BS EN ISO/IEC 15408-2:2023

BSI Standards Publication

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

Part 2: Security functional components

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 15408-2:2023

National foreword

This British Standard is the UK implementation of EN ISO/IEC 15408-2:2023. It is identical to ISO/IEC 15408-2:2022. It supersedes BS EN ISO/IEC 15408-2:2020, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/3, Security Evaluation, Testing and Specification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 580 99017 5

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2023.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 15408-2:2023

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

© 2023 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

AVA Documents Document Sharing Hub

Full document details: BS EN ISO/IEC 15408-2:2023

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.

AVA Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 15408-2:2023

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

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 15408-2:2023

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

AVA Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 15408-2:2023

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

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 15408-2:2023

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

© ISO/IEC 2022 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 15408-2:2023

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

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 15408-2:2023

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

© ISO/IEC 2022 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 15408-2:2023

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

© ISO/IEC 2022 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 15408-2:2023

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**

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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	Ministerio de Asuntos Económicos y Transformación Digital
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 15408-2:2023

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

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 15408-2:2023

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 (SFP)* (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 evalution (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* (3.5) of the target of evalution (TOE) upon which the enforcement of the security functional requirement (SFR) relies

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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* (3.5) of the TOE security funtionality (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
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

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

RPC	remote procedure call
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 15408-1:2022, 8.4.

5.2 Organization of this document

Clause 5 describes the paradigm used in the SFRs of this document.

Clause 7 introduces the catalogue of functional components, while Clauses 8 through 18 describe the functional classes.

Annex A provides explanatory information for potential users of the functional components.

Annex B provides a complete cross reference table of the functional component dependencies.

Annexes C through M provide the explanatory information for the functional classes. This material shall be seen as normative instructions on how to apply relevant operations and select appropriate audit or documentation information. Where different options are given, the choice is left to the PP, PP-Module, functional package and ST author.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

Those who author PPs, PP-Modules, functional packages, or STs shall refer to ISO/IEC 15408-1:2022 for relevant structures, rules, and guidance, in particular:

a) ISO/IEC 15408-1:2022, Clause 3 defines the terms and definitions used in the ISO/IEC 15408 series;

b) ISO/IEC 15408-1:2022, Clause 7 describes how SFRs can be specified using the security functional components;

c) ISO/IEC 15408-1:2022, Clause 8 describes how security functional components are organized, and the operations that may be applied to them;

d) ISO/IEC 15408-1:2022, Annex A provides further information on the structure for security functional packages;

e) ISO/IEC 15408-1:2022, Annex B provides further information on the structure for PPs;

f) ISO/IEC 15408-1:2022, Annex C provides further information on the structure of PP-Modules and PP-Configurations;

g) ISO/IEC 15408-1:2022, 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:

a) 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

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 15408-2:2023

separately evaluated). Exchanges of information in this situation are called inter-TSF transfers, as they are between the TSFs of distinct trusted products;

b) 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 (man-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 FMT_SMR) 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. Several types of subjects may exist within a TOE:

a) those acting on behalf of an authorized user;

EXAMPLE 4 UNIX processes.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

b) those acting as a specific functional process that may in turn act on behalf of multiple users;

EXAMPLE 5 Functions as can be found in client/server architectures.

c) those acting as part of the TOE itself.

EXAMPLE 6 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 7 An example of a subject is an inter-process communication.

Objects can contain information. This concept is required to specify information flow control policies as addressed in the FDP class.

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 8

User data:

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

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.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

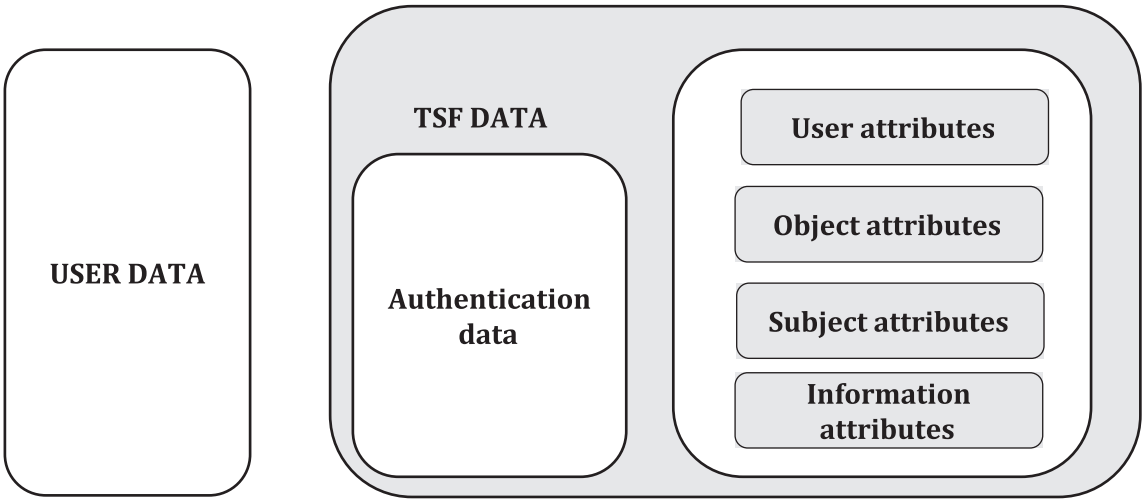

Figure 1 — Relationship between user data and TSF data

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 9

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 subclauses are indicated.

