



# SLOVENSKI STANDARD

## SIST EN ISO/IEC 15408-2:2020

01-maj-2020

---

### Informacijska tehnologija - Varnostne tehnike - Merila za vrednotenje varnosti IT - 2. del: Funkcionalne varnostne komponente (ISO/IEC 15408-2:2008)

Information technology - Security techniques - Evaluation criteria for IT security - Part 2:  
Security functional components (ISO/IEC 15408-2:2008)

Informationstechnik - Sicherheitstechniken - Bewertungskriterien für die IT-Sicherheit -  
Teil 2: Sicherheitsfunktionskomponenten (ISO/IEC 15408-2:2008)

Technologies de l'information - Techniques de sécurité - Critères d'évaluation pour la  
sécurité TI - Partie 2: Composants fonctionnels de sécurité (ISO/IEC 15408-2:2008)

<https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ee12372e3e3f/sist-en-iso-iec-15408-2-2020>

Ta slovenski standard je istoveten z: **EN ISO/IEC 15408-2:2020**

---

#### **ICS:**

35.030            Informacijska varnost            IT Security

**SIST EN ISO/IEC 15408-2:2020**            **en**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN ISO/IEC 15408-2:2020](https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020)

<https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020>

EUROPEAN STANDARD

EN ISO/IEC 15408-2

NORME EUROPÉENNE

EUROPÄISCHE NORM

March 2020

ICS 35.030

English version

## Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components (ISO/IEC 15408-2:2008)

Technologies de l'information - Techniques de sécurité  
- Critères d'évaluation pour la sécurité TI - Partie 2:  
Composants fonctionnels de sécurité (ISO/IEC 15408-  
2:2008)

Informationstechnik - Sicherheitstechniken -  
Bewertungskriterien für die IT-Sicherheit - Teil 2:  
Sicherheitsfunktionskomponenten (ISO/IEC 15408-  
2:2008)

This European Standard was approved by CEN on 2 March 2020.

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, Turkey and United Kingdom.



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

Contents	Page
European foreword.....	3

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN ISO/IEC 15408-2:2020](https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020)  
<https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020>

## European foreword

The text of ISO/IEC 15408-2:2008 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 15408-2:2020 by Technical Committee CEN/CLC/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 September 2020, and conflicting national standards shall be withdrawn at the latest by September 2020.

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

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, Turkey and the United Kingdom.

## iTeh STANDARD PREVIEW Endorsement notice (standards.iteh.ai)

The text of ISO/IEC 15408-2:2008 has been approved by CEN as EN ISO/IEC 15408-2:2020 without any modification.

[SIST EN ISO/IEC 15408-2:2020](https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020)

<https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN ISO/IEC 15408-2:2020](https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020)

<https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020>

# INTERNATIONAL STANDARD

# ISO/IEC 15408-2

Third edition  
2008-08-15

Corrected version  
2011-06-01

---

---

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

### Part 2: Security functional components

**iTeh STANDARD PREVIEW**  
*Technologies de l'information — Techniques de sécurité — Critères  
d'évaluation pour la sécurité TI —  
(standards.iteh.ai)*  
*Partie 2: Composants fonctionnels de sécurité*

[SIST EN ISO/IEC 15408-2:2020](https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020)

<https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020>

---

---

Reference number  
ISO/IEC 15408-2:2008(E)



## iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO/IEC 15408-2:2020

<https://standards.iteh.ai/catalog/standards/sist/e97c5427-be26-40c1-9ab7-ec12372c3a3f/sist-en-iso-iec-15408-2-2020>



