Critères communs pour l'évaluation de la sécurité des technologies de l'information

Partie 2 : Exigences fonctionnelles de sécurité

Août 1999

Version 2.1

CCIMB-99-032

Avant-propos

L'ISO (International Organisation for Standardisation, l'organisation internationale pour la normalisation) et l'IEC (International Electrotechnical Commission, la commission internationale électrotechnique) forment le système dédié à la normalisation mondiale. Les organisations nationales qui sont membres de l'ISO ou de l'IEC participent au développement des normes internationales par le biais de comités techniques établis par les organisations respectives pour traiter de domaines particuliers d'activités techniques. Les comités techniques de l'ISO et de l'IEC collaborent dans les domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, prennent également part au travail.

Dans le domaine des technologies de l'information, l'ISO et l'IEC ont établi un comité technique commun, l'ISO/IEC JTC 1. Les normes internationales provisoires (Draft International Standards) adoptées par le comité technique commun sont mises en circulation dans les organisations nationales pour être soumises à un vote. La publication comme norme internationale (International Standard) nécessite l'approbation d'au moins 75% des organisations nationales ayant voté.

La norme internationale ISO/IEC 15408 a été préparée par le comité technique commun ISO/IEC JTC 1, Technologies de l'Information, en collaboration avec le comité d'édition des critères communs (Common Criteria Implementation Board), une entité qui regroupe des membres des organisations commanditaires du projet Critères Communs. Le texte identique à la norme ISO/IEC 15408 est publié par les organisations commanditaires du projet Critères Communs sous le titre *Common Criteria for Information Technology Security Evaluation, version 2.0 (Critères Communs pour l'évaluation de la sécurité des technologies de l'information, version 2.0).* Des informations supplémentaires concernant le projet Critères Communs ainsi que les coordonnées des organisations commanditaires, sont fournies dans l'annexe A de la partie 1.

La norme ISO/IEC 15408, sous le titre général *Critères Communs pour l'évaluation de la sécurité des technologies de l'information,* comprend les parties suivantes :

Partie 1 : Introduction et modèle général

Partie 2 : Exigences fonctionnelles de sécurité

Partie 3 : Exigences d'assurance de sécurité

La présente NOTICE À CARACTÈRE LÉGAL a été introduite dans toutes les parties de la norme ISO/IEC 15408 sur demande :
Les sept organisations gouvernementales (collectivement dénommées les "organisations commanditaires du projet Critères Communs") citées ci-dessous et identifiées plus complètement dans l'Annexe A de la Partie 1, en tant que détentrices communes du copyright du document Critères Communs pour l'évaluation de la sécurité des technologies de l'information (Common Criteria for Information Technology Security Evaluation), version 2.0, comprenant les Parties 1 à 3 (appelé "CC 2.0"), accordent par la présente notice à l'ISO/IEC la licence non exclusive d'utilisation du document CC 2.0 pour le développement de la norme internationale ISO/IEC 15408. Cependant, les organisations commanditaires du projet Critères Communs conservent le droit d'utiliser, copier, distribuer ou modifier le document CC 2.0 quand elles le jugent bon.

- Allemagne :	*Bundesamt für Sicherheit in der Informationstechnik*
- Canada :	*Communications Security Establishment*
- Etats-Unis :	*National Institute of Standards and Technology*
- Etats-Unis :	*National Security Agency*
- France :	*Service Central de la Sécurité des Systèmes d'Information*
- Pays-Bas :	*Netherlands National Communications Security Agency*
- Royaume Uni :	*Communications-Electronics Security Group*

Table des matières

Liste des figures

1 Introduction

1.1 Champ d'application

1 Les composants fonctionnels de sécurité, tels qu'ils sont définis dans la présente partie 2 des CC, constituent la base des exigences fonctionnelles de sécurité des TI de la TOE qui sont exprimées dans un profil de protection (PP) ou une cible de sécurité (ST). Ces exigences décrivent le comportement de sécurité souhaité qui est attendu d'une cible d'évaluation (TOE) et sont destinées à satisfaire aux objectifs de sécurité tels qu'ils sont formulés dans un PP ou une ST. Ces exigences décrivent les propriétés de sécurité que les utilisateurs peuvent détecter par interaction directe avec la TOE (i.e. entrées, sorties) ou par la réponse de la TOE à des stimuli.

2 Les composants fonctionnels de sécurité expriment les exigences de sécurité destinées à contrer les menaces dans l'environnement opérationnel supposé de la TOE, ou à couvrir toutes les politiques de sécurité organisationnelles et les hypothèses identifiées.

3 L'audience de la partie 2 des CC comprend les utilisateurs, les développeurs et les évaluateurs de systèmes et de produits TI sûrs. Le chapitre 3 de la partie 1 des CC donne des informations supplémentaires sur l'audience visée des CC et sur l'utilisation des CC par les groupes qui constituent l'audience visée. Ces groupes peuvent utiliser cette partie des CC de la façon suivante :

- Les utilisateurs qui se servent de la partie 2 des CC lorsqu'ils choisissent des composants afin d'exprimer les exigences fonctionnelles pour satisfaire aux objectifs de sécurité exprimés dans un PP ou une ST. Le chapitre 4.3 de la partie 1 des CC fournit des informations plus détaillées concernant les relations entre les objectifs de sécurité et les exigences de sécurité.

- Les développeurs qui, en construisant une TOE, répondent aux exigences de sécurité réelles ou perçues des utilisateurs, et qui peuvent trouver dans cette partie des CC une méthode normalisée pour assimiler ces exigences. Ils peuvent également utiliser le contenu de cette partie des CC comme une base pour définir de façon plus approfondie les fonctions de sécurité et les mécanismes de la TOE qui satisfont à ces exigences.

- Les évaluateurs qui utilisent les exigences fonctionnelles définies dans cette partie des CC pour contrôler que les exigences fonctionnelles de la TOE exprimées dans le PP ou la ST satisfont aux objectifs de sécurité TI, et que toutes les dépendances sont prises en compte et se révèlent avoir été satisfaites. Les évaluateurs devraient aussi utiliser cette partie des CC pour aider à déterminer si une TOE donnée satisfait aux exigences formulées.

1.1.1 Extension et maintenance des exigences fonctionnelles

4 Les CC et les exigences fonctionnelles de sécurité associées décrites ici ne sont pas censés constituer une réponse définitive à tous les problèmes de sécurité des TI. En

fait, les CC offrent un ensemble d'exigences fonctionnelles de sécurité bien définies, qui peuvent être utilisées pour créer des produits ou des systèmes de confiance reflétant les besoins du marché. Ces exigences fonctionnelles de sécurité sont présentées comme l'état de l'art pour la spécification et l'évaluation d'exigences.

5 Cette partie des CC ne prétend pas inclure toutes les exigences fonctionnelles de sécurité possibles, mais plutôt contenir celles qui sont connues et acceptées comme ayant de la valeur par les auteurs de la partie 2 des CC au moment de la parution de ces derniers.

6 Comme la compréhension et les besoins des utilisateurs peuvent changer, il sera nécessaire de maintenir les exigences fonctionnelles de cette partie des CC. Il a été envisagé que certains auteurs de PP ou de ST pourraient avoir des besoins de sécurité qui ne sont pas (encore) couverts par les composants d'exigences fonctionnelles de la partie 2 des CC. Dans ce cas, l'auteur du PP ou de la ST peut envisager d'utiliser des exigences fonctionnelles ne figurant pas dans les CC (possibilité qui est appelée extensibilité), comme cela est expliqué dans les annexes B et C de la partie 1 des CC.

1.2 Organisation de la partie 2

7 Le chapitre 1 contient l'introduction de la partie 2 des CC.

8 Le chapitre 2 introduit le catalogue des composants fonctionnels de la partie 2 des CC tandis que les chapitres 3 à 13 décrivent les classes fonctionnelles.

9 L'annexe A donne des informations complémentaires qui sont intéressantes pour les utilisateurs potentiels des composants fonctionnels, comprenant une table complète des références croisées des dépendances relatives aux composants fonctionnels.

10 Les annexes B à M contiennent les notes d'application relatives aux classes fonctionnelles. Elles constituent un répertoire d'informations pouvant aider les utilisateurs de cette partie des CC, en particulier pour appliquer les opérations adéquates et sélectionner les informations appropriées pour l'audit ou la documentation.

11 Les auteurs de PP ou de ST devraient consulter le chapitre 2 de la partie 1 des CC pour prendre connaissance des structures, règles et conseils adéquats :

- le chapitre 2 de la partie 1 des CC définit les termes utilisés dans les CC ;
- l'annexe B de la partie 1 des CC définit la structure des PP ;
- l'annexe C de la partie 1 des CC définit la structure des ST.