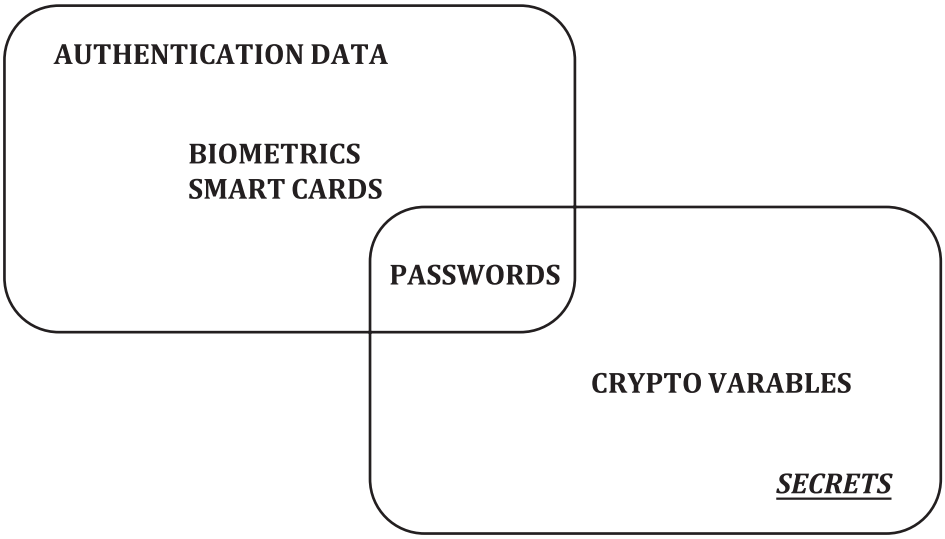

Figure 2 — Relationship between "authentication data" and "secrets"

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

7 Security functional components

7.1 Overview

7.1.1 General

This clause defines the content and presentation of the functional requirements of this document and provides guidance on the organization of the requirements for new, extended components that may be included in a PP, PP-Module, functional package or ST. As described in ISO/IEC 15408-1:2022, Clause 8, the functional components and requirements are expressed in classes, families, components and elements.

7.1.2 Class structure

7.1.2.1 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.

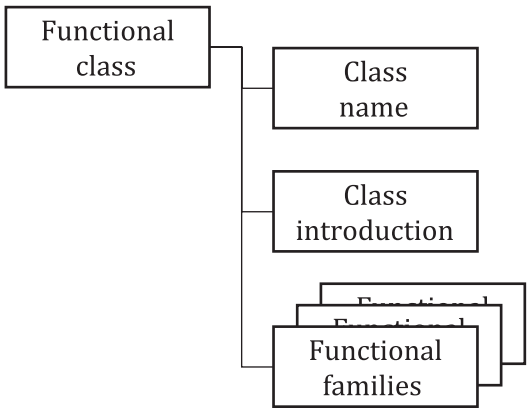

Figure 3 — Functional class structure

NOTE A functional class can contain multiple functional families.

7.1.2.2 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.

7.1.2.3 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 7.2.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

7.1.3 Family structure

7.1.3.1 General

Figure 4 illustrates the functional family structure in diagrammatic form.

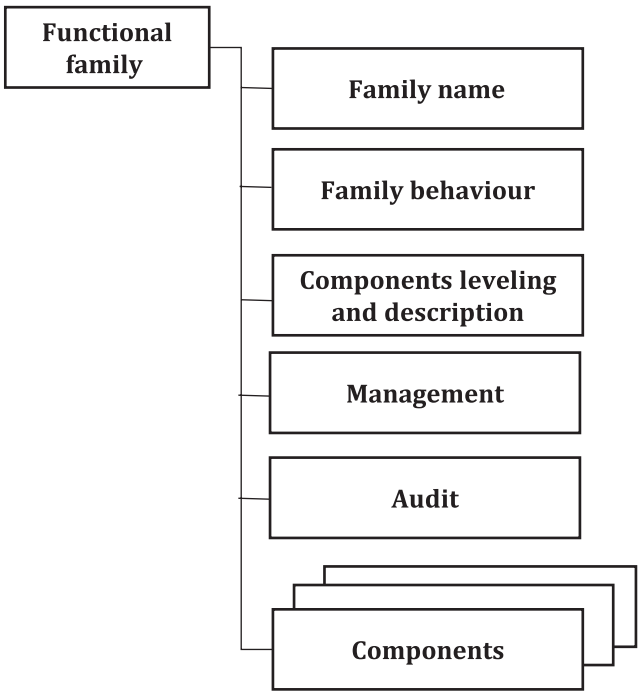

Figure 4 — Functional family structure

7.1.3.2 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.