### **COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland



## Contents

Page

Foreword .....	xviii
Introduction.....	xx
1 Scope .....	1
2 Normative references .....	1
3 Terms and definitions, symbols and abbreviated terms .....	1
4 Overview.....	1
4.1 Organisation of this part of ISO/IEC 15408 .....	1
5 Functional requirements paradigm .....	2
6 Security functional components.....	5
6.1 Overview.....	5
6.1.1 Class structure .....	5
6.1.2 Family structure.....	6
6.1.3 Component structure .....	8
6.2 Component catalogue.....	9
6.2.1 Component changes highlighting.....	10
7 Class FAU: Security audit.....	10
7.1 Security audit automatic response (FAU_ARP).....	11
7.1.1 Family Behaviour.....	11
7.1.2 Component levelling .....	11
7.1.3 Management of FAU_ARP.1 .....	11
7.1.4 Audit of FAU_ARP.1 .....	11
7.1.5 FAU_ARP.1 Security alarms.....	11
7.2 Security audit data generation (FAU_GEN) .....	11
7.2.1 Family Behaviour.....	11
7.2.2 Component levelling .....	11
7.2.3 Management of FAU_GEN.1, FAU_GEN.2.....	11
7.2.4 Audit of FAU_GEN.1, FAU_GEN.2 .....	11
7.2.5 FAU_GEN.1 Audit data generation .....	12
7.2.6 FAU_GEN.2 User identity association.....	12
7.3 Security audit analysis (FAU_SAA) .....	12
7.3.1 Family Behaviour.....	12
7.3.2 Component levelling .....	12
7.3.3 Management of FAU_SAA.1 .....	13
7.3.4 Management of FAU_SAA.2 .....	13
7.3.5 Management of FAU_SAA.3 .....	13
7.3.6 Management of FAU_SAA.4 .....	13
7.3.7 Audit of FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4.....	13
7.3.8 FAU_SAA.1 Potential violation analysis .....	13
7.3.9 FAU_SAA.2 Profile based anomaly detection .....	14
7.3.10 FAU_SAA.3 Simple attack heuristics .....	14
7.3.11 FAU_SAA.4 Complex attack heuristics.....	15
7.4 Security audit review (FAU_SAR) .....	15
7.4.1 Family Behaviour.....	15
7.4.2 Component levelling .....	15
7.4.3 Management of FAU_SAR.1 .....	15
7.4.4 Management of FAU_SAR.2, FAU_SAR.3 .....	15
7.4.5 Audit of FAU_SAR.1 .....	15
7.4.6 Audit of FAU_SAR.2 .....	16
7.4.7 Audit of FAU_SAR.3 .....	16

## ISO/IEC 15408-2:2008(E)

7.4.8	FAU_SAR.1 Audit review .....	16
7.4.9	FAU_SAR.2 Restricted audit review .....	16
7.4.10	FAU_SAR.3 Selectable audit review .....	16
7.5	Security audit event selection (FAU_SEL) .....	16
7.5.1	Family Behaviour .....	16
7.5.2	Component levelling .....	17
7.5.3	Management of FAU_SEL.1 .....	17
7.5.4	Audit of FAU_SEL.1 .....	17
7.5.5	FAU_SEL.1 Selective audit .....	17
7.6	Security audit event storage (FAU_STG) .....	17
7.6.1	Family Behaviour .....	17
7.6.2	Component levelling .....	17
7.6.3	Management of FAU_STG.1 .....	18
7.6.4	Management of FAU_STG.2 .....	18
7.6.5	Management of FAU_STG.3 .....	18
7.6.6	Management of FAU_STG.4 .....	18
7.6.7	Audit of FAU_STG.1, FAU_STG.2 .....	18
7.6.8	Audit of FAU_STG.3 .....	18
7.6.9	Audit of FAU_STG.4 .....	18
7.6.10	FAU_STG.1 Protected audit trail storage .....	18
7.6.11	FAU_STG.2 Guarantees of audit data availability .....	19
7.6.12	FAU_STG.3 Action in case of possible audit data loss .....	19
7.6.13	FAU_STG.4 Prevention of audit data loss .....	19
8	Class FCO: Communication .....	20
8.1	Non-repudiation of origin (FCO_NRO) .....	20
8.1.1	Family Behaviour .....	20
8.1.2	Component levelling .....	20
8.1.3	Management of FCO_NRO.1, FCO_NRO.2 .....	20
8.1.4	Audit of FCO_NRO.1 .....	20
8.1.5	Audit of FCO_NRO.2 .....	21
8.1.6	FCO_NRO.1 Selective proof of origin .....	21
8.1.7	FCO_NRO.2 Enforced proof of origin .....	21
8.2	Non-repudiation of receipt (FCO_NRR) .....	22
8.2.1	Family Behaviour .....	22
8.2.2	Component levelling .....	22
8.2.3	Management of FCO_NRR.1, FCO_NRR.2 .....	22
8.2.4	Audit of FCO_NRR.1 .....	22
8.2.5	Audit of FCO_NRR.2 .....	22
8.2.6	FCO_NRR.1 Selective proof of receipt .....	22
8.2.7	FCO_NRR.2 Enforced proof of receipt .....	23
9	Class FCS: Cryptographic support .....	24
9.1	Cryptographic key management (FCS_CKM) .....	24
9.1.1	Family Behaviour .....	24
9.1.2	Component levelling .....	24
9.1.3	Management of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 .....	25
9.1.4	Audit of FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 .....	25
9.1.5	FCS_CKM.1 Cryptographic key generation .....	25
9.1.6	FCS_CKM.2 Cryptographic key distribution .....	25
9.1.7	FCS_CKM.3 Cryptographic key access .....	25
9.1.8	FCS_CKM.4 Cryptographic key destruction .....	26
9.2	Cryptographic operation (FCS_COP) .....	26
9.2.1	Family Behaviour .....	26
9.2.2	Component levelling .....	26
9.2.3	Management of FCS_COP.1 .....	26
9.2.4	Audit of FCS_COP.1 .....	26
9.2.5	FCS_COP.1 Cryptographic operation .....	27
10	Class FDP: User data protection .....	27
10.1	Access control policy (FDP_ACC) .....	29