1.3 Paradigme des exigences fonctionnelles

12 Cette section décrit le paradigme utilisé dans les exigences fonctionnelles de sécurité de la présente partie 2 des CC. Les figures 1.1 et 1.2 représentent certains des concepts clés du paradigme. Cette section donne des commentaires relatifs à ces figures et aux autres concepts clés qui ne sont pas représentés. Les concepts clés commentés sont mis en évidence en caractères gras ou italiques. La présente section n'est pas destinée à remplacer ou redéfinir un terme quelconque du glossaire des CC du chapitre 2 de la partie 1 des CC.

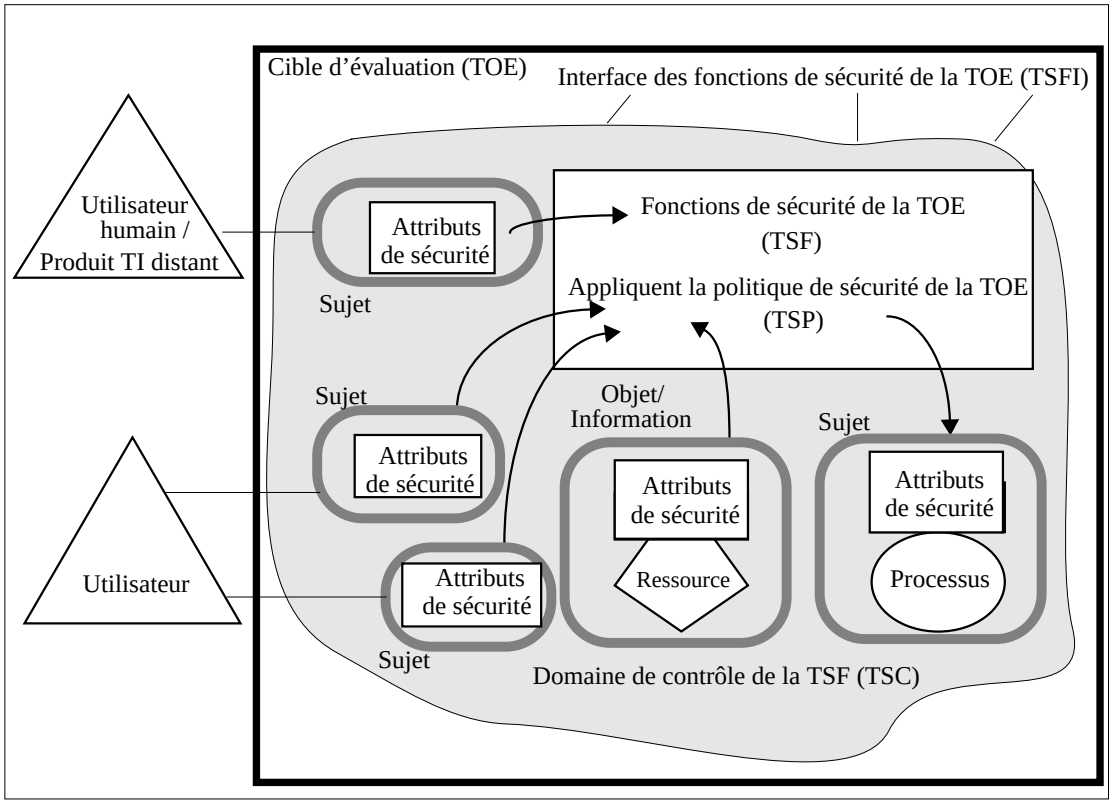


Figure 1.1 - Paradigme des exigences fonctionnelles de sécurité (TOE monolithique)

13 La présente partie 2 des CC est un catalogue d'exigences fonctionnelles de sécurité qui peuvent être spécifiées pour une ***cible d'évaluation (TOE)***. Une TOE est un produit ou système TI (avec ses guides d'utilisation et d'administration) contenant des ressources telles que des moyens de stockage électroniques (e.g. des disques), des périphériques (e.g. des imprimantes), et des capacités de calcul (e.g. du temps CPU), qui peut être utilisé pour traiter et stocker des informations et fait l'objet d'une évaluation.

14 L'évaluation de la TOE est destinée principalement à garantir qu'une ***politique de sécurité de la TOE (TSP)*** définie est appliquée aux ressources de la TOE. La TSP définit les règles par lesquelles la TOE régit l'accès à ses ressources, et donc aux informations et services qu'elle contrôle.

15 La TSP est constituée à son tour de diverses ***politiques d'une fonction de sécurité (SFP)***. Chacune des SFP a un domaine de contrôle qui définit les sujets, objets et opérations sous le contrôle de la SFP. La SFP est implémentée par une ***fonction de sécurité (SF)***, dont les mécanismes mettent en œuvre la politique et fournissent les moyens nécessaires.

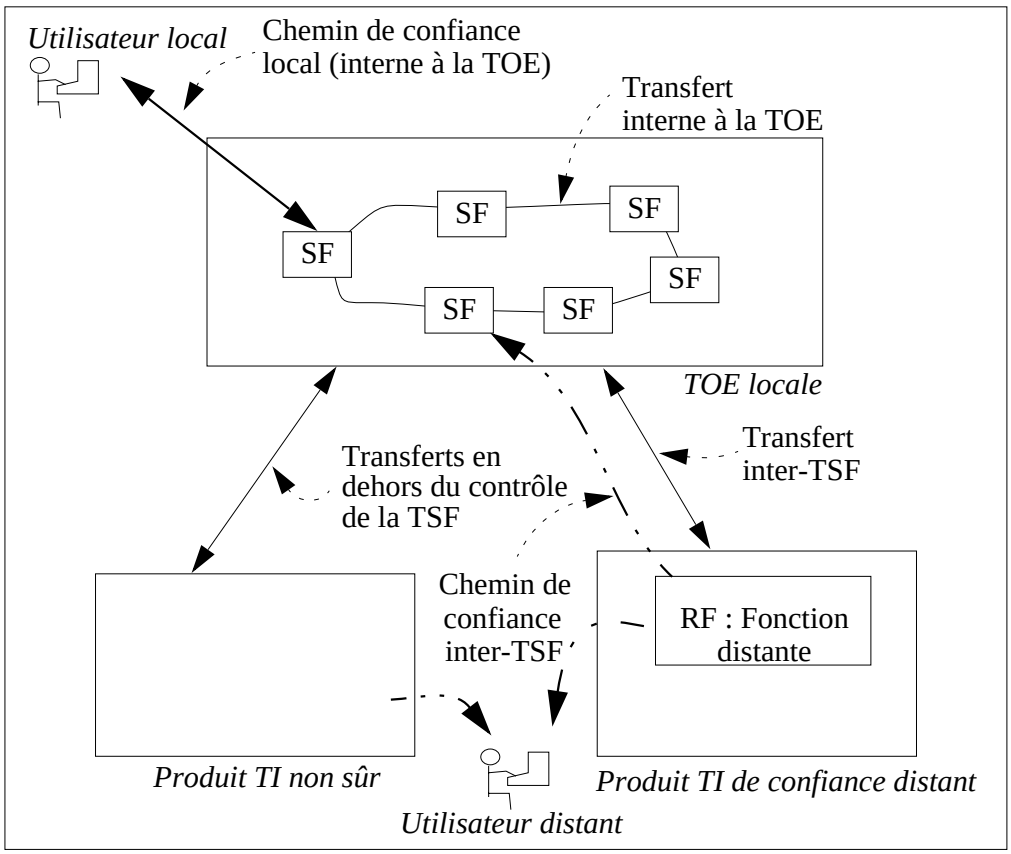


Figure 1.2 - Diagramme des fonctions de sécurité dans une TOE distribuée

16 Les parties d'une TOE auxquelles on doit se fier pour l'application correcte de la TSP sont référencées collectivement sous l'appellation de ***fonctions de sécurité de la TOE (TSF)***. La TSF est constituée par tous les matériels, logiciels et micro-programmes d'une TOE auxquels on fait confiance directement ou indirectement pour la mise en œuvre de la sécurité.

17 Un ***moniteur de référence*** est une machine abstraite qui applique les politiques de contrôle d'accès d'une TOE. Un ***mécanisme de validation de référence*** est une implémentation du concept de moniteur de référence qui possède les propriétés suivantes : résistant aux intrusions, systématiquement appelé et suffisamment simple pour faire l'objet d'une analyse et de tests approfondis. La ***TSF*** peut consister en un mécanisme de validation de référence ou en d'autres fonctions de sécurité nécessaires au fonctionnement de la TOE.

18 La TOE peut être un produit monolithique contenant des matériels, micro-programmes et logiciels.

19 Une TOE peut aussi être un produit distribué qui est constitué en interne de plusieurs parties séparées. Chacune de ces parties de la TOE fournit à cette dernière un service spécifique et est connectée à toutes les autres parties de la TOE via un ***canal de communication interne***. Ce canal peut être réduit à un bus de processeur ou peut englober un réseau interne à la TOE.