7.1.3.3 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:

a) 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;

b) 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.

7.1.3.4 Components leveling 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 leveling and description subclause is to provide information to users in selecting an appropriate functional

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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 7.2 the descriptions of the families provide a graphical overview of the hierarchy of the components in a family.

7.1.3.5 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 the management class (FMT) 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.

7.1.3.6 Audit

The audit requirements subclauses contain auditable events for the authors to select, if requirements from the class FAU 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) 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 the FAU class the rules governing the audit are explained in more detail.

7.1.4 Component structure

7.1.4.1 General

Figure 5 illustrates the functional component structure.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

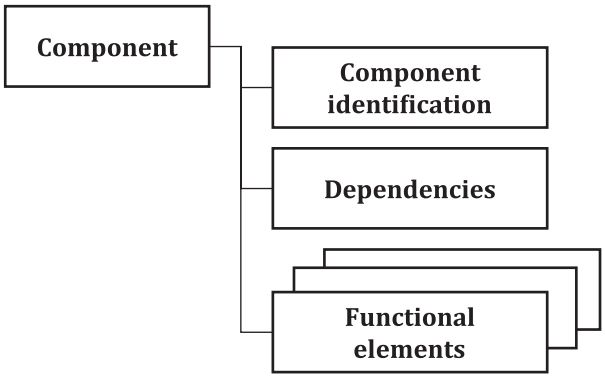

Figure 5 — Functional component structure

7.1.4.2 Component identification

The component identification subclause(s) provide 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;

— 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.

7.1.4.3 Functional elements

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

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

The component 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.

7.1.4.4 Dependencies

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.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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 Annex B of this document. 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.

EXAMPLE FDP_UIT.1 Data exchange integrity.

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.

7.2 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 6 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 similar to Figure 6 is provided. In Figure 6, 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.

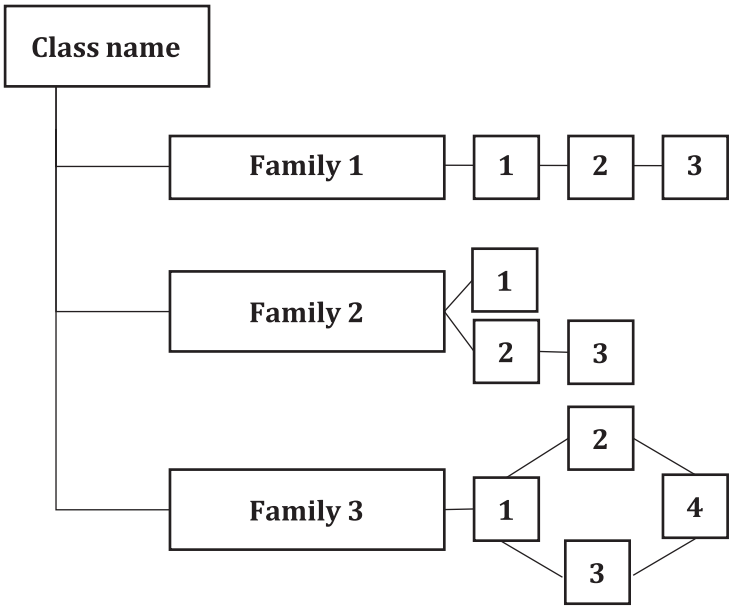

Figure 6 — Sample class decomposition diagram

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

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.

8 Class FAU: Security audit

8.1 Class description

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 7 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex C provides explanatory information for this class and should be consulted when using the components identified in this class.