10.1.1	Family Behaviour.....	29
10.1.2	Component levelling .....	30
10.1.3	Management of FDP_ACC.1, FDP_ACC.2.....	30
10.1.4	Audit of FDP_ACC.1, FDP_ACC.2.....	30
10.1.5	FDP_ACC.1 Subset access control .....	30
10.1.6	FDP_ACC.2 Complete access control.....	30
10.2	Access control functions (FDP_ACF) .....	30
10.2.1	Family Behaviour.....	30
10.2.2	Component levelling .....	30
10.2.3	Management of FDP_ACF.1 .....	31
10.2.4	Audit of FDP_ACF.1 .....	31
10.2.5	FDP_ACF.1 Security attribute based access control .....	31
10.3	Data authentication (FDP_DAU).....	32
10.3.1	Family Behaviour.....	32
10.3.2	Component levelling .....	32
10.3.3	Management of FDP_DAU.1, FDP_DAU.2.....	32
10.3.4	Audit of FDP_DAU.1 .....	32
10.3.5	Audit of FDP_DAU.2.....	32
10.3.6	FDP_DAU.1 Basic Data Authentication.....	32
10.3.7	FDP_DAU.2 Data Authentication with Identity of Guarantor .....	33
10.4	Export from the TOE (FDP_ETC) .....	33
10.4.1	Family Behaviour.....	33
10.4.2	Component levelling .....	33
10.4.3	Management of FDP_ETC.1.....	33
10.4.4	Management of FDP_ETC.2.....	33
10.4.5	Audit of FDP_ETC.1, FDP_ETC.2.....	33
10.4.6	FDP_ETC.1 Export of user data without security attributes.....	34
10.4.7	FDP_ETC.2 Export of user data with security attributes.....	34
10.5	Information flow control policy (FDP_IFC) .....	34
10.5.1	Family Behaviour.....	34
10.5.2	Component levelling .....	35
10.5.3	Management of FDP_IFC.1, FDP_IFC.2.....	35
10.5.4	Audit of FDP_IFC.1, FDP_IFC.2.....	35
10.5.5	FDP_IFC.1 Subset information flow control .....	35
10.5.6	FDP_IFC.2 Complete information flow control.....	35
10.6	Information flow control functions (FDP_IFF).....	35
10.6.1	Family Behaviour.....	35
10.6.2	Component levelling .....	36
10.6.3	Management of FDP_IFF.1, FDP_IFF.2.....	36
10.6.4	Management of FDP_IFF.3, FDP_IFF.4, FDP_IFF.5.....	36
10.6.5	Management of FDP_IFF.6.....	36
10.6.6	Audit of FDP_IFF.1, FDP_IFF.2, FDP_IFF.5.....	36
10.6.7	Audit of FDP_IFF.3, FDP_IFF.4, FDP_IFF.6.....	37
10.6.8	FDP_IFF.1 Simple security attributes .....	37
10.6.9	FDP_IFF.2 Hierarchical security attributes .....	37
10.6.10	FDP_IFF.3 Limited illicit information flows.....	38
10.6.11	FDP_IFF.4 Partial elimination of illicit information flows .....	39
10.6.12	FDP_IFF.5 No illicit information flows.....	39
10.6.13	FDP_IFF.6 Illicit information flow monitoring.....	39
10.7	Import from outside of the TOE (FDP_ITC).....	39
10.7.1	Family Behaviour.....	39
10.7.2	Component levelling .....	39
10.7.3	Management of FDP_ITC.1, FDP_ITC.2.....	40
10.7.4	Audit of FDP_ITC.1, FDP_ITC.2.....	40
10.7.5	FDP_ITC.1 Import of user data without security attributes.....	40
10.7.6	FDP_ITC.2 Import of user data with security attributes .....	40
10.8	Internal TOE transfer (FDP_ITT).....	41
10.8.1	Family Behaviour.....	41
10.8.2	Component levelling .....	41
10.8.3	Management of FDP_ITT.1, FDP_ITT.2.....	41

