
**Technologies de l'information —
Techniques de sécurité — Critères
d'évaluation pour la sécurité TI —**

**Partie 2:
Composants fonctionnels de sécurité**

iTeh STANDARD PREVIEW
*Information technology — Security techniques — Evaluation criteria
for IT security —
Part 2: Security functional components*
(standards.iteh.ai)

[ISO/IEC 15408-2:2008](https://standards.iteh.ai/catalog/standards/sist/ab53d166-1c55-4a55-b9b3-6aa75658af21/iso-iec-15408-2-2008)

<https://standards.iteh.ai/catalog/standards/sist/ab53d166-1c55-4a55-b9b3-6aa75658af21/iso-iec-15408-2-2008>



iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 15408-2:2008](https://standards.iteh.ai/catalog/standards/sist/ab53d166-1c55-4a55-b9b3-6aa75658af21/iso-iec-15408-2-2008)

<https://standards.iteh.ai/catalog/standards/sist/ab53d166-1c55-4a55-b9b3-6aa75658af21/iso-iec-15408-2-2008>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2008

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos	xv
Introduction	xvii
1 Domaine d'application	1
2 Références normatives	1
3 Termes, définitions, symboles et abréviations	1
4 Vue d'ensemble	1
4.1 Organisation de la présente partie de l'ISO/IEC 15408	1
5 Modèle d'exigences fonctionnelles	2
6 Composants fonctionnels de sécurité	6
6.1 Vue d'ensemble	6
6.1.1 Structure des classes	6
6.1.2 Structure d'une famille	6
6.1.3 Structure d'un composant	8
6.2 Catalogue de composants	10
6.2.1 Mise en évidence des changements de composants	11
7 Classe FAU: Audit de sécurité	11
7.1 Réponse automatique de l'audit de sécurité (FAU_ARP)	11
7.1.1 Comportement de la famille	11
7.1.2 Classement des composants	12
7.1.3 Gestion de FAU_ARP1	12
7.1.4 Audit de FAU_ARP1	12
7.1.5 FAU_ARP1 Alarmes de sécurité	12
7.2 Génération de données de l'audit de sécurité (FAU_GEN)	12
7.2.1 Comportement de la famille	12
7.2.2 Classement des composants	12
7.2.3 Gestion de FAU_GEN.1, FAU_GEN.2	12
7.2.4 Audit de FAU_GEN.1, FAU_GEN.2	12
7.2.5 FAU_GEN.1 Génération de données d'audit	12
7.2.6 FAU_GEN.2 Lien avec l'identité de l'utilisateur	13
7.3 Analyse de l'audit de sécurité (FAU_SAA)	13
7.3.1 Comportement de la famille	13
7.3.2 Classement des composants	13
7.3.3 Gestion de FAU_SAA.1	14
7.3.4 Gestion de FAU_SAA.2	14
7.3.5 Gestion de FAU_SAA.3	14
7.3.6 Gestion de FAU_SAA.4	14
7.3.7 Audit de FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4	14
7.3.8 FAU_SAA.1 Analyse de violation potentielle	14
7.3.9 FAU_SAA.2 Détection d'anomalie basée sur un profil	15
7.3.10 FAU_SAA.3 Heuristique des attaques simples	15
7.3.11 FAU_SAA.4 Heuristique des attaques complexes	16
7.4 Revue de l'audit de sécurité (FAU_SAR)	16
7.4.1 Comportement de la famille	16
7.4.2 Classement des composants	16
7.4.3 Gestion de FAU_SAR.1	16
7.4.4 Gestion de FAU_SAR.2, FAU_SAR.3	17
7.4.5 Audit de FAU_SAR.1	17
7.4.6 Audit de FAU_SAR.2	17
7.4.7 Audit de FAU_SAR.3	17
7.4.8 FAU_SAR.1 Revue d'audit	17
7.4.9 FAU_SAR.2 Revue d'audit restreinte	17
7.4.10 FAU_SAR.3 Revue d'audit sélective	17

