
15.15	Testing of external entities (FPT_TEE)	118
15.15.1	Family behaviour	118
15.15.2	Components leveling and description	118
15.15.3	Management of FPT_TEE.1	118
15.15.4	Audit of FPT_TEE.1	119
15.15.5	FPT_TEE.1 Testing of external entities	119
15.16	Internal TOE TSF data replication consistency (FPT_TRC)	119
15.16.1	Family behaviour	119
15.16.2	Components leveling and description	119
15.16.3	Management of FPT_TRC.1	119
15.16.4	Audit of FPT_TRC.1	120
15.16.5	FPT_TRC.1 Internal TSF consistency	120
15.17	TSF self-test (FPT_TST)	120
15.17.1	Family behaviour	120
15.17.2	Components leveling and description	120
15.17.3	Management of FPT_TST.1	121
15.17.4	Audit of FPT_TST.1	121
15.17.5	FPT_TST.1 TSF self-testing	121
16	Class FRU: Resource utilization	121
16.1	Class description	121
16.2	Fault tolerance (FRU_FLT)	122
16.2.1	Family behaviour	122
16.2.2	Components leveling and description	122
16.2.3	Management of FRU_FLT.1, FRU_FLT.2	122
16.2.4	Audit of FRU_FLT.1	122
16.2.5	Audit of FRU_FLT.2	122
16.2.6	FRU_FLT.1 Degraded fault tolerance	123
16.2.7	FRU_FLT.2 Limited fault tolerance	123
16.3	Priority of service (FRU_PRS)	123
16.3.1	Family behaviour	123
16.3.2	Components leveling and description	123
16.3.3	Management of FRU_PRS.1, FRU_PRS.2	123
16.3.4	Audit of FRU_PRS.1, FRU_PRS.2	124
16.3.5	FRU_PRS.1 Limited priority of service	124
16.3.6	FRU_PRS.2 Full priority of service	124
16.4	Resource allocation (FRU_RSA)	124
16.4.1	Family behaviour	124

16.4.2	Components leveling and description	124
16.4.3	Management of FRU_RSA.1	125
16.4.4	Management of FRU_RSA.2	125
16.4.5	Audit of FRU_RSA.1, FRU_RSA.2	125
16.4.6	FRU_RSA.1 Maximum quotas	125
16.4.7	FRU_RSA.2 Minimum and maximum quotas	125
17	Class FTA: TOE access	126
17.1	Class description	126
17.2	Limitation on scope of selectable attributes (FTA_LSA)	126
17.2.1	Family behaviour	126
17.2.2	Components leveling and description	126
17.2.3	Management of FTA_LSA.1	127
17.2.4	Audit of FTA_LSA.1	127
17.2.5	FTA_LSA.1 Limitation on scope of selectable attributes	127
17.3	Limitation on multiple concurrent sessions (FTA_MCS)	127
17.3.1	Family behaviour	127
17.3.2	Components leveling and description	127
17.3.3	Management of FTA_MCS.1	128
17.3.4	Management of FTA_MCS.2	128
17.3.5	Audit of FTA_MCS.1, FTA_MCS.2	128
17.3.6	FTA_MCS.1 Basic limitation on multiple concurrent sessions	128
17.3.7	FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions	128
17.4	Session locking and termination (FTA_SSL)	129
17.4.1	Family behaviour	129
17.4.2	Components leveling and description	129
17.4.3	Management of FTA_SSL.1	129
17.4.4	Management of FTA_SSL.2	129
17.4.5	Management of FTA_SSL.3	129
17.4.6	Management of FTA_SSL.4	130
17.4.7	Audit of FTA_SSL.1, FTA_SSL.2	130
17.4.8	Audit of FTA_SSL.3	130
17.4.9	Audit of FTA_SSL.4	130
17.4.10	FTA_SSL.1 TSF-initiated session locking	130
17.4.11	FTA_SSL.2 User-initiated locking	130
17.4.12	FTA_SSL.3 TSF-initiated termination	131
17.4.13	FTA_SSL.4 User-initiated termination	131
17.5	TOE access banners (FTA_TAB)	131
17.5.1	Family behaviour	131
17.5.2	Components leveling and description	131
17.5.3	Management of FTA_TAB.1	131
17.5.4	Audit of FTA_TAB.1	132
17.5.5	FTA_TAB.1 Default TOE access banners	132
17.6	TOE access history (FTA_TAH)	132
17.6.1	Family behaviour	132
17.6.2	Components leveling and description	132
17.6.3	Management of FTA_TAH.1	132
17.6.4	Audit of FTA_TAH.1	132
17.6.5	FTA_TAH.1 TOE access history	132
17.7	TOE session establishment (FTA_TSE)	133
17.7.1	Family behaviour	133
17.7.2	Components leveling and description	133
17.7.3	Management of FTA_TSE.1	133
17.7.4	Audit of FTA_TSE.1	133
17.7.5	FTA_TSE.1 TOE session establishment	133
18	Class FTP: Trusted path/channels	134
18.1	Class description	134
18.2	Inter-TSF trusted channel (FTP_ITC)	135