20 Lorsque la TOE est constituée de plusieurs parties, chacune d'entre elles peut contenir sa propre partie de la TSF qui échange des données de l'utilisateur et des données de la TSF via des canaux de communication internes avec d'autres parties de la TSF. Cette interaction est appelée ***transfert interne à la TOE***. Dans ce cas, les parties séparées de la TSF forment de façon abstraite la TSF composée, qui met en œuvre la TSP.

21 Les interfaces de la TOE peuvent être internes à la TOE, ou bien elles peuvent permettre des interactions avec d'autres produits TI via ***des canaux de communication externes***. Ces interactions externes avec d'autres produits TI peuvent revêtir deux formes :

a) La politique de sécurité du "produit TI de confiance distant" et les TSP des TOE locales ont été coordonnées sur le plan organisationnel et évaluées. Les échanges d'informations dans cette situation sont appelés ***transferts inter-TSF***, car ils ont lieu entre les TSF de produits de confiance distincts.

b) Le produit TI distant peut ne pas avoir été évalué, et est alors représenté dans la figure 1.2 sous l'appellation de "produit TI non sûr" ; par conséquent sa politique de sécurité n'est pas connue. Les échanges d'informations dans cette situation sont appelés ***transferts en dehors du contrôle de la TSF***, car il n'existe pas de TSF (ou les caractéristiques de sa politique ne sont pas connues) pour le produit TI distant.

22 L'ensemble des interactions qui peuvent avoir lieu avec une TOE ou à l'intérieur d'une TOE et qui sont soumises aux règles de la TSP est appelé le ***champ de contrôle de la TSF (TSC)***. Le TSC englobe un ensemble défini d'interactions basées sur des sujets, objets et opérations au sein de la TOE, mais il n'est pas nécessaire qu'il comprenne toutes les ressources d'une TOE.

23 L'ensemble des interfaces, qu'elles soient interactives (interface homme-machine) ou programmatiques (interface entre programmes d'application), permettant d'accéder aux ressources de la TSF ou d'obtenir des informations de la TSF, est appelé ***interface de la TSF (TSFI)***. La TSFI définit les frontières des fonctions de la TOE qui permettent la mise en œuvre de la TSP.

24 Les utilisateurs sont situés à l'extérieur de la TOE, et par conséquent en dehors du TSC. Cependant, afin de pouvoir demander des services à la TOE, les utilisateurs dialoguent avec la TOE par la TSFI. Il existe deux types d'utilisateurs intéressants pour les exigences fonctionnelles de sécurité de la partie 2 des CC : ***les utilisateurs (humains)*** et ***les entités TI externes***. Les utilisateurs humains sont à leur tour

différenciés en ***utilisateurs locaux***, ce qui signifie qu'ils dialoguent directement avec la TOE via les dispositifs propres à la TOE (e.g. des stations de travail) et en ***utilisateurs distants***, ce qui signifie qu'ils dialoguent indirectement avec la TOE par l'intermédiaire d'un autre produit TI.

25 Une plage de temps pendant laquelle les utilisateurs dialoguent avec la TSF est appelée une ***session*** utilisateur. L'établissement de sessions utilisateur peut être contrôlé sur la base de divers moyens incluant par exemple : l'authentification de l'utilisateur, la date et l'heure, la méthode d'accès à la TOE et le nombre de sessions concurrentes autorisées par utilisateur.

26 La présente partie 2 des CC utilise le terme ***autorisé*** pour désigner un utilisateur qui possède les droits ou les privilèges nécessaires pour exécuter une opération. Le terme ***utilisateur autorisé*** indique par conséquent qu'un utilisateur est autorisé à exécuter une opération comme définie dans la TSP.

27 Pour exprimer des exigences qui demandent la séparation des tâches d'administration, les composants fonctionnels de sécurité concernés de la partie 2 des CC (faisant partie de la famille FMT_SMR) stipulent de façon explicite que des ***rôles*** administratifs sont requis. Un rôle est un ensemble de règles prédéfini qui établit les interactions autorisées entre un utilisateur et la TOE. Une TOE peut supporter la définition d'un nombre quelconque de rôles. Par exemple, les rôles liés à l'exploitation sûre d'une TOE peuvent inclure le rôle "administrateur de l'audit" et le rôle "administrateur des comptes utilisateur".

28 Les TOE contiennent des ressources qui peuvent être utilisées pour le traitement et le stockage d'informations. Le but principal de la TSF est l'application complète et correcte de la TSP sur les ressources et les informations que contrôle la TOE.

29 Les ressources de la TOE peuvent être structurées et utilisées de plusieurs façons différentes. Cependant, la partie 2 des CC fait une distinction particulière qui permet la spécification de propriétés de sécurité souhaitées. Toutes les entités qui peuvent être créées à partir des ressources peuvent être classées de deux manières différentes. Les entités peuvent être actives, ce qui signifie qu'elles sont à l'origine d'actions qui surviennent à l'intérieur de la TOE et des opérations devant être exécutées sur des informations ; ou bien les entités peuvent être passives, ce qui signifie qu'elles sont soit le contenant à partir duquel des informations sont issues, soit le contenant dans lequel des informations sont stockées.

30 Les entités actives sont appelés des ***sujets***. Plusieurs types de sujets peuvent exister dans une TOE :

a) ceux qui agissent pour le compte d'un utilisateur autorisé et qui sont soumis à toutes les règles de la TSP (e.g. des processus UNIX) ;

b) ceux qui agissent comme un processus fonctionnel spécifique qui peut à son tour agir pour le compte de plusieurs utilisateurs (e.g. des fonctions comme celles qui pourraient être trouvées dans les architectures client-serveur) ;

c) ou ceux qui agissent comme une partie de la TOE elle-même (e.g. des processus de confiance).

31 La partie 2 des CC traite de l'application de la TSP à plusieurs types de sujets tels que ceux cités ci-dessus.

32 Les entités passives (i.e. les contenants d'informations) sont désignées dans les exigences fonctionnelles de sécurité de la partie 2 des CC sous l'appellation d'***objets***. Les objets constituent les cibles d'opérations qui peuvent être exécutées par des sujets. Dans le cas où un sujet (une entité active) est la cible d'une opération (e.g. une communication inter-processus), un sujet peut aussi être traité de la même façon qu'un objet.

33 Les objets peuvent contenir des ***informations***. Ce concept est nécessaire pour spécifier les politiques de contrôle de flux d'information comme cela est traité dans la classe FDP.

34 Les utilisateurs, sujets, informations et objets possèdent certains ***attributs*** qui contiennent des informations permettant à la TOE de se comporter correctement. Certains attributs, tels que les noms de fichier, peuvent n'avoir qu'un but informatif (i.e. améliorer le confort de l'utilisateur de la TOE) alors que d'autres, tels que les informations de contrôle d'accès, peuvent exister spécifiquement pour appliquer la TSP. Ces derniers attributs sont généralement référencés sous l'appellation d'"***attributs de sécurité"***. Le terme attribut sera utilisé à titre de simplification dans cette partie des CC à la place de l'expression "attribut de sécurité", à moins qu'il n'en soit indiqué autrement. Cependant, quel que soit le but prévu pour les informations contenues dans les attributs, il peut être nécessaire de disposer de contrôles sur les attributs comme cela est exigé par la TSP.

35 Les données dans une TOE sont classées comme étant, soit des données utilisateur, soit des données de la TSF. La figure 1.3 représente ces relations. Les ***données de l'utilisateur*** sont des informations stockées dans les ressources de la TOE qui peuvent être traitées par des utilisateurs en conformité avec la TSP et au sujet desquelles la TSF n'accorde aucune signification particulière. Par exemple, le contenu d'un message électronique constitue une donnée utilisateur. Les ***données de la TSF*** sont des informations utilisées par la TSF pour prendre des décisions relevant de la TSP. Les utilisateurs peuvent agir sur les données de la TSF si cela est permis par la TSP. Les attributs de sécurité, les données d'authentification et les éléments d'une liste de contrôle d'accès sont des exemples de données de la TSF.

36 Il existe plusieurs SFP qui s'appliquent à la protection de données, telles que les ***SFP de contrôle d'accès*** et les ***SFP de contrôle de flux d'information***. Les mécanismes qui implémentent les SFP de contrôle d'accès basent les décisions de leur politique sur les attributs des sujets, objets et opérations à l'intérieur du champ de contrôle. Ces attributs sont utilisés par l'ensemble des règles qui régissent les opérations que les sujets peuvent effectuer sur les objets.

37 Les mécanismes qui implémentent les SFP de contrôle de flux d'information basent les décisions de leur politique sur les attributs des sujets et des informations à l'intérieur du champ de contrôle et sur l'ensemble des règles qui régissent les

opérations que les sujets peuvent effectuer sur les informations. Les attributs d'une information, qui peuvent être associés avec les attributs du contenant (ou peuvent ne pas l'être, comme dans le cas d'une base de données multi-niveaux) demeurent avec l'informations quand celle-ci est déplacée.