## ISO/IEC 15408-2:2008(E)

10.8.4	Management of FDP_ITT.3, FDP_ITT.4 .....	42
10.8.5	Audit of FDP_ITT.1, FDP_ITT.2 .....	42
10.8.6	Audit of FDP_ITT.3, FDP_ITT.4 .....	42
10.8.7	FDP_ITT.1 Basic internal transfer protection .....	42
10.8.8	FDP_ITT.2 Transmission separation by attribute .....	42
10.8.9	FDP_ITT.3 Integrity monitoring .....	43
10.8.10	FDP_ITT.4 Attribute-based integrity monitoring .....	43
10.9	Residual information protection (FDP_RIP) .....	43
10.9.1	Family Behaviour .....	43
10.9.2	Component levelling .....	44
10.9.3	Management of FDP_RIP.1, FDP_RIP.2 .....	44
10.9.4	Audit of FDP_RIP.1, FDP_RIP.2 .....	44
10.9.5	FDP_RIP.1 Subset residual information protection .....	44
10.9.6	FDP_RIP.2 Full residual information protection .....	44
10.10	Rollback (FDP_ROL) .....	44
10.10.1	Family Behaviour .....	44
10.10.2	Component levelling .....	44
10.10.3	Management of FDP_ROL.1, FDP_ROL.2 .....	45
10.10.4	Audit of FDP_ROL.1, FDP_ROL.2 .....	45
10.10.5	FDP_ROL.1 Basic rollback .....	45
10.10.6	FDP_ROL.2 Advanced rollback .....	45
10.11	Stored data integrity (FDP_SDI) .....	46
10.11.1	Family Behaviour .....	46
10.11.2	Component levelling .....	46
10.11.3	Management of FDP_SDI.1 .....	46
10.11.4	Management of FDP_SDI.2 .....	46
10.11.5	Audit of FDP_SDI.1 .....	46
10.11.6	Audit of FDP_SDI.2 .....	46
10.11.7	FDP_SDI.1 Stored data integrity monitoring .....	46
10.11.8	FDP_SDI.2 Stored data integrity monitoring and action .....	47
10.12	Inter-TSF user data confidentiality transfer protection (FDP_UCT) .....	47
10.12.1	Family Behaviour .....	47
10.12.2	Component levelling .....	47
10.12.3	Management of FDP_UCT.1 .....	47
10.12.4	Audit of FDP_UCT.1 .....	47
10.12.5	FDP_UCT.1 Basic data exchange confidentiality .....	47
10.13	Inter-TSF user data integrity transfer protection (FDP_UIT) .....	48
10.13.1	Family Behaviour .....	48
10.13.2	Component levelling .....	48
10.13.3	Management of FDP_UIT.1, FDP_UIT.2, FDP_UIT.3 .....	48
10.13.4	Audit of FDP_UIT.1 .....	48
10.13.5	Audit of FDP_UIT.2, FDP_UIT.3 .....	48
10.13.6	FDP_UIT.1 Data exchange integrity .....	49
10.13.7	FDP_UIT.2 Source data exchange recovery .....	49
10.13.8	FDP_UIT.3 Destination data exchange recovery .....	49
11	Class FIA: Identification and authentication .....	50
11.1	Authentication failures (FIA_AFL) .....	51
11.1.1	Family Behaviour .....	51
11.1.2	Component levelling .....	51
11.1.3	Management of FIA_AFL.1 .....	52
11.1.4	Audit of FIA_AFL.1 .....	52
11.1.5	FIA_AFL.1 Authentication failure handling .....	52
11.2	User attribute definition (FIA_ATD) .....	52
11.2.1	Family Behaviour .....	52
11.2.2	Component levelling .....	52
11.2.3	Management of FIA_ATD.1 .....	52
11.2.4	Audit of FIA_ATD.1 .....	52
11.2.5	FIA_ATD.1 User attribute definition .....	53
11.3	Specification of secrets (FIA_SOS) .....	53