7.5	Sélection des événements de l'audit de sécurité (FAU_SEL).....	18
7.5.1	Comportement de la famille.....	18
7.5.2	Classement des composants.....	18
7.5.3	Gestion de FAU_SEL.1.....	18
7.5.4	Audit de FAU_SEL.1.....	18
7.5.5	FAU_SEL.1 Audit sélectif.....	18
7.6	Stockage d'événements de l'audit de sécurité (FAU_STG).....	18
7.6.1	Comportement de la famille.....	18
7.6.2	Classement des composants.....	19
7.6.3	Gestion de FAU_STG.1.....	19
7.6.4	Gestion de FAU_STG.2.....	19
7.6.5	Gestion de FAU_STG.3.....	19
7.6.6	Gestion de FAU_STG.4.....	19
7.6.7	Audit de FAU_STG.1, FAU_STG.2.....	19
7.6.8	Audit de FAU_STG.3.....	19
7.6.9	Audit de FAU_STG.4.....	19
7.6.10	FAU_STG.1 Stockage protégé de la trace d'audit.....	20
7.6.11	FAU_STG.2 Garanties de disponibilité des données d'audit.....	20
7.6.12	FAU_STG.3 Action en cas de perte possible de données d'audit.....	20
7.6.13	FAU_STG.4 Prévention des pertes de données d'audit.....	20
8	Classe FCO: Communication.....	21
8.1	Non-répudiation de l'origine (FCO_NRO).....	21
8.1.1	Comportement de la famille.....	21
8.1.2	Classement des composants.....	21
8.1.3	Gestion de FCO_NRO.1, FCO_NRO.2.....	21
8.1.4	Audit de FCO_NRO.1.....	21
8.1.5	Audit de FCO_NRO.2.....	22
8.1.6	FCO_NRO.1 Preuve sélective de l'origine.....	22
8.1.7	FCO_NRO.2 Preuve systématique de l'origine.....	22
8.2	Non-répudiation de la réception (FCO_NRR).....	23
8.2.1	Comportement de la famille.....	23
8.2.2	Classement des composants.....	23
8.2.3	Gestion de FCO_NRR.1, FCO_NRR.2.....	23
8.2.4	Audit de FCO_NRR.1.....	23
8.2.5	Audit de FCO_NRR.2.....	23
8.2.6	FCO_NRR.1 Preuve sélective de la réception.....	23
8.2.7	FCO_NRR.2 Preuve systématique de la réception.....	24
9	Classe FCS: Support cryptographique.....	24
9.1	Gestion de clés cryptographiques (FCS_CKM).....	25
9.1.1	Comportement de la famille.....	25
9.1.2	Classement des composants.....	25
9.1.3	Gestion de FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4.....	25
9.1.4	Audit de FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4.....	26
9.1.5	FCS_CKM.1 Génération de clés cryptographiques.....	26
9.1.6	FCS_CKM.2 Distribution de clés cryptographiques.....	26
9.1.7	FCS_CKM.3 Accès aux clés cryptographiques.....	26
9.1.8	FCS_CKM.4 Destruction de clés cryptographiques.....	27
9.2	Opération cryptographique (FCS_COP).....	27
9.2.1	Comportement de la famille.....	27
9.2.2	Classement des composants.....	27
9.2.3	Gestion de FCS_COP.1.....	27
9.2.4	Audit de FCS_COP.1.....	27
9.2.5	FCS_COP.1 Opération cryptographique.....	28
10	Classe FDP: Protection des données utilisateur.....	28
10.1	Politique de contrôle d'accès (FDP_ACC).....	30
10.1.1	Comportement de la famille.....	30
10.1.2	Classement des composants.....	31

10.1.3	Gestion de FDP_ACC.1, FDP_ACC.2	31
10.1.4	Audit de FDP_ACC.1, FDP_ACC.2	31
10.1.5	FDP_ACC.1 Contrôle d'accès partiel	31
10.1.6	FDP_ACC.2 Contrôle d'accès complet	31
10.2	Fonctions de contrôle d'accès (FDP_ACF)	31
10.2.1	Comportement de la famille	31
10.2.2	Classement des composants	32
10.2.3	Gestion de FDP_ACF.1	32
10.2.4	Audit de FDP_ACF.1	32
10.2.5	FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité	32
10.3	Authentification de données (FDP_DAU)	33
10.3.1	Comportement de la famille	33
10.3.2	Classement des composants	33
10.3.3	Gestion de FDP_DAU.1, FDP_DAU.2	33
10.3.4	Audit de FDP_DAU.1	33
10.3.5	Audit de FDP_DAU.2	33
10.3.6	FDP_DAU.1 Authentification de données élémentaire	33
10.3.7	FDP_DAU.2 Authentification de données avec identité du garant	34
10.4	Exportation depuis la TOE (FDP_ETC)	34
10.4.1	Comportement de la famille	34
10.4.2	Classement des composants	34
10.4.3	Gestion de FDP_ETC.1	34
10.4.4	Gestion de FDP_ETC.2	34
10.4.5	Audit de FDP_ETC.1, FDP_ETC.2	35
10.4.6	FDP_ETC.1 Exportation de données de l'utilisateur sans attributs de sécurité	35
10.4.7	FDP_ETC.2 Exportation de données de l'utilisateur avec attributs de sécurité	35
10.5	Politique de contrôle de flux d'information (FDP_IFC)	36
10.5.1	Comportement de la famille	36
10.5.2	Classement des composants	36
10.5.3	Gestion de FDP_IFC.1, FDP_IFC.2	36
10.5.4	Audit de FDP_IFC.1, FDP_IFC.2	36
10.5.5	FDP_IFC.1 Contrôle de flux d'information partiel	36
10.5.6	FDP_IFC.2 Contrôle de flux d'information complet	37
10.6	Fonctions de contrôle de flux d'information (FDP_IFF)	37
10.6.1	Comportement de la famille	37
10.6.2	Classement des composants	37
10.6.3	Gestion de FDP_IFF.1, FDP_IFF.2	38
10.6.4	Gestion de FDP_IFF.3, FDP_IFF.4, FDP_IFF.5	38
10.6.5	Gestion de FDP_IFF.6	38
10.6.6	Audit de FDP_IFF.1, FDP_IFF.2, FDP_IFF.5	38
10.6.7	Audit de FDP_IFF.3, FDP_IFF.4, FDP_IFF.6	38
10.6.8	FDP_IFF.1 Attributs de sécurité simples	38
10.6.9	FDP_IFF.2 Attributs de sécurité hiérarchiques	39
10.6.10		
	FDP_IFF.3 Flux d'information illicites limités	40
10.6.11		
	FDP_IFF.4 Élimination partielle des flux d'information illicites	40
10.6.12		
	FDP_IFF.5 Aucun flux d'information illicite	41
10.6.13		
	FDP_IFF.6 Contrôle des flux d'information illicites	41
10.7	Importation depuis une zone hors du contrôle de la TSF (FDP_ITC)	41
10.7.1	Comportement de la famille	41
10.7.2	Classement des composants	41
10.7.3	Gestion de FDP_ITC.1, FDP_ITC.2	41
10.7.4	Audit de FDP_ITC.1, FDP_ITC.2	41