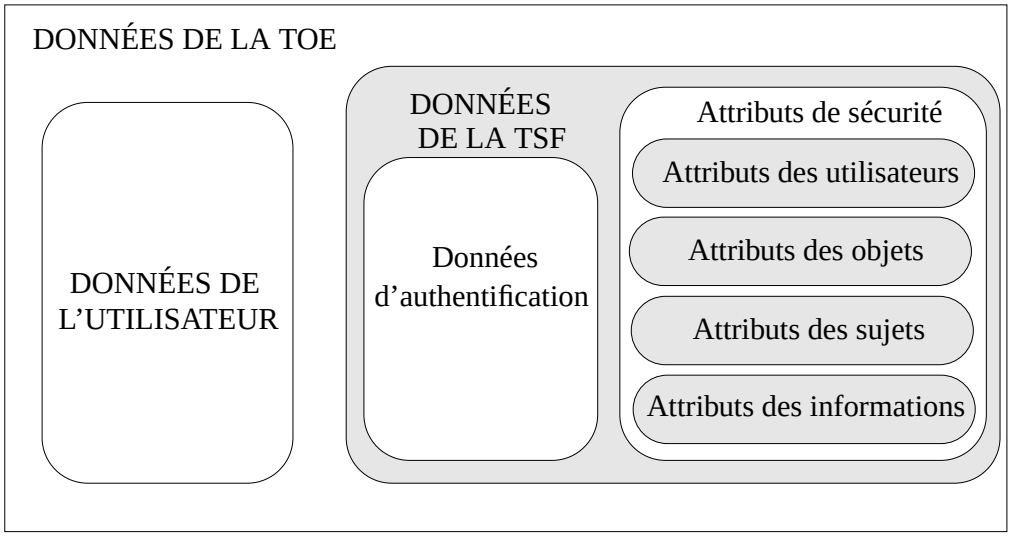


Figure 1.3 - Relations entre les données utilisateur et les données de la TSF

38 Deux types spécifiques de données de la TSF qui sont traités dans la partie 2 des CC peuvent éventuellement être confondus. Il s'agit des ***données d'authentification*** et des ***secrets***.

39 Les données d'authentification sont utilisées pour contrôler l'identité annoncée par un utilisateur qui demande des services à une TOE. La forme la plus commune des données d'authentification est le mot de passe qui, pour constituer un mécanisme de sécurité efficace, doit être tenu secret. Cependant, toutes les formes de données d'authentification n'ont pas besoin d'être tenues secrètes. Les dispositifs d'authentification biométriques (e.g. les lecteurs d'empreintes digitales, les scanners de la rétine) ne se fondent pas sur le fait que les données sont tenues secrètes, mais plutôt sur le fait que ces données n'appartiennent qu'à un seul utilisateur et ne peuvent pas être contrefaites.

40 Le terme "secrets", tel qu'il est utilisé dans les exigences fonctionnelles de la partie 2 des CC, tout en étant applicable aux données d'authentification, est également censé être applicable à d'autres types de données qui doivent être tenues secrètes pour appliquer une SFP particulière. Par exemple, un mécanisme de canal de confiance qui est basé sur la cryptographie pour préserver la confidentialité des informations transmises par le canal, ne peut pas être plus fort que la méthode utilisée pour protéger les clés cryptographiques d'une divulgation non autorisée.

41 Par conséquent, certaines données d'authentification, mais pas toutes, doivent être tenues secrètes et certains secrets, mais pas tous, sont utilisés comme données d'authentification. La figure 1.4 montre ces relations entre les secrets et les données

d'authentification. La figure indique les types de données que l'on trouve habituellement dans les données d'authentification et les secrets.

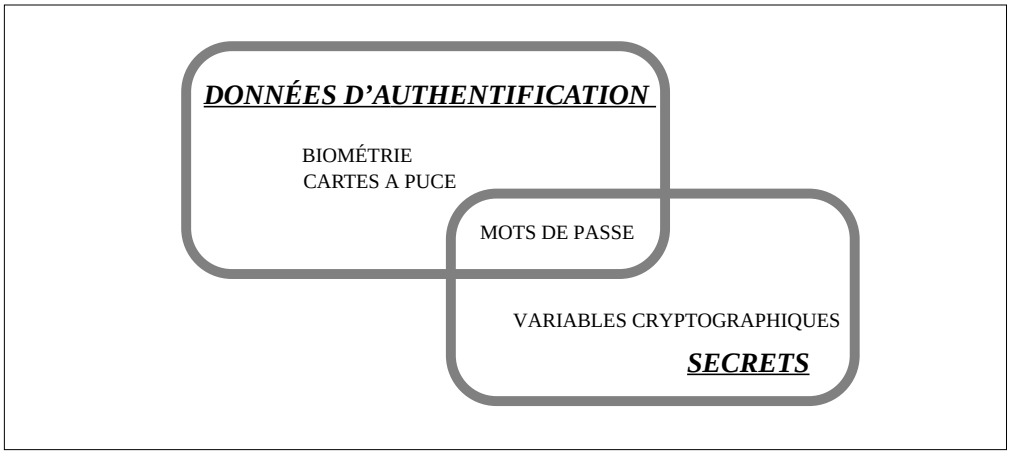


Figure 1.4 - Relations entre "données d'authentification" et "secrets"

2 Composants fonctionnels de sécurité

2.1 Vue d'ensemble

42 La présente section définit le contenu et la présentation des exigences fonctionnelles des CC et offre une assistance relative à l'organisation des exigences pour l'introduction de nouveaux composants dans une ST. Les exigences fonctionnelles sont exprimées dans des classes, familles et composants.

2.1.1 Structure d'une classe

43 La figure 2.1 illustre la structure d'une classe fonctionnelle sous forme de diagramme. Chaque classe fonctionnelle comprend une rubrique "Nom de la classe", une rubrique "Introduction de la classe" et une ou plusieurs familles fonctionnelles.

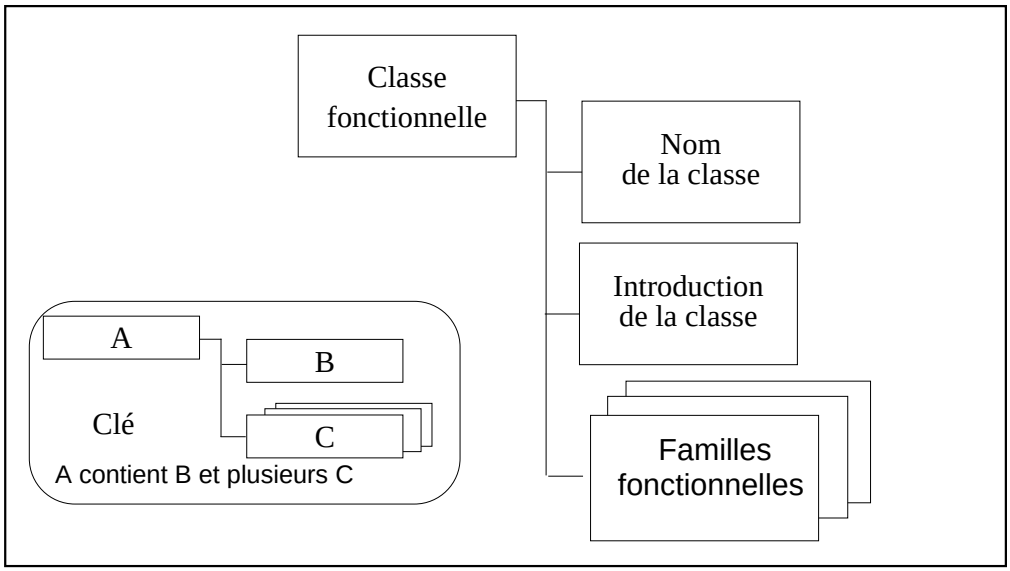


Figure 2.1 - Structure d'une classe fonctionnelle

2.1.1.1 Nom de la classe

44 La rubrique "Nom de la classe" donne les informations nécessaires pour identifier et classer une classe fonctionnelle. Chaque classe fonctionnelle a un nom unique. Les informations utilisées pour la classification consistent en une abréviation sur trois caractères. Cette abréviation est utilisée pour spécifier l'abréviation du nom des familles de cette classe.

2.1.1.2 Introduction de la classe

45 La rubrique “Introduction de la classe” exprime le but ou l’approche commune des familles de cette classe pour satisfaire aux objectifs de sécurité. La définition des classes fonctionnelles ne reflète pas une taxinomie formelle dans la spécification des exigences.

46 Dans l’introduction de la classe se trouve une figure qui décrit les familles de cette classe et la hiérarchie des composants dans chaque famille, comme expliqué dans la section 2.2.