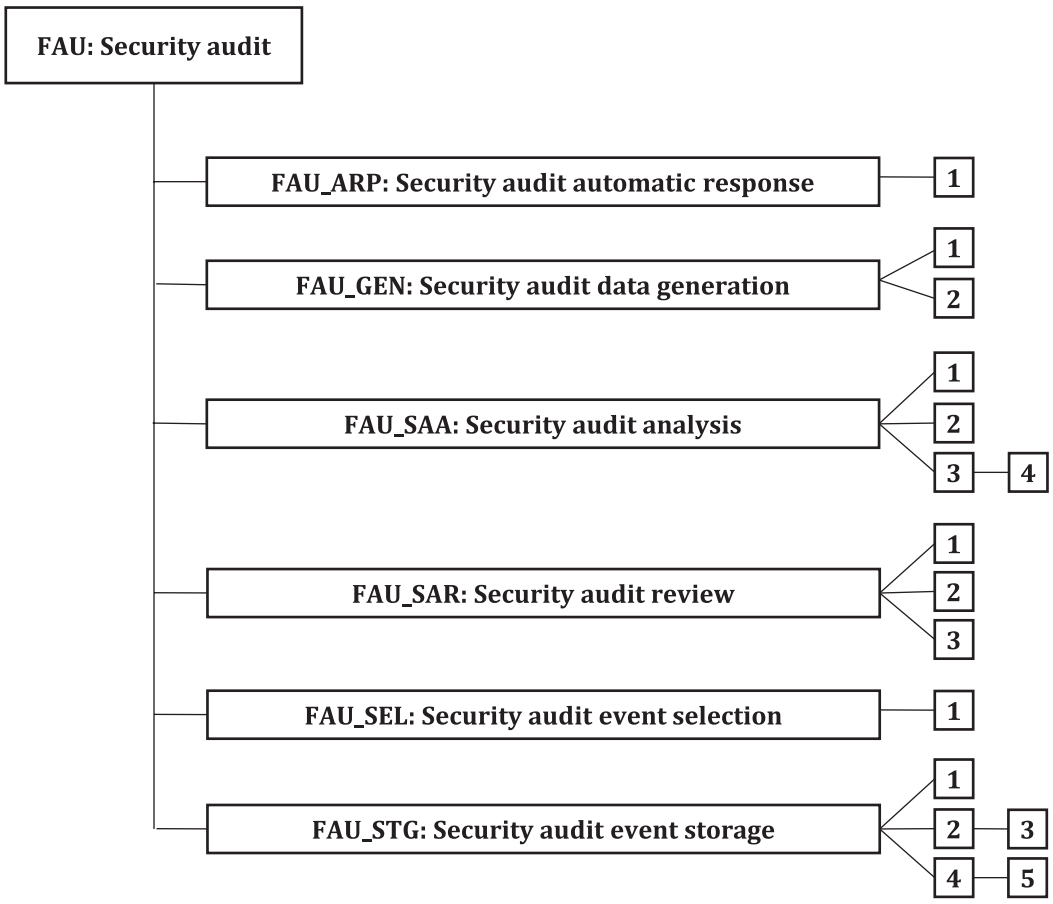

Figure 7 — FAU: Security audit class decomposition

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

8.2 Security audit automatic response (FAU_ARP)

8.2.1 Family behaviour

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

8.2.2 Components leveling and description

Figure 8 shows the component leveling for this family.

Figure 8 — FAU_ARP: Component leveling

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

8.2.3 Management of FAU_ARP.1

The following actions can be considered for the management functions in FMT:

a) the management (addition, removal, or modification) of actions.

8.2.4 Audit of FAU_ARP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Actions taken due to potential security violations.

8.2.5 FAU_ARP.1 Security alarms

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1

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

8.3 Security audit data generation (FAU_GEN)

8.3.1 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.

8.3.2 Components leveling and description

Figure 9 shows the component leveling for this family.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

Figure 9 — FAU_GEN: Component leveling

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.

8.3.3 Management of FAU_GEN.1, FAU_GEN.2

The following actions can be considered for the management functions in FMT:

a) there are no management activities foreseen.

8.3.4 Audit of FAU_GEN.1, FAU_GEN.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

8.3.5 FAU_GEN.1 Audit data generation

Component relationships

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit;

c) [assignment: other specifically defined auditable events].

FAU_GEN.1.2

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

a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;

b) 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: *other audit relevant information*].

8.3.6 FAU_GEN.2 User identity association

Component relationships

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification

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.

8.4 Security audit analysis (FAU_SAA)

8.4.1 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) family as desired.

8.4.2 Components leveling and description

Figure 10 shows the component leveling for this family.

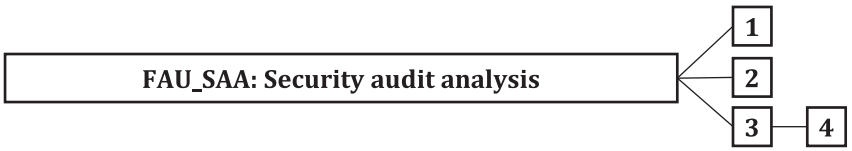

Figure 10 — FAU_SAA: Component leveling

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.

8.4.3 Management of FAU_SAA.1

The following actions can be considered for the management functions in FMT:

a) maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.

AVA Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 15408-2:2023

8.4.4 Management of FAU_SAA.2

The following actions can be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users in the profile target group.

8.4.5 Management of FAU_SAA.3

The following actions can be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the subset of system events.