10.7.5	FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité.....	42
10.7.6	FDP_ITC.2 Importation de données de l'utilisateur avec attributs de sécurité.....	42
10.8	Transfert interne à la TOE (FDP_ITT).....	43
10.8.1	Comportement de la famille.....	43
10.8.2	Classement des composants.....	43
10.8.3	Gestion de FDP_ITT.1, FDP_ITT.2.....	43
10.8.4	Gestion de FDP_ITT.3, FDP_ITT.4.....	43
10.8.5	Audit de FDP_ITT.1, FDP_ITT.2.....	44
10.8.6	Audit de FDP_ITT.3, FDP_ITT.4.....	44
10.8.7	FDP_ITT.1 Protection élémentaire d'un transfert interne.....	44
10.8.8	FDP_ITT.2 Séparation de données au cours d'une transmission en fonction d'attributs.....	44
10.8.9	FDP_ITT.3 Contrôle de l'intégrité.....	45
10.8.10	
	FDP_ITT.4 Contrôle de l'intégrité basé sur des attributs.....	45
10.9	Protection des informations résiduelles (FDP_RIP).....	45
10.9.1	Comportement de la famille.....	45
10.9.2	Classement des composants.....	46
10.9.3	Gestion de FDP_RIP.1, FDP_RIP.2.....	46
10.9.4	Audit de FDP_RIP.1, FDP_RIP.2.....	46
10.9.5	FDP_RIP.1 Protection partielle des informations résiduelles.....	46
10.9.6	FDP_RIP.2 Protection totale des informations résiduelles.....	46
10.10	Annulation (FDP_ROL).....	46
10.10.1	Comportement de la famille.....	46
10.10.2	
	Classement des composants.....	47
10.10.3	
	Gestion de FDP_ROL.1, FDP_ROL.2.....	47
10.10.4	Audit de FDP_ROL.1, FDP_ROL.2.....	47
10.10.5	
	FDP_ROL.1 Annulation élémentaire.....	47
10.10.6	FDP_ROL.2 Annulation avancée.....	47
10.11	Intégrité des données stockées (FDP_SDI).....	48
10.11.1	Comportement de la famille.....	48
10.11.2	
	Classement des composants.....	48
10.11.3	
	Gestion de FDP_SDI.1.....	48
10.11.4	Gestion de FDP_SDI.2.....	48
10.11.5	
	Audit de FDP_SDI.1.....	48
10.11.6	Audit de FDP_SDI.2.....	49
10.11.7	FDP_SDI.1 Contrôle de l'intégrité des données stockées.....	49
10.11.8	
	FDP_SDI.2 Contrôle de l'intégrité des données stockées et action à entreprendre.....	49
10.12	Protection de la confidentialité des données utilisateur lors d'un transfert inter-TSF (FDP_UCT).....	49
10.12.1	
	Comportement de la famille.....	49
10.12.2	
	Classement des composants.....	49
10.12.3	
	Gestion de FDP_UCT.1.....	50
10.12.4	
	Audit de FDP_UCT.1.....	50
10.12.5	
	FDP_UCT.1 Confidentialité élémentaire lors d'un échange de données.....	50