2.1.2 Structure d’une famille

47 La figure 2.2 illustre la structure d’une famille fonctionnelle sous forme de diagramme.

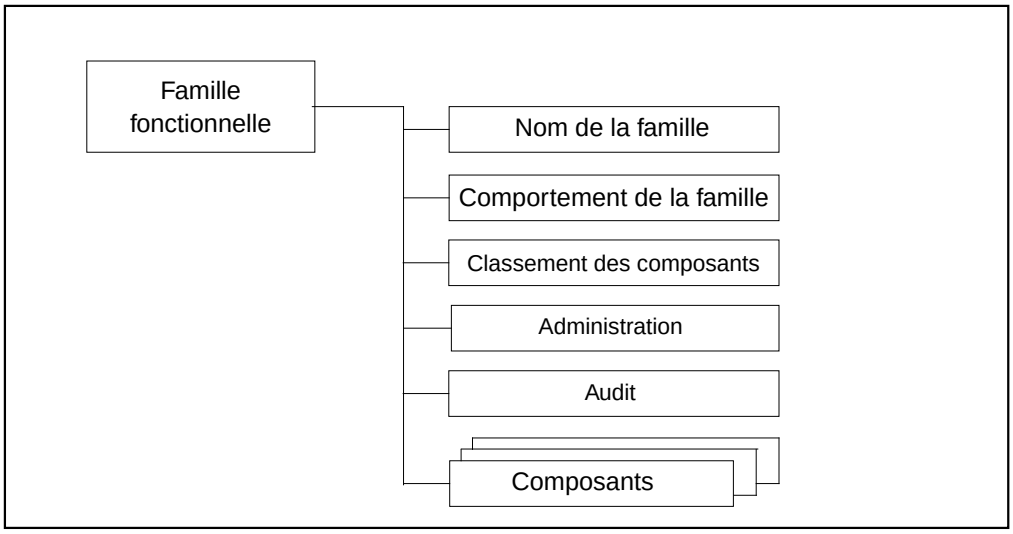


Figure 2.2 - Structure d’une famille fonctionnelle

2.1.2.1 Nom de la famille

48 La rubrique “Nom de la famille” fournit les informations de classification et de description nécessaires pour identifier et classer une famille fonctionnelle. Chaque famille fonctionnelle a un nom unique. Les informations de classification consistent en une abréviation sur sept caractères, les trois premiers étant identiques à l’abréviation du nom de la classe, suivie par le caractère “_” (*underscore*) puis par l’abréviation du nom de la famille, comme suit : XXX_YYY. L’abréviation unique du nom de la famille est la principale référence utilisée pour identifier les composants.

2.1.2.2 Comportement de la famille

49 La rubrique “Comportement de la famille” comprend la description sous forme narrative des objectifs de sécurité de la famille fonctionnelle et une description générale de ses exigences fonctionnelles. Ils sont décrits de façon plus détaillée ci-dessous :

a) Les *objectifs de sécurité* de la famille couvrent un problème de sécurité qui peut être résolu à l’aide d’une TOE qui inclut un composant de cette famille ;

b) La description des *exigences fonctionnelles* résume toutes les exigences qui sont comprises dans le ou les composant(s). La description est destinée aux auteurs de PP, de ST et de paquets fonctionnels, qui souhaitent déterminer si la famille convient à leurs besoins spécifiques.

2.1.2.3 Classement des composants

50 Les familles fonctionnelles contiennent un ou plusieurs composants, chacun d’entre eux pouvant être choisi pour figurer dans des PP, ST et paquets fonctionnels. Le but de cette section est de fournir aux utilisateurs des informations pour sélectionner un composant fonctionnel approprié, après avoir déterminé si la famille concernée devait nécessairement ou utilement faire partie de leurs exigences de sécurité.

51 Cette rubrique de la description de la famille fonctionnelle décrit les composants disponibles et leur argumentaire. Les caractéristiques détaillées des composants figurent dans chaque composant.

52 Les relations entre composants au sein d’une famille fonctionnelle peuvent être hiérarchiques ou non. Un composant est hiérarchiquement supérieur à un autre s’il offre plus de sécurité.

53 Comme cela est expliqué dans la section 2.2, les descriptions des familles fournissent une vue d’ensemble sous forme graphique de la hiérarchie des composants dans une famille.

2.1.2.4 Administration

54 Les exigences d’*administration* contiennent les informations destinées aux auteurs du PP ou de la ST à prendre en compte au titre des activités d’administration pour un composant donné. Les exigences d’administration sont détaillées dans les composants de la classe administration (FMT).

55 Un auteur de PP ou de ST peut sélectionner les exigences d’administration indiquées ou peut inclure d’autres exigences d’administration non citées. En tant que telles, ces exigences devraient être considérées comme informatives.

2.1.2.5 Audit

56 Les exigences d'*audit* contiennent des événements auditables pouvant être choisis par les auteurs du PP ou de la ST, si les exigences de la classe "FAU, Audit de sécurité", figurent dans le PP ou la ST. Ces exigences comprennent les événements touchant à la sécurité décrits selon les différents niveaux de détail apportés par les composants de la famille "FAU_GEN Génération des données de l'audit de sécurité". Par exemple, une note d'audit pourrait inclure des actions formulées dans les termes suivants : Audit minimal - utilisation réussie du mécanisme de sécurité ; Audit élémentaire - toute utilisation du mécanisme de sécurité ainsi que les informations pertinentes concernant les attributs de sécurité impliqués ; Audit détaillé - tout changement de configuration effectué sur le mécanisme, comprenant les valeurs de la configuration en vigueur avant et après le changement.

57 On devrait observer que la classification des événements auditables est hiérarchique. Par exemple, si la génération d'Audit élémentaire est souhaitée, tous les événements auditables identifiés comme étant à la fois "Audit minimal" et "Audit élémentaire" devraient être inclus dans le PP ou la ST en utilisant l'opération d'affectation appropriée, sauf dans le cas où l'événement de niveau le plus élevé fournit tout simplement plus de détails que l'événement de plus bas niveau. Si la génération d'Audit détaillé est souhaitée, tous les événements auditables identifiés (de types Audit minimal, Audit élémentaire et Audit détaillé) devraient être inclus dans le PP ou la ST.

58 Dans la classe FAU, les règles qui régissent l'audit sont expliquées avec plus de détails.

2.1.3 Structure d'un composant

59 La figure 2.3 illustre la structure d'un composant fonctionnel.

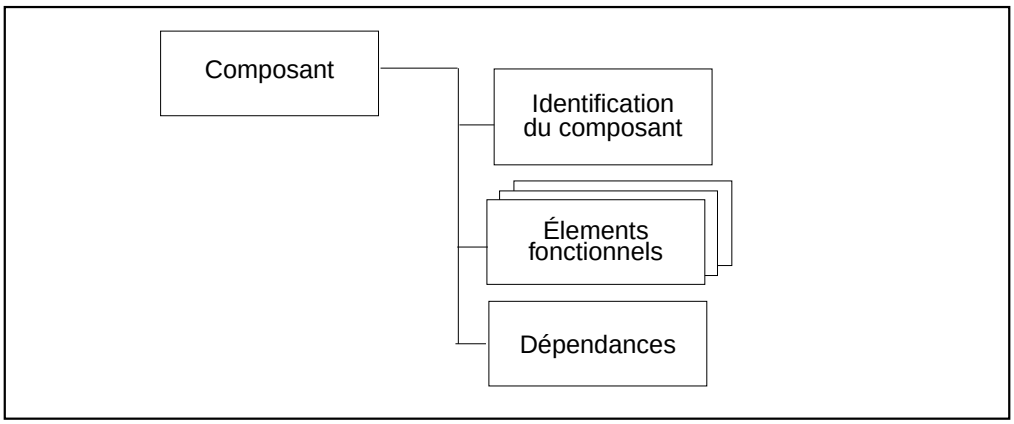


Figure 2.3 - Structure d'un composant fonctionnel

2.1.3.1 Identification du composant

60 La rubrique “Identification du composant” fournit les informations descriptives nécessaires pour identifier, classer, enregistrer et référencer un composant. Les informations suivantes sont fournies pour chaque composant fonctionnel :

61 Un *nom unique* : le nom indique le but du composant.

62 Une *abréviation* : une abréviation unique du nom du composant fonctionnel. Cette abréviation sert à classer, enregistrer et référencer le composant. Elle indique la classe et la famille auxquelles appartient le composant ainsi que le numéro du composant dans la famille.

63 Une rubrique “*hiérarchique à”* : une liste de composants auxquels le composant considéré est hiérarchique, celui-ci pouvant être utilisé pour satisfaire aux dépendances des composants cités dans la liste.

2.1.3.2 Éléments fonctionnels

64 Un ensemble d’éléments est fourni pour chaque composant. Chaque élément est défini individuellement et se suffit à lui-même.

65 Un élément fonctionnel est une exigence fonctionnelle de sécurité qui, si elle était encore divisée n’aboutirait pas à un résultat d’évaluation significatif. C’est la plus petite exigence fonctionnelle de sécurité identifiée et reconnue dans les CC.