8.4.6 Management of FAU_SAA.4

The following actions can be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the subset of system events;

b) maintenance (deletion, modification, addition) of the set of sequences of system events.

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

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: Enabling and disabling of any of the analysis mechanisms;

b) minimal: Automated responses performed by the tool.

8.4.8 FAU_SAA.1 Potential violation analysis

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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.

FAU_SAA.1.2

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

a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;

b) [assignment: *any other rules*].

8.4.9 FAU_SAA.2 Profile based anomaly detection

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FAU_SAA.2.1

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: *the profile target group*].

FAU_SAA.2.2

The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.

FAU_SAA.2.3

The TSF shall be able to indicate a possible violation of the enforcement of the SFRs when a user's suspicion rating exceeds the following threshold conditions [assignment: *conditions under which anomalous activity is reported by the TSF*].

8.4.10 FAU_SAA.3 Simple attack heuristics

Component relationships

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAA.3.1

The TSF shall be able to maintain an internal representation of the following signature events [assignment: *a subset of system events*] that may indicate a violation of the enforcement of the SFRs.

FAU_SAA.3.2

The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].

FAU_SAA.3.3

The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when a system event is found to match a signature event that indicates a potential violation of the enforcement of the SFRs.

8.4.11 FAU_SAA.4 Complex attack heuristics

Component relationships

Hierarchical to: FAU_SAA.3 Simple attack heuristics

Dependencies: No dependencies.

FAU_SAA.4.1

The TSF shall be able to maintain an internal representation of the following **event sequences of known intrusion scenarios [assignment: *list of sequences of system events whose occurrence are representative of known penetration scenarios*] and the following** signature events [assignment: *a subset of system events*] that may indicate a **potential** violation of the enforcement of the SFRs.

FAU_SAA.4.2

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

The TSF shall be able to compare the signature events **and event sequences** against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].

FAU_SAA.4.3

The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when system **activity** is found to match a signature event **or event sequence** that indicates a potential violation of the enforcement of the SFRs.

8.5 Security audit review (FAU_SAR)

8.5.1 Family behaviour

This family defines the requirements for tools that are made available to authorized users to assist in the review of audit data.

8.5.2 Components leveling and description

Figure 11 shows the component leveling for this family.

Figure 11 — FAU_SAR: Component leveling

FAU_SAR.1 Audit review, provides the capability to read information from the audit data.

FAU_SAR.2 Restricted audit review, requires that there are no other users except those that have been identified in FAU_SAR.1 Audit review that can read the information.

FAU_SAR.3 Selectable audit review, requires audit review tools to select the audit data to be reviewed based on criteria.

8.5.3 Management of FAU_SAR.1

The following actions can be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.

8.5.4 Management of FAU_SAR.2, FAU_SAR.3

The following actions can be considered for the management functions in FMT:

a) there are no management activities foreseen.

8.5.5 Audit of FAU_SAR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Reading of information from the audit records.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

8.5.6 Audit of FAU_SAR.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Unsuccessful attempts to read information from the audit records.

8.5.7 Audit of FAU_SAR.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) detailed: The parameters used for the viewing.

8.5.8 FAU_SAR.1 Audit review

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of audit information*] from the audit data.

FAU_SAR.1.2

The TSF shall provide the audit data in a manner suitable for the user to interpret the information.

8.5.9 FAU_SAR.2 Restricted audit review

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit data, except those users that have been granted explicit read access.

8.5.10 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1

The TSF shall provide the ability to apply [assignment: *methods of selection and/or ordering*] of audit data based on [assignment: *criteria with logical relations*].

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

8.6 Security audit event selection (FAU_SEL)

8.6.1 Family behaviour

This family defines requirements to select the set of events to be audited during TOE operation from the set of all auditable events.

8.6.2 Components leveling and description

Figure 12 shows the component leveling for this family.

Figure 12 — FAU_SEL: Component leveling

FAU_SEL.1 Selective audit, requires the ability to select the set of events to be audited from the set of all auditable events, identified in FAU_GEN.1 Audit data generation, based upon attributes to be specified by the author of a PP, PP-Module, functional package or ST.

8.6.3 Management of FAU_SEL.1

The following actions can be considered for the management functions in FMT:

a) maintenance of the rights to view/modify the audit data.

8.6.4 Audit of FAU_SEL.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: All modifications to the audit configuration that occur while the audit collection functions are operating.

8.6.5 FAU_SEL.1 Selective audit

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_SEL.1.1

The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [selection: *object identity, user identity, subject identity, host identity, event type*]

b) [assignment: *list of additional attributes that audit selectivity is based upon*]

8.7 Security audit data storage (FAU_STG)

8.7.1 Family behaviour

This family defines the requirements for the TSF to be able to create and maintain a secure audit trail. Stored audit data refers to those data stored within an audit trail, and not to any audit data that has been retrieved (to temporary storage) through selection.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

8.7.2 Components leveling and description

Figure 13 shows the component leveling for this family.