18.2.1	Family behaviour	135
18.2.2	Components leveling and description	135
18.2.3	Management of FTP_ITC.1	135
18.2.4	Audit of FTP_ITC.1	135
18.2.5	FTP_ITC.1 Inter-TSF trusted channel	135
18.3	Trusted channel protocol (FTP_PRO)	136
18.3.1	Family behavior	136
18.3.2	Components leveling and description	136
18.3.3	Management of FTP_PRO.1	136
18.3.4	Management of FTP_PRO.2	136
18.3.5	Management of FTP_PRO.3	136
18.3.6	Audit of FTP_PRO.1	137
18.3.7	Audit of FTP_PRO.2	137
18.3.8	Audit of FTP_PRO.3	137
18.3.9	FTP_PRO.1 Trusted channel protocol	137
18.3.10	FTP_PRO.2 Trusted channel establishment	138
18.3.11	FTP_PRO.3 Trusted channel data protection	138
18.4	Trusted path (FTP_TRP)	139
18.4.1	Family behaviour	139
18.4.2	Components leveling and description	139
18.4.3	Management of FTP_TRP.1	139
18.4.4	Audit of FTP_TRP.1	139
18.4.5	FTP_TRP.1 Trusted path	139
Annex A (informative) Security functional requirements (SFRs) structure of the application notes		141
Annex B (informative) Dependency tables for security functional components		144
Annex C (normative) Class FAU: Security audit — Application notes		153
Annex D (normative) Class FCO: Communication — Application notes		166
Annex E (normative) Class FCS: Cryptographic support — Application notes		171
Annex F (normative) Class FDP: User data protection — Application notes		181
Annex G (normative) Class FIA: Identification and authentication — Application notes		208
Annex H (normative) Class FMT: Security management — Application notes		218
Annex I (normative) Class FPR: Privacy — Application notes		228
Annex J (normative) Class FPT: Protection of the TSF — Application notes		240
Annex K (normative) Class FRU: Resource utilization — Application notes		258
Annex L (normative) Class FTA: TOE access — Application notes		263
Annex M (normative) Class FTP: Trusted path/channels- application notes		269
Bibliography		273

Foreword

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

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 document 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 or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see <https://patents.iec.ch>).

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. In the IEC, see www.iec.ch/understanding-standards.

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

This fourth edition cancels and replaces the third edition (ISO 15408-2:2008), which has been technically revised.

The main changes are as follows:

- new security functional components have been introduced.

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

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 and www.iec.ch/national-committees.

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 15408-1:2022, 5.2, 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:

- a) 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 15408-1:20—, Clause 7, provides more detailed information on the relationship between security objectives and security requirements;
- b) developers, who respond to actual or perceived consumer security requirements in constructing a TOE, 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;
- c) 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 This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type 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.

The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

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 15408-1:2022, *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 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 <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

identity

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

EXAMPLE An example of such a representation is a string.

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.

Note 2 to entry: An entity can have more than one identity.

3.2

inter TSF transfer

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