11.3.1	Family Behaviour.....	53
11.3.2	Component levelling .....	53
11.3.3	Management of FIA_SOS.1.....	53
11.3.4	Management of FIA_SOS.2.....	53
11.3.5	Audit of FIA_SOS.1, FIA_SOS.2 .....	53
11.3.6	FIA_SOS.1 Verification of secrets .....	53
11.3.7	FIA_SOS.2 TSF Generation of secrets .....	54
11.4	User authentication (FIA_UAU).....	54
11.4.1	Family Behaviour.....	54
11.4.2	Component levelling .....	54
11.4.3	Management of FIA_UAU.1.....	54
11.4.4	Management of FIA_UAU.2.....	55
11.4.5	Management of FIA_UAU.3, FIA_UAU.4, FIA_UAU.7 .....	55
11.4.6	Management of FIA_UAU.5.....	55
11.4.7	Management of FIA_UAU.6.....	55
11.4.8	Audit of FIA_UAU.1 .....	55
11.4.9	Audit of FIA_UAU.2 .....	55
11.4.10	Audit of FIA_UAU.3 .....	55
11.4.11	Audit of FIA_UAU.4 .....	56
11.4.12	Audit of FIA_UAU.5 .....	56
11.4.13	Audit of FIA_UAU.6 .....	56
11.4.14	Audit of FIA_UAU.7 .....	56
11.4.15	FIA_UAU.1 Timing of authentication .....	56
11.4.16	FIA_UAU.2 User authentication before any action .....	56
11.4.17	FIA_UAU.3 Unforgeable authentication .....	57
11.4.18	FIA_UAU.4 Single-use authentication mechanisms .....	57
11.4.19	FIA_UAU.5 Multiple authentication mechanisms.....	57
11.4.20	FIA_UAU.6 Re-authenticating .....	57
11.4.21	FIA_UAU.7 Protected authentication feedback.....	57
11.5	User identification (FIA_UID).....	58
11.5.1	Family Behaviour.....	58
11.5.2	Component levelling .....	58
11.5.3	Management of FIA_UID.1.....	58
11.5.4	Management of FIA_UID.2.....	58
11.5.5	Audit of FIA_UID.1, FIA_UID.2.....	58
11.5.6	FIA_UID.1 Timing of identification.....	58
11.5.7	FIA_UID.2 User identification before any action .....	59
11.6	User-subject binding (FIA_USB).....	59
11.6.1	Family Behaviour.....	59
11.6.2	Component levelling .....	59
11.6.3	Management of FIA_USB.1.....	59
11.6.4	Audit of FIA_USB.1.....	59
11.6.5	FIA_USB.1 User-subject binding .....	59
12	Class FMT: Security management.....	60
12.1	Management of functions in TSF (FMT_MOF).....	61
12.1.1	Family Behaviour.....	61
12.1.2	Component levelling .....	61
12.1.3	Management of FMT_MOF.1.....	61
12.1.4	Audit of FMT_MOF.1.....	62
12.1.5	FMT_MOF.1 Management of security functions behaviour .....	62
12.2	Management of security attributes (FMT_MSA).....	62
12.2.1	Family Behaviour.....	62
12.2.2	Component levelling .....	62
12.2.3	Management of FMT_MSA.1.....	62
12.2.4	Management of FMT_MSA.2.....	62
12.2.5	Management of FMT_MSA.3.....	63
12.2.6	Management of FMT_MSA.4.....	63
12.2.7	Audit of FMT_MSA.1.....	63
12.2.8	Audit of FMT_MSA.2.....	63