10.13	Protection de l'intégrité des données de l'utilisateur lors d'un transfert inter-TSF (FDP_UIT).....	50
10.13.1	Comportement de la famille.....	50
10.13.2	
	Classement des composants.....	50
10.13.3	
	Gestion de FDP_UIT.1, FDP_UIT.2, FDP_UIT.3.....	51
10.13.4	
	Audit de FDP_UIT.1.....	51
10.13.5	
	Audit de FDP_UIT.2, FDP_UIT.3.....	51
10.13.6	
	FDP_UIT.1 Intégrité lors d'un échange de données.....	51
10.13.7	FDP_UIT.2 Reconstitution grâce à l'émetteur lors d'un échange de données.....	52
10.13.8	
	FDP_UIT.3 Reconstitution par le destinataire lors d'un échange de données.....	52
11	Classe FIA: Identification et authentification.....	52
11.1	Échecs de l'authentification (FIA_AFL).....	53
11.1.1	Comportement de la famille.....	53
11.1.2	Classement des composants.....	53
11.1.3	Gestion de FIA_AFL.1.....	54
11.1.4	Audit de FIA_AFL.1.....	54
11.1.5	FIA_AFL.1 Traitement des échecs d'authentification.....	54
11.2	Définition des attributs de l'utilisateur (FIA_ATD).....	54
11.2.1	Comportement de la famille.....	54
11.2.2	Classement des composants.....	54
11.2.3	Gestion de FIA_ATD.1.....	55
11.2.4	Audit de FIA_ATD.1.....	55
11.2.5	FIA_ATD.1 Définition des attributs de l'utilisateur.....	55
11.3	Spécification des secrets (FIA_SOS).....	55
11.3.1	Comportement de la famille.....	55
11.3.2	Classement des composants.....	55
11.3.3	Gestion de FIA_SOS.1.....	55
11.3.4	Gestion de FIA_SOS.2.....	55
11.3.5	Audit de FIA_SOS.1, FIA_SOS.2.....	55
11.3.6	FIA_SOS.1 Vérification des secrets.....	56
11.3.7	FIA_SOS.2 Génération de secrets par la TSF.....	56
11.4	Authentification de l'utilisateur (FIA_UAU).....	56
11.4.1	Comportement de la famille.....	56
11.4.2	Classement des composants.....	56
11.4.3	Gestion de FIA_UAU.1.....	57
11.4.4	Gestion de FIA_UAU.2.....	57
11.4.5	Gestion de FIA_UAU.3, FIA_UAU.4, FIA_UAU.7.....	57
11.4.6	Gestion de FIA_UAU.5.....	57
11.4.7	Gestion de FIA_UAU.6.....	57
11.4.8	Audit de FIA_UAU.1.....	57
11.4.9	Audit de FIA_UAU.2.....	57
11.4.10	Audit de FIA_UAU.3.....	58
11.4.11	Audit de FIA_UAU.4.....	58
11.4.12	
	Audit de FIA_UAU.5.....	58
11.4.13	
	Audit de FIA_UAU.6.....	58
11.4.14	Audit de FIA_UAU.7.....	58
11.4.15	
	FIA_UAU.1 Synchronisation de l'authentification.....	58
11.4.16	FIA_UAU.2 Authentification de l'utilisateur avant toute action.....	58
11.4.17	FIA_UAU.3 Authentification infalsifiable.....	59

11.4.18	FIA_UAU.4 Mécanismes d'authentification à usage unique.....	59
11.4.19	FIA_UAU.5 Mécanismes d'authentification multiples.....	59
11.4.20	
	FIA_UAU.6 Réauthentification.....	59
11.4.21	
	FIA_UAU.7 Retour d'information sur l'authentification protégée.....	60
11.5	Identification d'un utilisateur (FIA_UID).....	60
11.5.1	Comportement de la famille.....	60
11.5.2	Classement des composants.....	60
11.5.3	Gestion de FIA_UID.1.....	60
11.5.4	Gestion de FIA_UID.2.....	60
11.5.5	Audit de FIA_UID.1, FIA_UID.2.....	60
11.5.6	FIA_UID.1 Synchronisation de l'identification.....	61
11.5.7	FIA_UID.2 Identification de l'utilisateur avant toute action.....	61
11.6	Lien utilisateur-sujet (FIA_USB).....	61
11.6.1	Comportement de la famille.....	61
11.6.2	Classement des composants.....	61
11.6.3	Gestion de FIA_USB.1.....	61
11.6.4	Audit de FIA_USB.1.....	61
11.6.5	FIA_USB.1 Lien utilisateur-sujet.....	62
12	Classe FMT: Gestion de la sécurité.....	62
12.1	Gestion des fonctions de la TSF (FMT_MOF).....	63
12.1.1	Comportement de la famille.....	63
12.1.2	Classement des composants.....	63
12.1.3	Gestion de FMT_MOF.1.....	64
12.1.4	Audit de FMT_MOF.1.....	64
12.1.5	FMT_MOF.1 Gestion du comportement des fonctions de sécurité.....	64
12.2	Gestion des attributs de sécurité (FMT_MSA).....	64
12.2.1	Comportement de la famille.....	64
12.2.2	Classement des composants.....	64
12.2.3	Gestion de FMT_MSA.1.....	64
12.2.4	Gestion de FMT_MSA.2.....	65
12.2.5	Gestion de FMT_MSA.3.....	65
12.2.6	Gestion de FMT_MSA.4.....	65
12.2.7	Audit de FMT_MSA.1.....	65
12.2.8	Audit de FMT_MSA.2.....	65
12.2.9	Audit de FMT_MSA.3.....	65
12.2.10	
	Audit de FMT_MSA.4.....	65
12.2.11	
	FMT_MSA.1 Gestion des attributs de sécurité.....	65
12.2.12	
	FMT_MSA.2 Attributs de sécurité sûrs.....	66
12.2.13	
	FMT_MSA.3 Initialisation statique d'attribut.....	66
12.2.14	
	FMT_MSA.4 Héritage des valeurs d'attribut de sécurité.....	66
12.3	Gestion des données de la TSF (FMT_MTD).....	67
12.3.1	Comportement de la famille.....	67
12.3.2	Classement des composants.....	67
12.3.3	Gestion de FMT_MTD.1.....	67
12.3.4	Gestion de FMT_MTD.2.....	67
12.3.5	Gestion de FMT_MTD.3.....	67
12.3.6	Audit de FMT_MTD.1.....	67
12.3.7	Audit de FMT_MTD.2.....	67
12.3.8	Audit de FMT_MTD.3.....	68
12.3.9	FMT_MTD.1 Gestion des données de la TSF.....	68