66 Pour l’élaboration de paquets, de PP ou de ST, il n’est pas permis de sélectionner seulement un ou plusieurs éléments au sein d’un composant. L’ensemble complet des éléments d’un composant doit être sélectionné pour être inclus dans un PP, une ST ou un paquet.

67 Une abréviation unique du nom de l’élément fonctionnel est donnée. Par exemple, le nom de l’exigence FDP_IFF.4.2 se lit comme suit : F - exigence fonctionnelle, DP - classe “Protection des données de l’utilisateur (user data protection)”, _IFF - famille “Fonctions de contrôle de flux d’information (information flow control functions)”, .4 - 4ème composant dénommé “Elimination partielle des flux d’information illicites”, .2 - 2ème élément du composant.

2.1.3.3 Dépendances

68 Les dépendances entre les composants fonctionnels apparaissent quand un composant ne se suffit pas à lui-même et dépend des fonctionnalités d’un autre composant, ou d’interactions avec lui, pour son propre fonctionnement.

69 Chaque composant fonctionnel fournit une liste complète des dépendances vers d’autres composants fonctionnels et d’assurance. Certains composants peuvent indiquer “Pas de dépendances”. Les composants dont un composant dépend peuvent à leur tour dépendre d’autres composants. La liste indiquée pour les composants donne les dépendances directes, c’est-à-dire les seules références vers les exigences fonctionnelles qui sont requises pour que l’exigence considérée

puisse être correctement appliquée. Les dépendances indirectes, c'est-à-dire les dépendances résultant des composants dont dépend le composant considéré, peuvent être trouvées dans l'annexe A de la partie 2 des CC. On notera que, dans certains cas, la dépendance est optionnelle du fait qu'un certain nombre d'exigences fonctionnelles est fourni, alors que chacune d'entre elles suffirait pour satisfaire à la dépendance (voir par exemple FDP_UIT.1).

70 La liste des dépendances identifie les composants fonctionnels ou d'assurance minimum nécessaires pour satisfaire aux exigences de sécurité associées à un composant identifié. Les composants qui sont hiérarchiquement supérieurs au composant identifié peuvent aussi être utilisés pour satisfaire la dépendance.

71 Les dépendances indiquées dans la partie 2 des CC sont à caractère normatif. Elles doivent être satisfaites dans un PP ou une ST. Dans des situations particulières, les dépendances indiquées pourraient ne pas être applicables. L'auteur du PP ou de la ST, en fournissant l'argumentaire qui explique la raison pour laquelle la dépendance n'est pas applicable, peut ne pas inclure le composant vers lequel porte la dépendance dans le paquet, le PP ou la ST.

2.1.4 Opérations autorisées sur un composant fonctionnel

72 Les composants fonctionnels utilisés dans la définition des exigences dans un PP, une ST ou un paquet fonctionnel peuvent être exactement tels qu'ils sont spécifiés dans le chapitre 2 de la présente partie des CC, ou bien peuvent être adaptés pour satisfaire à un objectif de sécurité spécifique. Cependant, la sélection et l'adaptation de ces composants fonctionnels est compliquée par le fait que les dépendances identifiées du composant doivent être prises en compte. Ainsi, cette adaptation est limitée à un ensemble approuvé d'opérations.

73 Une liste des opérations autorisées est associée à chaque composant fonctionnel. Toutes les opérations ne sont pas autorisées sur tous les composants fonctionnels.

74 Les opérations autorisées sont sélectionnées à partir de l'ensemble suivant :

- itération : opération qui permet à un composant d'être utilisé plus d'une fois avec des opérations différentes,
- affectation : opération qui permet la spécification d'un paramètre identifié,
- sélection : opération qui permet la sélection d'un ou de plusieurs éléments à partir d'une liste,
- raffinement : opération qui permet l'addition de détails.

2.1.4.1 Itération

75 Quand il est nécessaire de couvrir des aspects différents d'une même exigence (e.g. l'identification de plus d'un type d'utilisateur), l'utilisation répétitive du même composant de la partie 2 des CC pour couvrir chaque aspect est autorisée.

2.1.4.2 Affectation

76 Certains éléments de composants fonctionnels contiennent des paramètres ou des variables qui permettent à l'auteur du PP ou de la ST de spécifier une politique ou un ensemble de valeurs à incorporer dans le PP ou la ST, afin de satisfaire à un objectif de sécurité spécifique. Ces éléments identifient clairement chaque paramètre et chaque contrainte portant sur les valeurs qui peuvent être affectées à ce paramètre.

77 Tout aspect d'un élément dont les valeurs acceptables peuvent être décrites ou énumérées de façon non ambiguë peut être représenté au moyen d'un paramètre. Le paramètre peut être un attribut ou une règle qui restreint l'exigence à une valeur spécifique ou à une plage de valeurs. Par exemple, pour répondre à un objectif de sécurité spécifié, l'élément d'un composant fonctionnel peut indiquer qu'une opération donnée devrait être exécutée un certain nombre de fois. Dans ce cas, l'affectation indiquerait le nombre, ou la plage de nombres, devant être utilisé pour le paramètre.

2.1.4.3 Sélection

78 C'est l'opération qui consiste à prendre un ou plusieurs articles dans une liste afin de réduire le champ d'application d'un élément d'un composant.

2.1.4.4 Raffinement

79 Pour tous les éléments d'un composant fonctionnel, l'auteur du PP ou de la ST est autorisé à limiter l'ensemble des implémentations acceptables en spécifiant des détails complémentaires afin de satisfaire à un objectif de sécurité. Le raffinement d'un élément consiste à ajouter de tels détails techniques.

80 Dans une ST, il pourrait être nécessaire d'expliquer la signification des termes "sujet" et "objet" pour que la TOE ait tout son sens, et ceux-ci peuvent par conséquent faire l'objet d'un raffinement.

81 Comme pour les autres opérations, le raffinement ne génère aucune exigence qui soit complètement nouvelle. Elle rajoute des détails élaborés, une interprétation ou une signification spéciale à une exigence, une règle, une constante ou une condition, en fonction des objectifs de sécurité. Le raffinement doit seulement restreindre encore l'ensemble des fonctions ou mécanismes pouvant être acceptables pour implémenter les exigences, mais ne doit jamais l'augmenter. Le raffinement n'autorise pas la création de nouvelles exigences, et donc ne rallonge pas la liste des dépendances associées à un composant. L'auteur du PP ou de la ST doit veiller à ce que les dépendances des exigences qui dépendent de l'exigence considérée soient satisfaites.

2.2 Catalogue des composants

82 Le regroupement des composants dans la présente partie des CC ne relève d'aucune taxinomie formelle.

83 La présente partie 2 des CC contient des classes de familles et de composants qui constituent des regroupements approximatifs établis sur la base de fonctions ou d'objectifs communs, présentés par ordre alphabétique. Au début de chaque classe figure un diagramme qui indique la taxinomie de cette classe, citant les familles de cette classe et les composants de chaque famille. Le diagramme constitue un indicateur utile des relations hiérarchiques qui peuvent exister entre composants.

84 Dans la description des composants fonctionnels, une rubrique identifie les dépendances entre ce composant et tous les autres composants.

85 Pour chaque classe, une figure décrivant la hiérarchie de la famille, semblable à la figure 2.4, est fournie. Dans la figure 2.4, la première famille, soit la famille 1, contient trois composants hiérarchiques, où le composant 2 et le composant 3 peuvent tous deux être utilisés pour satisfaire aux dépendances associées au composant 1. Le composant 3 est hiérarchique au composant 2 et peut aussi être utilisé pour satisfaire aux dépendances associées au composant 2.

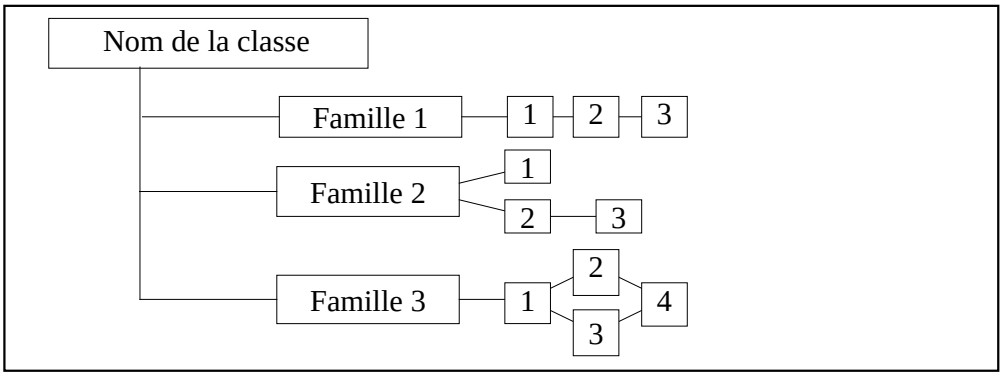


Figure 2.4 - Exemple de diagramme de décomposition d'une classe

86 Dans la famille 2, il y a trois composants qui ne sont pas tous hiérarchiques. Les composants 1 et 2 ne sont hiérarchiques à aucun autre composant. Le composant 3 est hiérarchique au composant 2 et peut aussi être utilisé pour satisfaire aux dépendances associées au composant 2, mais pas pour satisfaire aux dépendances associées au composant 1.