## ISO/IEC 15408-2:2008(E)

12.2.9	Audit of FMT_MSA.3	63
12.2.10	Audit of FMT_MSA.4	63
12.2.11	FMT_MSA.1 Management of security attributes	63
12.2.12	FMT_MSA.2 Secure security attributes	64
12.2.13	FMT_MSA.3 Static attribute initialisation	64
12.2.14	FMT_MSA.4 Security attribute value inheritance	64
12.3	Management of TSF data (FMT_MTD)	65
12.3.1	Family Behaviour	65
12.3.2	Component levelling	65
12.3.3	Management of FMT_MTD.1	65
12.3.4	Management of FMT_MTD.2	65
12.3.5	Management of FMT_MTD.3	65
12.3.6	Audit of FMT_MTD.1	65
12.3.7	Audit of FMT_MTD.2	65
12.3.8	Audit of FMT_MTD.3	65
12.3.9	FMT_MTD.1 Management of TSF data	65
12.3.10	FMT_MTD.2 Management of limits on TSF data	66
12.3.11	FMT_MTD.3 Secure TSF data	66
12.4	Revocation (FMT_REV)	66
12.4.1	Family Behaviour	66
12.4.2	Component levelling	66
12.4.3	Management of FMT_REV.1	66
12.4.4	Audit of FMT_REV.1	67
12.4.5	FMT_REV.1 Revocation	67
12.5	Security attribute expiration (FMT_SAE)	67
12.5.1	Family Behaviour	67
12.5.2	Component levelling	67
12.5.3	Management of FMT_SAE.1	67
12.5.4	Audit of FMT_SAE.1	67
12.5.5	FMT_SAE.1 Time-limited authorisation	67
12.6	Specification of Management Functions (FMT_SMF)	68
12.6.1	Family Behaviour	68
12.6.2	Component levelling	68
12.6.3	Management of FMT_SMF.1	68
12.6.4	Audit of FMT_SMF.1	68
12.6.5	FMT_SMF.1 Specification of Management Functions	68
12.7	Security management roles (FMT_SMR)	68
12.7.1	Family Behaviour	68
12.7.2	Component levelling	69
12.7.3	Management of FMT_SMR.1	69
12.7.4	Management of FMT_SMR.2	69
12.7.5	Management of FMT_SMR.3	69
12.7.6	Audit of FMT_SMR.1	69
12.7.7	Audit of FMT_SMR.2	69
12.7.8	Audit of FMT_SMR.3	69
12.7.9	FMT_SMR.1 Security roles	69
12.7.10	FMT_SMR.2 Restrictions on security roles	70
12.7.11	FMT_SMR.3 Assuming roles	70
13	Class FPR: Privacy	71
13.1	Anonymity (FPR_ANO)	71
13.1.1	Family Behaviour	71
13.1.2	Component levelling	71
13.1.3	Management of FPR_ANO.1, FPR_ANO.2	71
13.1.4	Audit of FPR_ANO.1, FPR_ANO.2	71
13.1.5	FPR_ANO.1 Anonymity	72
13.1.6	FPR_ANO.2 Anonymity without soliciting information	72
13.2	Pseudonymity (FPR_PSE)	72
13.2.1	Family Behaviour	72
13.2.2	Component levelling	72