12.3.10	FMT_MTD.2 Gestion des limites sur les données de la TSF	68
12.3.11	FMT_MTD.3 Données sûres de la TSF	68
12.4	Révocation (FMT_REV)	69
12.4.1	Comportement de la famille	69
12.4.2	Classement des composants	69
12.4.3	Gestion de FMT_REV.1	69
12.4.4	Audit de FMT_REV.1	69
12.4.5	FMT_REV.1 Révocation	69
12.5	Expiration des attributs de sécurité (FMT_SAE)	69
12.5.1	Comportement de la famille	69
12.5.2	Classement des composants	69
12.5.3	Gestion de FMT_SAE.1	70
12.5.4	Audit de FMT_SAE.1	70
12.5.5	FMT_SAE.1 Autorisation limitée dans le temps	70
12.6	Spécification des fonctions de gestion (FMT_SMF)	70
12.6.1	Comportement de la famille	70
12.6.2	Classement des composants	70
12.6.3	Gestion de FMT_SMF.1	71
12.6.4	Audit de FMT_SMF.1	71
12.6.5	FMT_SMF.1 Spécification des fonctions de gestion	71
12.7	Rôles de gestion de la sécurité (FMT_SMR)	71
12.7.1	Comportement de la famille	71
12.7.2	Classement des composants	71
12.7.3	Gestion de FMT_SMR.1	71
12.7.4	Gestion de FMT_SMR.2	71
12.7.5	Gestion de FMT_SMR.3	71
12.7.6	Audit de FMT_SMR.1	72
12.7.7	Audit de FMT_SMR.2	72
12.7.8	Audit de FMT_SMR.3	72
12.7.9	FMT_SMR.1 Rôles de sécurité	72
12.7.10	FMT_SMR.2 Restrictions sur les rôles de sécurité	72
12.7.11	FMT_SMR.3 Endossement de rôles	73
13	Classe FPR: Protection de la vie privée	73
13.1	Anonymat (FPR_ANO)	73
13.1.1	Comportement de la famille	73
13.1.2	Classement des composants	74
13.1.3	Gestion de FPR_ANO.1, FPR_ANO.2	74
13.1.4	Audit de FPR_ANO.1, FPR_ANO.2	74
13.1.5	FPR_ANO.1 Anonymat	74
13.1.6	FPR_ANO.2 Anonymat sans sollicitation d'informations	74
13.2	Pseudonymat (FPR_PSE)	74
13.2.1	Comportement de la famille	74
13.2.2	Classement des composants	75
13.2.3	Gestion de FPR_PSE.1, FPR_PSE.2, FPR_PSE.3	75
13.2.4	Audit de FPR_PSE.1, FPR_PSE.2, FPR_PSE.3	75
13.2.5	FPR_PSE.1 Pseudonymat	75
13.2.6	FPR_PSE.2 Pseudonymat réversible	75
13.2.7	FPR_PSE.3 Pseudonymat par alias	76
13.3	Impossibilité d'établir un lien (FPR_UNL)	76
13.3.1	Comportement de la famille	76
13.3.2	Classement des composants	76
13.3.3	Gestion de FPR_UNL.1	77
13.3.4	Audit de FPR_UNL.1	77
13.3.5	FPR_UNL.1 Impossibilité d'établir un lien	77
13.4	Non-observabilité (FPR_UNO)	77
13.4.1	Comportement de la famille	77