87 Dans la famille 3, les composants 2, 3 et 4 sont hiérarchiques au composant 1. Les composants 2 et 3 sont tous deux hiérarchiques au composant 1, mais ne sont pas comparables entre eux. Le composant 4 est hiérarchique à la fois au composant 2 et au composant 3.

88 Ces diagrammes sont destinés à compléter les explications sur les familles et permettent une identification plus facile des relations. Ils ne remplacent pas la rubrique "Hiérarchique à :" figurant dans chaque composant, qui constitue la déclaration obligatoire des liens de hiérarchie pour chaque composant.

2.2.1 Mise en évidence des modifications effectuées sur un composant

89 Les relations entre composants d'une famille sont mises en évidence en utilisant la convention **caractères gras**. Cette convention implique que toutes les nouvelles exigences sont indiquées en caractères gras. Pour les composants hiérarchiques à d'autres, les exigences ou les dépendances sont indiquées en caractères gras lorsqu'elles constituent un enrichissement ou une modification par rapport aux exigences du composant précédent. De plus, toutes opérations autorisées, nouvelles ou faisant l'objet d'un enrichissement par rapport au composant précédent, sont également indiquées en **caractères gras**.

3 Classe FAU : Audit de sécurité

90 Auditer la sécurité implique la reconnaissance, l'enregistrement, le stockage et l'analyse d'informations associées à des activités touchant à la sécurité (i.e. des activités sous le contrôle de la TSP). Les enregistrements d'audit en résultant peuvent être examinés pour déterminer quelles activités touchant à la sécurité ont eu lieu et quels personnes (utilisateurs) en sont responsables.

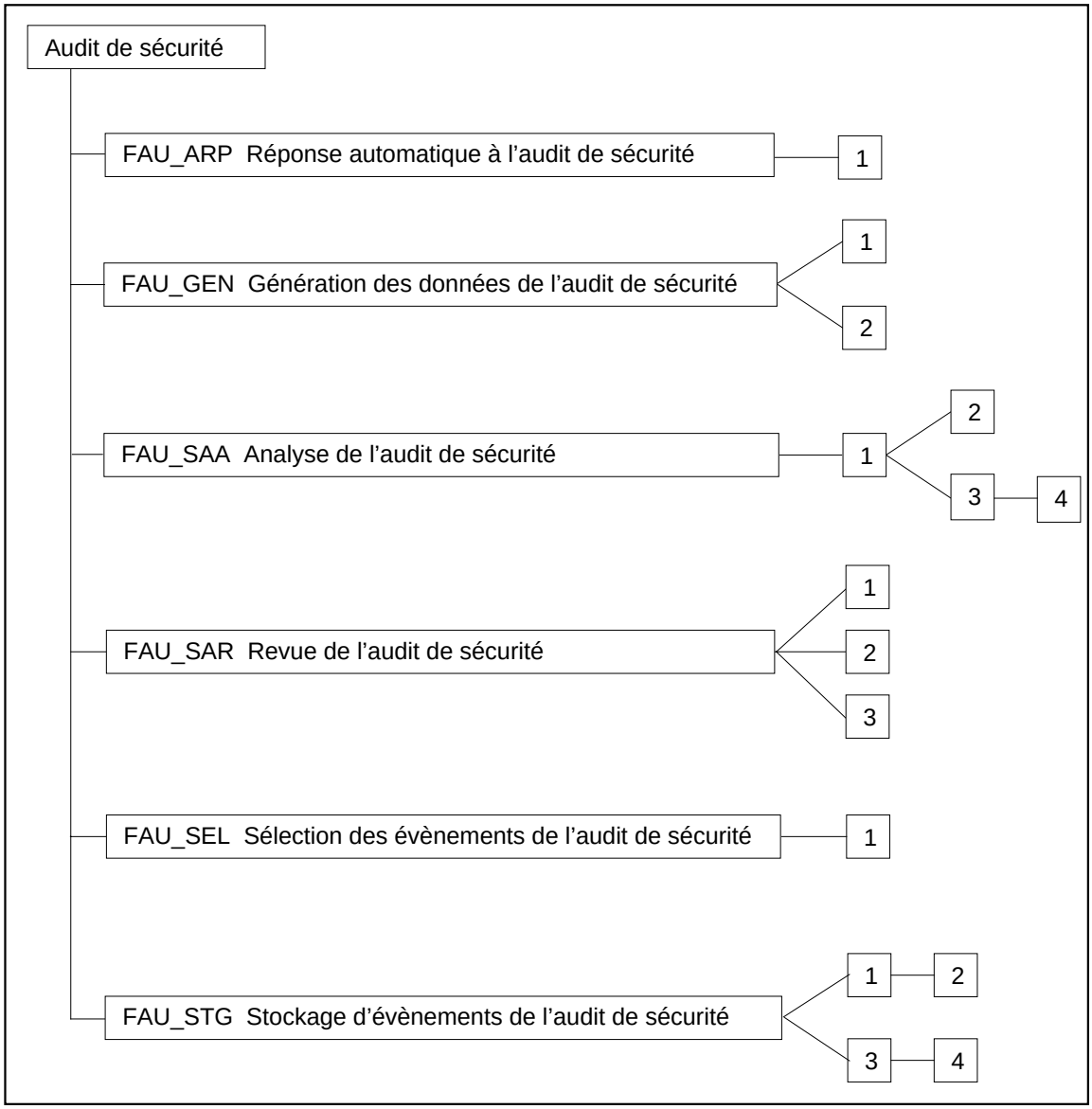


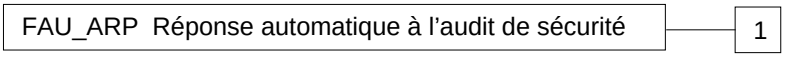
Figure 3.1 - Décomposition de la classe "Audit de sécurité"

3.1 Réponse automatique de l'audit de sécurité (FAU_ARP)

Comportement de la famille

91 La présente famille définit les mesures à prendre dans le cas où des événements indiquant une violation potentielle de la sécurité sont détectés.

Classement des composants



92 Selon le composant "FAU_ARP.1 Alarmes de sécurité", la TSF doit entreprendre des actions dans le cas où une violation potentielle de la sécurité est détectée.

Administration : FAU_ARP.1

93 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) l'administration (addition, suppression ou modification) d'actions.

Audit : FAU_ARP.1

94 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : actions entreprises à cause de violations imminentes de la sécurité.

FAU_ARP.1 Alarmes de sécurité

Hiérarchique à : aucun autre composant.

FAU_ARP.1.1 La TSF doit entreprendre [affectation : *liste des actions les moins perturbatrices*] dès la détection d'une violation potentielle de la sécurité.

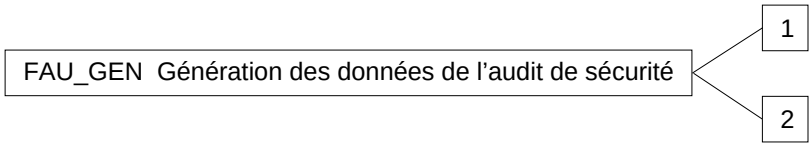
Dépendances : **FAU_SAA.1 Analyse de violation potentielle**

3.2 Génération des données de l'audit de sécurité (FAU_GEN)

Comportement de la famille

95 La présente famille définit des exigences pour enregistrer les occurrences d'événements touchant à la sécurité qui ont lieu sous le contrôle de la TSF. Cette famille identifie le niveau de l'audit, énumère les types d'événements qui doivent pouvoir être audités par la TSF et identifie l'ensemble minimum des informations liées à l'audit qui devraient être fournies par les divers types d'enregistrements d'audit.

Classement des composants



96 Le composant "FAU_GEN.1 Génération de données d'audit" définit le niveau des événements auditables et spécifie la liste des données que chaque enregistrement doit contenir.

97 Selon le composant "FAU_GEN.2 Lien avec l'identité de l'utilisateur", la TSF doit associer les événements auditables aux identités des utilisateurs individuels.

Administration : FAU_GEN.1, FAU_GEN.2

98 Il n'y a pas d'activités d'administration prévues.

Audit : FAU_GEN.1, FAU_GEN.2

99 Il n'y a pas d'actions identifiées qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FAU_GEN.1 Génération de données d'audit

Hiérarchique à : aucun autre composant.