13.2.3	Management of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3.....	72
13.2.4	Audit of FPR_PSE.1, FPR_PSE.2, FPR_PSE.3.....	72
13.2.5	FPR_PSE.1 Pseudonymity.....	73
13.2.6	FPR_PSE.2 Reversible pseudonymity .....	73
13.2.7	FPR_PSE.3 Alias pseudonymity .....	73
13.3	Unlinkability (FPR_UNL) .....	74
13.3.1	Family Behaviour.....	74
13.3.2	Component levelling .....	74
13.3.3	Management of FPR_UNL.1 .....	74
13.3.4	Audit of FPR_UNL.1 .....	74
13.3.5	FPR_UNL.1 Unlinkability.....	74
13.4	Unobservability (FPR_UNO).....	74
13.4.1	Family Behaviour.....	74
13.4.2	Component levelling .....	75
13.4.3	Management of FPR_UNO.1, FPR_UNO.2.....	75
13.4.4	Management of FPR_UNO.3.....	75
13.4.5	Management of FPR_UNO.4.....	75
13.4.6	Audit of FPR_UNO.1, FPR_UNO.2 .....	75
13.4.7	Audit of FPR_UNO.3.....	75
13.4.8	Audit of FPR_UNO.4.....	75
13.4.9	FPR_UNO.1 Unobservability .....	75
13.4.10	FPR_UNO.2 Allocation of information impacting unobservability.....	76
13.4.11	FPR_UNO.3 Unobservability without soliciting information.....	76
13.4.12	FPR_UNO.4 Authorised user observability .....	76
14	Class FPT: Protection of the TSF .....	76
14.1	Fail secure (FPT_FLS).....	77
14.1.1	Family Behaviour.....	77
14.1.2	Component levelling .....	78
14.1.3	Management of FPT_FLS.1.....	78
14.1.4	Audit of FPT_FLS.1 .....	78
14.1.5	FPT_FLS.1 Failure with preservation of secure state.....	78
14.2	Availability of exported TSF data (FPT_ITA).....	78
14.2.1	Family Behaviour.....	78
14.2.2	Component levelling .....	78
14.2.3	Management of FPT_ITA.1.....	78
14.2.4	Audit of FPT_ITA.1 .....	78
14.2.5	FPT_ITA.1 Inter-TSF availability within a defined availability metric.....	78
14.3	Confidentiality of exported TSF data (FPT_ITC) .....	79
14.3.1	Family Behaviour.....	79
14.3.2	Component levelling .....	79
14.3.3	Management of FPT_ITC.1.....	79
14.3.4	Audit of FPT_ITC.1 .....	79
14.3.5	FPT_ITC.1 Inter-TSF confidentiality during transmission.....	79
14.4	Integrity of exported TSF data (FPT_ITI).....	79
14.4.1	Family Behaviour.....	79
14.4.2	Component levelling .....	79
14.4.3	Management of FPT_ITI.1 .....	80
14.4.4	Management of FPT_ITI.2 .....	80
14.4.5	Audit of FPT_ITI.1 .....	80
14.4.6	Audit of FPT_ITI.2.....	80
14.4.7	FPT_ITI.1 Inter-TSF detection of modification.....	80
14.4.8	FPT_ITI.2 Inter-TSF detection and correction of modification.....	80
14.5	Internal TOE TSF data transfer (FPT_ITT).....	81
14.5.1	Family Behaviour.....	81
14.5.2	Component levelling .....	81
14.5.3	Management of FPT_ITT.1 .....	81
14.5.4	Management of FPT_ITT.2 .....	81
14.5.5	Management of FPT_ITT.3 .....	81
14.5.6	Audit of FPT_ITT.1, FPT_ITT.2.....	82