13.4.2	Classement des composants.....	77
13.4.3	Gestion de FPR_UNO.1, FPR_UNO.2.....	77
13.4.4	Gestion de FPR_UNO.3.....	77
13.4.5	Gestion de FPR_UNO.4.....	78
13.4.6	Audit de FPR_UNO.1, FPR_UNO.2.....	78
13.4.7	Audit de FPR_UNO.3.....	78
13.4.8	Audit de FPR_UNO.4.....	78
13.4.9	FPR_UNO.1 Non-observabilité.....	78
13.4.10	
	FPR_UNO.2 Affectation d'informations impactant la non-observabilité.....	78
13.4.11	
	FPR_UNO.3 Non-observabilité sans sollicitation d'informations.....	78
13.4.12	
	FPR_UNO.4 Observabilité par un utilisateur autorisé.....	79
14	Classe FPT: Protection de la TSF.....	79
14.1	Mode sûr après défaillance (FPT_FLS).....	80
14.1.1	Comportement de la famille.....	80
14.1.2	Classement des composants.....	80
14.1.3	Gestion de FPT_FLS.1.....	81
14.1.4	Audit de FPT_FLS.1.....	81
14.1.5	FPT_FLS.1 Défaillance avec préservation d'un état sûr.....	81
14.2	Disponibilité des données de la TSF exportées (FPT_ITA).....	81
14.2.1	Comportement de la famille.....	81
14.2.2	Classement des composants.....	81
14.2.3	Gestion de FPT_ITA.1.....	81
14.2.4	Audit de FPT_ITA.1.....	81
14.2.5	FPT_ITA.1 Disponibilité inter-TSF dans la limite d'une métrique de disponibilité définie.....	81
14.3	Confidentialité des données de la TSF exportées (FPT_ITC).....	82
14.3.1	Comportement de la famille.....	82
14.3.2	Classement des composants.....	82
14.3.3	Gestion de FPT_ITC.1.....	82
14.3.4	Audit de FPT_ITC.1.....	82
14.3.5	FPT_ITC.1 Confidentialité inter-TSF pendant une transmission.....	82
14.4	Intégrité des données de la TSF exportées (FPT_ITI).....	82
14.4.1	Comportement de la famille.....	82
14.4.2	Classement des composants.....	82
14.4.3	Gestion de FPT_ITI.1.....	83
14.4.4	Gestion de FPT_ITI.2.....	83
14.4.5	Audit de FPT_ITI.1.....	83
14.4.6	Audit de FPT_ITI.2.....	83
14.4.7	FPT_ITI.1 Détection inter-TSF d'une modification.....	83
14.4.8	FPT_ITI.2 Détection et correction inter-TSF d'une modification.....	84
14.5	Transfert de données de la TSF à l'intérieur de la TOE (FPT_ITT).....	84
14.5.1	Comportement de la famille.....	84
14.5.2	Classement des composants.....	84
14.5.3	Gestion de FPT_ITT.1.....	84
14.5.4	Gestion de FPT_ITT.2.....	84
14.5.5	Gestion de FPT_ITT.3.....	85
14.5.6	Audit de FPT_ITT.1, FPT_ITT.2.....	85
14.5.7	Audit de FPT_ITI.3.....	85
14.5.8	FDP_ITT.1 Protection élémentaire des données de la TSF lors d'un transfert interne.....	85
14.5.9	FPT_ITT.2 Séparation des données de la TSF pendant un transfert.....	85
14.5.10	FPT_ITT.3 Surveillance de l'intégrité des données de la TSF.....	86
14.6	Protection physique de la TSF (FPT_PHP).....	86
14.6.1	Comportement de la famille.....	86
14.6.2	Classement des composants.....	86

14.6.3	Gestion de FPT_PHP.1	86
14.6.4	Gestion de FPT_PHP.2	86
14.6.5	Gestion de FPT_PHP.3	87
14.6.6	Audit de FPT_PHP.1	87
14.6.7	Audit de FPT_PHP.2	87
14.6.8	Audit de FPT_PHP.3	87
14.6.9	FPT_PHP.1 Détection passive d'une attaque physique	87
14.6.10	FPT_PHP.2 Notification d'une attaque physique	87
14.6.11	FPT_PHP.3 Résistance à une attaque physique	88
14.7	Reprise sûre (FPT_RCV)	88
14.7.1	Comportement de la famille	88
14.7.2	Classement des composants	88
14.7.3	Gestion de FPT_RCV.1	88
14.7.4	Gestion de FPT_RCV.2, FPT_RCV.3	89
14.7.5	Gestion de FPT_RCV.4	89
14.7.6	Audit de FPT_RCV.1, FPT_RCV.2, FPT_RCV.3	89
14.7.7	Audit de FPT_RCV.4	89
14.7.8	FPT_RCV.1 Reprise manuelle	89
14.7.9	FPT_RCV.2 Reprise automatisée	89
14.7.10	FPT_RCV.3 Reprise automatisée sans perte induite	90
14.7.11	FPT_RCV.4 Reprise de fonction	90
14.8	Détection de rejeu (FPT_RPL)	90
14.8.1	Comportement de la famille	90
14.8.2	Classement des composants	91
14.8.3	Gestion de FPT_RPL.1	91
14.8.4	Audit de FPT_RPL.1	91
14.8.5	FPT_RPL.1 Détection de rejeu	91
14.9	Protocole de synchronisation d'états (FPT_SSP)	91
14.9.1	Comportement de la famille	91
14.9.2	Classement des composants	91
14.9.3	Gestion de FPT_SSP.1, FPT_SSP.2	92
14.9.4	Audit de FPT_SSP.1, FPT_SSP.2	92
14.9.5	FPT_SSP.1 Accusé de réception de confiance simple	92
14.9.6	FPT_SSP.2 Accusé de réception de confiance mutuel	92
14.10	Horodatage (FPT_STM)	92
14.10.1	Comportement de la famille	92
14.10.2	Classement des composants	92
14.10.3	Gestion de FPT_STM.1	92
14.10.4	Audit de FPT_STM.1	93
14.10.5	FPT_STM.1 Horodatage fiable	93
14.11	Cohérence des données de la TSF inter-TSF (FPT_TDC)	93
14.11.1	Comportement de la famille	93
14.11.2	Classement des composants	93
14.11.3	Gestion de FPT_TDC.1	93
14.11.4	Audit de FPT_TDC.1	93
14.11.5	FPT_TDC.1 Cohérence élémentaire des données de la TSF inter-TSF	93
14.12	Test d'entités externes (FPT_TEE)	94
14.12.1	Comportement de la famille	94
14.12.2	Classement des composants	94
14.12.3	Gestion de FPT_TEE.1	94
14.12.4	Audit de FPT_TEE.1	94
14.12.5	FPT_TEE.1 Test d'entités externes	94
14.13	Cohérence de la reproduction des données de la TSF à l'intérieur de la TOE (FPT_TRC)	95