Figure 13 — FAU_STG: Component leveling

FAU_STG.1 Audit data storage location, requires that the storage location(s) for audit data be specified.

FAU_STG.2 Protected audit data storage, requires that protections are placed on the audit data. It will be protected from unauthorized deletion and/or modification.

FAU_STG.3 Guarantees of audit data availability, specifies the guarantees that the TSF maintains over the audit data given the occurrence of an undesired condition.

FAU_STG.4 Action in case of possible audit data loss specifies actions to be taken if a threshold on the stored audit data is exceeded.

FAU_STG.5 Prevention of audit data loss specifies actions to be taken in the case that audit data storage is full.

8.7.3 Management of FAU_STG.1

The following actions can be considered for the management functions in FMT:

a) maintenance of remote audit storage locations.

8.7.4 Management of FAU_STG.2

The following actions can be considered for the management functions in FMT:

a) there are no management activities foreseen.

8.7.5 Management of FAU_STG.3

The following actions can be considered for the management functions in FMT:

a) maintenance of the parameters that control the audit data storage capability.

8.7.6 Management of FAU_STG.4

The following actions can be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of actions to be taken in case of imminent audit data storage failure.

8.7.7 Management of FAU_STG.5

The following actions can be considered for the management functions in FMT:

a) maintenance (deletion, modification, addition) of actions to be taken in case of audit data storage failure.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

8.7.8 Audit of FAU_STG.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Changes in the location of remote audit data storage.

8.7.9 Audit of FAU_STG.2, FAU_STG.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) there are no auditable events foreseen.

8.7.10 Audit of FAU_STG.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Actions taken due to exceeding of a threshold.

8.7.11 Audit of FAU_STG.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) basic: Actions taken due to the audit data storage failure.

8.7.12 FAU_STG.1 Audit data storage location

Component relationships

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FTP_ITC.1 Inter-TSF trusted channel

FAU_STG.1.1

The TSF shall be able to store generated audit data on the [selection: *TOE itself, transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC, [assignment: other storage location(s)]*.]

8.7.13 FAU_STG.2 Protected audit data storage

Component relationships

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation

FAU_STG.2.1

The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.2.2

The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorized modifications to the stored audit data in the audit trail.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

8.7.14 FAU_STG.3 Guarantees of audit data availability

Component relationships

Hierarchical to: FAU_STG.2 Protected audit data storage

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.3.1

The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.3.2

The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorized modifications to the stored audit data in the audit trail.

FAU_STG.3.3

The TSF shall ensure that [assignment: *metric for saving audit data*] stored audit data will be maintained when the following conditions occur: [selection: *audit data storage exhaustion, failure, attack*].

8.7.15 FAU_STG.4 Action in case of possible audit data loss

Component relationships

Hierarchical to: No other components.

Dependencies: FAU_STG.2 Protected audit data storage

FAU_STG.4.1

The TSF shall [assignment: ***actions to be taken in case of possible audit data storage failure***] if the audit data storage **exceeds** [assignment: ***pre-defined limit***].

8.7.16 FAU_STG.5 Prevention of audit data loss

Component relationships

Hierarchical to: FAU_STG.4 Action in case of possible audit data loss

Dependencies: FAU_STG.2 Protected audit data storage
FAU_GEN.1 Audit data generation

FAU_STG.5.1

The TSF shall [selection: *ignore audited events, "prevent audited events, except those taken by the authorized user with special rights", overwrite the oldest stored audit records*], [assignment: *other actions to be taken in case of audit storage failure and conditions for the actions*] if the audit data storage is full.

9 Class FCO: Communication

9.1 Class description

This class provides two families specifically concerned with assuring the identity of a party participating in a data exchange. These families are related to assuring the identity of the originator of transmitted information (proof of origin) and assuring the identity of the recipient of transmitted

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

information (proof of receipt). These families ensure that an originator cannot deny having sent the message, nor can the recipient deny having received it. Figure 14 shows the decomposition of the class.

Figure 14 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex D provides explanatory information for this class and should be consulted when using the components identified in this class.