14.13.1	Comportement de la famille.....	95
14.13.2	
	Classement des composants.....	95
14.13.3	
	Gestion de FPT_TRC.1	95
14.13.4	Audit de FPT_TRC.1.....	95
14.13.5	
	FPT_TRC.1 Cohérence interne de la TSF	95
14.14	Autotest de la TSF (FPT_TST).....	96
14.14.1	Comportement de la famille.....	96
14.14.2	Classement des composants.....	96
14.14.3	Gestion de FPT_TST.1	96
14.14.4	Audit de FPT_TST.1.....	96
14.14.5	FPT_TST.1 Test de la TSF	96
15	Classe FRU: Utilisation des ressources.....	97
15.1	Tolérance aux pannes (FRU_FLT).....	97
15.1.1	Comportement de la famille.....	97
15.1.2	Classement des composants.....	97
15.1.3	Gestion de FRU_FLT.1, FRU_FLT.2	97
15.1.4	Audit de FRU_FLT.1	98
15.1.5	Audit de FRU_FLT.2	98
15.1.6	FRU_FLT.1 Tolérance aux pannes avec mode dégradé	98
15.1.7	FRU_FLT.2 Tolérance aux pannes limitée.....	98
15.2	Priorité de service (FRU_PRS).....	98
15.2.1	Comportement de la famille.....	98
15.2.2	Classement des composants.....	98
15.2.3	Gestion de FRU_PRS.1, FRU_PRS.2	99
15.2.4	Audit de FRU_PRS.1, FRU_PRS.2	99
15.2.5	FRU_PRS.1 Priorité de service limitée.....	99
15.2.6	FRU_PRS.2 Priorité de service totale.....	99
15.3	Allocation des ressources (FRU_RSA).....	99
15.3.1	Comportement de la famille.....	99
15.3.2	Classement des composants.....	100
15.3.3	Gestion de FRU_RSA.1	100
15.3.4	Gestion de FRU_RSA.2	100
15.3.5	Audit de FRU_RSA.1, FRU_RSA.2.....	100
15.3.6	FRU_RSA.1 Quotas maximaux.....	100
15.3.7	FRU_RSA.2 Quotas minimaux et maximaux.....	100
16	Classe FTA: Accès à la TOE.....	101
16.1	Limitation de la portée des attributs sélectionnables (FTA_LSA).....	101
16.1.1	Comportement de la famille.....	101
16.1.2	Classement des composants.....	101
16.1.3	Gestion de FTA_LSA.1	101
16.1.4	Audit de FTA_LSA.1.....	102
16.1.5	FTA_LSA.1 Limitation de la portée des attributs sélectionnables.....	102
16.2	Limitation du nombre de sessions parallèles (FTA_MCS).....	102
16.2.1	Comportement de la famille.....	102
16.2.2	Classement des composants.....	102
16.2.3	Gestion de FTA_MCS.1	102
16.2.4	Gestion de FTA_MCS.2.....	102
16.2.5	Audit de FTA_MCS.1, FTA_MCS.2	102
16.2.6	FTA_MCS.1 Limitation élémentaire du nombre de sessions parallèles.....	103
16.2.7	FTA_MCS.2 Limitation du nombre de sessions parallèles par les attributs de l'utilisateur.....	103
16.3	Verrouillage et arrêt de session (FTA_SSL).....	103
16.3.1	Comportement de la famille.....	103
16.3.2	Classement des composants.....	103

16.3.3	Gestion de FTA_SSL.1	104
16.3.4	Gestion de FTA_SSL.2	104
16.3.5	Gestion de FTA_SSL.3	104
16.3.6	Gestion de FTA_SSL.4	104
16.3.7	Audit de FTA_SSL.1, FTA_SSL.2	104
16.3.8	Audit de FTA_SSL.3	104
16.3.9	Audit de FTA_SSL.4	104
16.3.10	FTA_SSL.1 Verrouillage de session, initié par la TSF	104
16.3.11	FTA_SSL.2 Verrouillage de session, initié par l'utilisateur	105
16.3.12	FTA_SSL.3 Clôture de session, initiée par la TSF	105
16.3.13	FTA_SSL.4 Clôture de session, initiée par l'utilisateur	105
16.4	Messages d'accès à la TOE (FTA_TAB)	106
16.4.1	Comportement de la famille	106
16.4.2	Classement des composants	106
16.4.3	Gestion de FTA_TAB.1	106
16.4.4	Audit de FTA_TAB.1	106
16.4.5	FTA_TAB.1 Messages par défaut d'accès à la TOE	106
16.5	Historique des accès à la TOE (FTA_TAH)	106
16.5.1	Comportement de la famille	106
16.5.2	Classement des composants	106
16.5.3	Gestion de FTA_TAH.1	106
16.5.4	Audit de FTA_TAH.1	106
16.5.5	FTA_TAH.1 Historique des accès à la TOE	107
16.6	Établissement d'une session de la TOE (FTA_TSE)	107
16.6.1	Comportement de la famille	107
16.6.2	Classement des composants	107
16.6.3	Gestion de FTA_TSE.1	107
16.6.4	Audit de FTA_TSE.1	107
16.6.5	FTA_TSE.1 Établissement d'une session de la TOE	107
17	Classe FTP: Chemin et canaux de confiance	108
17.1	Canal de confiance inter-TSF (FTP_ITC)	108
17.1.1	Comportement de la famille	108
17.1.2	Classement des composants	108
17.1.3	Gestion de FTP_ITC.1	109
17.1.4	Audit de FTP_ITC.1	109
17.1.5	FTP_ITC.1 Canal de confiance inter-TSF	109
17.2	Chemin de confiance (FTP_TRP)	109
17.2.1	Comportement de la famille	109
17.2.2	Classement des composants	109
17.2.3	Gestion de FTP_TRP.1	110
17.2.4	Audit de FTP_TRP.1	110
17.2.5	FTP_TRP.1 Chemin de confiance	110
	Annexe A (normative) Notes d'application sur les exigences fonctionnelles de sécurité	111
	Annexe B (normative) Classes, familles et composants fonctionnels	119
	Annexe C (normative) Classe FAU: Audit de sécurité	120
	Annexe D (normative) Classe FCO: Communication	133
	Annexe E (normative) Classe FCS: Support cryptographique	138
	Annexe F (normative) Classe FDP: Protection des données utilisateur	143
	Annexe G (normative) Classe FIA: Identification et authentification	171
	Annexe H (normative) Classe FMT: Gestion de la sécurité	181

Annexe I (normative) Classe FPR: Protection de la vie privée	191
Annexe J (normative) Classe FPT: Protection de la TSF	203
Annexe K (normative) Classe FRU: Utilisation des ressources	221
Annexe L (normative) Classe FTA: Accès à la TOE	226
Annexe M (normative) Classe FTP: Chemin et canaux de confiance	233

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 15408-2:2008](https://standards.iteh.ai/catalog/standards/sist/ab53d166-1c55-4a55-b9b3-6aa75658af21/iso-iec-15408-2-2008)

<https://standards.iteh.ai/catalog/standards/sist/ab53d166-1c55-4a55-b9b3-6aa75658af21/iso-iec-15408-2-2008>

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/IEC, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*. Le texte identique de l'ISO/IEC 15408 est publié par les organisations commanditaires du projet Critères communs sous le titre Common Criteria for Information Technology Security Evaluation (Critères Communs pour l'évaluation de la sécurité des technologies de l'information). La source XML commune aux deux publications peut être obtenue à l'adresse <http://www.oc.ccn.cni.es/xml>.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 15408-2:2005), qui a fait l'objet d'une révision technique.

L'ISO/IEC 15408 comprend les parties suivantes, présentées sous le titre général *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI*:

- Partie 1: Introduction et modèle général
- Partie 2: Composants fonctionnels de sécurité
- Partie 3: Exigences d'assurance de sécurité

La présente version corrigée de l'ISO/IEC 15408-2:2008 incorpore diverses corrections éditoriales portant essentiellement sur FDP.UTC, FDP.UIT, FDP.ACF.1.4, FAU_SEL.1.1, FPT_TST.1, FDP_ITT.4, et FPT_TEE.

Mention légale

Les organismes gouvernementaux énumérés ci-après ont contribué à l'élaboration de cette version des critères communs pour l'évaluation de la sécurité des technologies de l'information (Common Criteria for Information Technology Security Evaluations). En tant que co-titulaires du copyright relatif aux critères communs pour l'évaluation de la sécurité des technologies de l'information, version 3.1, Parties 1 à 3 (appelés CC 3.1), ils accordent par la présente une licence non exclusive à l'ISO/IEC pour utiliser les CC 3.1 dans la poursuite de l'élaboration et de la tenue à jour de la norme internationale ISO/IEC 15408. Ces organismes gouvernementaux conservent toutefois le droit d'utiliser, de copier, de distribuer, de traduire ou de modifier les CC 3.1 comme ils l'entendent.

Australie/Nouvelle-Zélande: The Defence Signals Directorate and the Government Communications Security Bureau, respectivement;