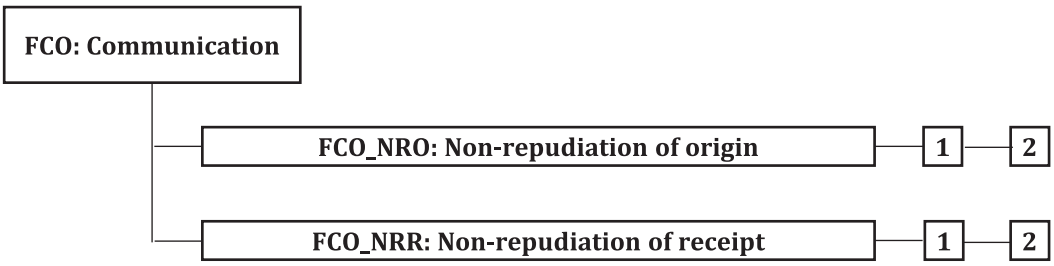

Figure 14 — FCO: Communication class decomposition

9.2 Non-repudiation of origin (FCO_NRO)

9.2.1 Family behaviour

Non-repudiation of origin ensures that the originator of information cannot successfully deny having sent the information. This family requires that the TSF provide a method to ensure that a subject that receives information during a data exchange is provided with evidence of the origin of the information. This evidence can then be verified by either this subject or other subjects.

9.2.2 Components leveling and description

Figure 15 shows the component leveling for this family.

Figure 15 — FCO_NRO: Component leveling

FCO_NRO.1 Selective proof of origin, requires the TSF to provide subjects with the capability to request evidence of the origin of information.

FCO_NRO.2 Enforced proof of origin, requires that the TSF always generate evidence of origin for transmitted information.

9.2.3 Management of FCO_NRO.1, FCO_NRO.2

The following actions can be considered for the management functions in FMT:

a) the management of changes to information types, fields, originator attributes and recipients of evidence.

9.2.4 Audit of FCO_NRO.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The identity of the user who requested that evidence of origin would be generated;

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

b) minimal: The invocation of the non-repudiation service;

c) basic: Identification of the information, the destination, and a copy of the evidence provided;

d) Ddetailed: The identity of the user who requested a verification of the evidence.

9.2.5 Audit of FCO_NRO.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The invocation of the non-repudiation service;

b) basic: Identification of the information, the destination, and a copy of the evidence provided;

c) detailed: The identity of the user who requested a verification of the evidence.

9.2.6 FCO_NRO.1 Selective proof of origin

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.1.1

The TSF shall be able to generate evidence of origin for transmitted [assignment: *list of information types*] at the request of the [selection: *originator, recipient, [assignment: list of third parties]*].

FCO_NRO.1.2

The TSF shall be able to relate the [assignment: *list of attributes*] of the originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

FCO_NRO.1.3

The TSF shall provide a capability to verify the evidence of origin of information to [selection: *originator, recipient, [assignment: list of third parties]*] given [assignment: *limitations on the evidence of origin*].

9.2.7 FCO_NRO.2 Enforced proof of origin

Component relationships

Hierarchical to: FCO_NRO.1 Selective proof of origin

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.2.1

The TSF shall **enforce the generation of** evidence of origin for transmitted [assignment: *list of information types*] at **all times.**

FCO_NRO.2.2

The TSF shall be able to relate the [assignment: *list of attributes*] of the originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

FCO_NRO.2.3

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

The TSF shall provide a capability to verify the evidence of origin of information to [selection: *originator, recipient, [assignment: list of third parties]*] given [assignment: *limitations on the evidence of origin*].

9.3 Non-repudiation of receipt (FCO_NRR)

9.3.1 Family behaviour

Non-repudiation of receipt ensures that the recipient of information cannot successfully deny receiving the information. This family requires that the TSF provide a method to ensure that a subject that transmits information during a data exchange is provided with evidence of receipt of the information. This evidence can then be verified by either this subject or other subjects.

9.3.2 Components leveling and description

Figure 16 shows the component leveling for this family.

Figure 16 — FCO_NRR: Component leveling

FCO_NRR.1 Selective proof of receipt, requires the TSF to provide subjects with a capability to request evidence of the receipt of information.

FCO_NRR.2 Enforced proof of receipt, requires that the TSF always generate evidence of receipt for received information.

9.3.3 Management of FCO_NRR.1, FCO_NRR.2

The following actions can be considered for the management functions in FMT:

a) the management of changes to information types, fields, originator attributes and third-party recipients of evidence.

9.3.4 Audit of FCO_NRR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The identity of the user who requested that evidence of receipt would be generated;

b) minimal: The invocation of the non-repudiation service;

c) basic: Identification of the information, the destination, and a copy of the evidence provided;

d) detailed: The identity of the user who requested a verification of the evidence.

9.3.5 Audit of FCO_NRR.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP, PP-Module, functional package or ST:

a) minimal: The invocation of the non-repudiation service;

b) basic: Identification of the information, the destination, and a copy of the evidence provided;

c) detailed: The identity of the user who requested a verification of the evidence.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

9.3.6 FCO_NRR.1 Selective proof of receipt

Component relationships

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FCO_NRR.1.1

The TSF shall be able to generate evidence of receipt for received [assignment: *list of information types*] at the request of the [selection: *originator, recipient, [assignment: list of third parties]*].

FCO_NRR.1.2

The TSF shall be able to relate the [assignment: *list of attributes*] of the recipient of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

FCO_NRR.1.3

The TSF shall provide a capability to verify the evidence of receipt of information to [selection: *originator, recipient, [assignment: list of third parties]*] given [assignment: *limitations on the evidence of receipt*].

9.3.7 FCO_NRR.2 Enforced proof of receipt

Component relationships

Hierarchical to: FCO_NRR.1 Selective proof of receipt

Dependencies: FIA_UID.1 Timing of identification

FCO_NRR.2.1

The TSF shall **enforce the generation of** evidence of receipt for received [assignment: *list of information types*] at **all times.**

FCO_NRR.2.2

The TSF shall be able to relate the [assignment: *list of attributes*] of the recipient of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

FCO_NRR.2.3

The TSF shall provide a capability to verify the evidence of receipt of information to [selection: *originator, recipient, [assignment: list of third parties]*] given [assignment: *limitations on the evidence of receipt*].

10 Class FCS: Cryptographic support

10.1 Class description

The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include, but are not limited to: identification and authentication, non-repudiation, trusted path, trusted channel, and data separation. This class is used when the TOE implements cryptographic functions, the implementation of which can be in hardware, firmware and/or software.

The FCS: Cryptographic support class is composed of four families.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023

Figure 17 shows the decomposition of this class, it's families and components. Elements are not shown in the figure.

Annex E provides explanatory information for this class and should be consulted when using the components identified in this class.

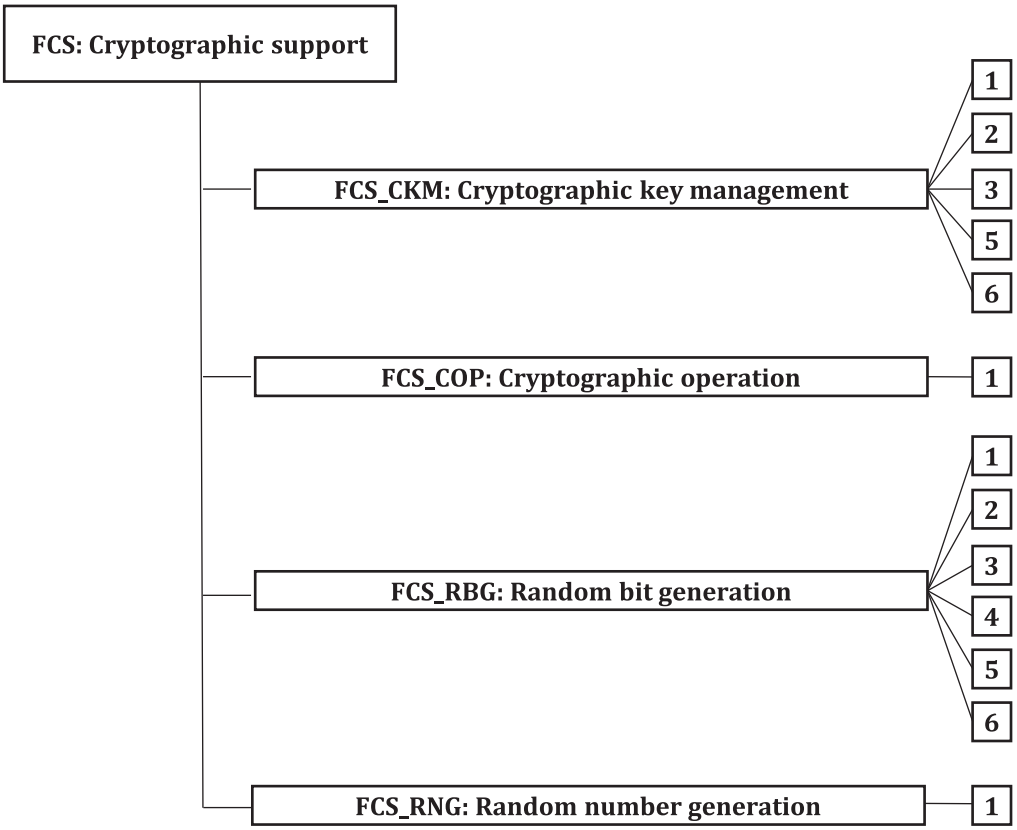

Figure 17 — FCS: Cryptographic support class decomposition

10.2 Cryptographic key management (FCS_CKM)

10.2.1 Family behaviour

Cryptographic keys must be managed throughout their life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities:

— cryptographic key generation;

— cryptographic key distribution;

— cryptographic key access;

— cryptographic key derivation;

— timing and event of cryptographic key destruction.

This family should be included whenever there are functional requirements for the management of cryptographic keys.

10.2.2 Components leveling and description

Figure 18 shows the component leveling for this family.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 15408-2:2023