FAU_GEN.1.1 La TSF doit pouvoir générer un enregistrement d'audit des événements auditables suivants :

a) démarrage et arrêt des fonctions d'audit ;

b) tous les événements auditables pour le niveau d'audit [sélection : *minimum, élémentaire, détaillé, non spécifié*] ;

c) et [affectation : *autres événements auditables définis spécifiquement*].

FAU_GEN.1.2 **La TSF doit enregistrer au minimum les informations suivantes dans chaque enregistrement d'audit :**

a) **date et heure de l'événement, type d'événement, identité du sujet, ainsi que le résultat (succès ou échec) de l'événement ;**

b) **et, pour chaque type d'événement d'audit, sur la base des définitions d'événements auditables contenues dans les composants fonctionnels inclus dans le PP ou la ST, [affectation : *autres informations d'audit pertinentes*]**

Dépendances : **FPT_STM.1 Horodatage fiable**

FAU_GEN.2 Lien avec l'identité de l'utilisateur

Hiérarchique à : aucun autre composant.

FAU_GEN.2.1 **La TSF doit pouvoir associer chaque événement auditable avec l'identité de l'utilisateur qui est à l'origine de l'événement.**

Dépendances : **FAU_GEN.1 Génération de données d'audit**
FIA_UID.1 Programmation de l'identification

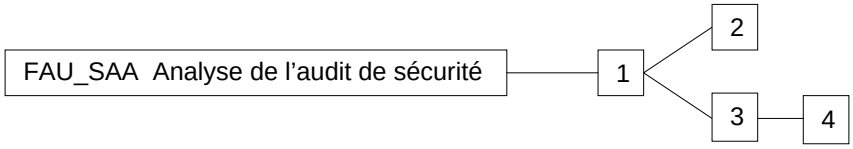
3.3 Analyse de l'audit de sécurité (FAU_SAA)

Comportement de la famille

100 La présente famille définit des exigences relatives aux moyens automatisés qui analysent l'activité du système et les données d'audit, à la recherche de violations possibles ou effectives de la sécurité. Cette analyse peut contribuer à la détection d'intrusion ou à la réponse automatique à une violation de la sécurité imminente.

101 Les actions qui doivent être entreprises en fonction de la détection peuvent être spécifiées en utilisant la famille FAU_ARP si cela est souhaité.

Classement des composants



102 Dans le composant "**FAU_SAA.1 Analyse de violation potentielle**", un seuil de détection élémentaire est exigé, défini selon une règle fixée.

103 Selon le composant "FAU_SAA.2 Détection d'anomalie basée sur un profil", la TSF maintient des *profils* individuels d'utilisation du système, où un profil représente les modèles historiques de comportements des membres du *groupe cible du profil*. Un groupe cible de profil est un groupe formé d'un ou de plusieurs individus (e.g. un utilisateur unique, des utilisateurs travaillant sous un même identifiant de groupe (group ID) ou sous un même compte, des utilisateurs travaillant sous un rôle qui leur est attribué, des utilisateurs d'un système complet ou d'un noeud de réseau) qui interagissent avec la TSF. À chaque membre d'un groupe cible de profil est attribué un *indice de représentativité* individuel qui mesure le degré d'adéquation de l'activité actuelle du membre aux modèles d'utilisation établis représentés dans le profil. Cette analyse peut être réalisée pendant l'exploitation ou être effectuée en temps différé sur des informations recueillies lors de l'exploitation.

104 Selon le composant "FAU_SAA.3 Heuristiques des attaques simples", la TSF doit pouvoir détecter les occurrences d'événements caractéristiques qui représentent une menace significative à l'encontre de l'application de la TSP. Cette recherche d'événements caractéristiques peut se faire en temps réel ou au cours d'une analyse différée des informations recueillies en exploitation.

105 Selon le composant "FAU_SAA.4 Heuristiques des attaques complexes", la TSF doit pouvoir stocker des scénarios d'intrusion comportant plusieurs phases et les détecter. La TSF est à même de comparer des événements système (qui peuvent être causés par plusieurs individus) à des séquences d'événements connues pour représenter des scénarios complets d'intrusion. La TSF doit être capable d'indiquer quand un événement ou une séquence d'événements caractéristiques indique une violation potentielle de la TSP.

Administration : FAU_SAA.1

106 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la maintenance des règles par (addition, modification, suppression) de règles dans l'ensemble des règles.

Administration : FAU_SAA.2

107 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la maintenance (suppression, modification, addition) du groupe d'utilisateurs au sein du groupe cible d'un profil.

Administration : FAU_SAA.3

108 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la maintenance (suppression, modification, addition) du sous-ensemble d'événements système.

Administration : FAU_SAA.4

109 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la maintenance (suppression, modification, addition) du sous-ensemble d'événements système ;

b) la maintenance (suppression, modification, addition) de l'ensemble des séquences d'événements système.

Audit : FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4

110 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : activation et désactivation de tout mécanisme d'analyse ;

b) Minimal : réponses automatisées effectuées par l'outil.

FAU_SAA.1 Analyse de violation potentielle

Hiérarchique à : aucun autre composant.

FAU_SAA.1.1 **La TSF doit pouvoir appliquer un ensemble de règles en surveillant les événements audités et indiquer, en fonction de ces règles, une violation potentielle de la TSP.**

FAU_SAA.1.2 **La TSF doit appliquer les règles suivantes pour la surveillance des événements audités :**

a) **accumulation ou combinaison de [affectation : *sous-ensemble d'événements auditables définis*] connus pour indiquer une violation potentielle de la sécurité ;**

b) **[affectation : *toutes les autres règles*].**

Dépendances : **FAU_GEN.1 Génération de données d'audit**

FAU_SAA.2 Détection d'anomalie basée sur un profil

Hiéarchique à : FAU_SAA.1

FAU_SAA.2.1 **La TSF doit pouvoir maintenir des profils d'utilisation du système, où un profil individuel représente les modèles historiques de comportements d'un ou de plusieurs membres de [affectation : *le groupe cible du profil*].**

FAU_SAA.2.2 **La TSF doit pouvoir maintenir un indice de représentativité associé à chaque utilisateur dont l'activité est enregistrée dans un profil, où l'indice de représentativité indique le degré avec lequel l'activité actuelle de l'utilisateur se révèle différer des modèles établis d'utilisation représentés dans le profil.**

FAU_SAA.2.3 **La TSF doit être capable d'indiquer une violation imminente de la TSP quand l'indice de représentativité d'un utilisateur dépasse les conditions limites suivantes [affectation : *conditions sous lesquelles une activité anormale est signalée par la TSF*].**

Dépendances : **FIA_UID.1 Programmation de l'identification**

FAU_SAA.3 Heuristiques des attaques simples

Hiéarchique à : FAU_SAA.1

FAU_SAA.3.1 **La TSF doit pouvoir maintenir une représentation interne des événements caractéristiques suivants [affectation : *un sous-ensemble d'événements système*] qui peuvent indiquer une violation de la TSP.**

FAU_SAA.3.2 **La TSF doit pouvoir comparer les événements caractéristiques à l'enregistrement de l'activité du système discernables par l'examen de [affectation : *les informations à utiliser pour déterminer l'activité du système*].**

FAU_SAA.3.3 **La TSF doit être capable d'indiquer une violation imminente de la TSP quand un événement système se révèle correspondre à un événement caractéristique qui indique une violation potentielle de la TSP.**

Dependencies: No dependencies

FAU_SAA.4 Heuristiques des attaques complexes

Hiéarchique à : FAU_SAA.3

FAU_SAA.4.1 La TSF doit pouvoir maintenir une représentation interne **des enchaînements d'événements faisant partie de scénarios d'intrusion connus suivants [affectation :** ***liste des enchaînements d'événements système dont l'occurrence est représentative de scénarios de pénétration connus*****] et** des événements caractéristiques suivants [affectation : *un sous-ensemble d'événements système*] qui peuvent indiquer une violation potentielle de la TSP.

FAU_SAA.4.2 La TSF doit pouvoir comparer les événements caractéristiques **et les enchaînements d'événements** à l'enregistrement de l'activité du système discernables par l'examen de [affectation : *les informations à utiliser pour déterminer l'activité du système*].

FAU_SAA.4.3 La TSF doit être capable d'indiquer une violation imminente de la TSP quand **l'activité du système** se révèle correspondre à un événement caractéristique **ou à un enchaînement d'événements** qui indique une violation potentielle de la TSP.

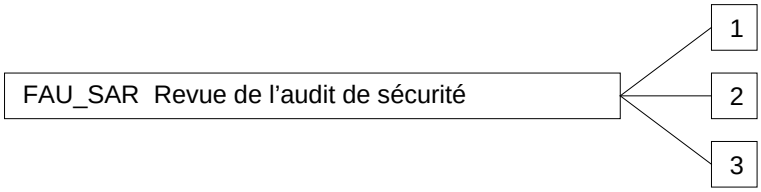
Dependencies: No dependencies

3.4 Revue de l'audit de sécurité (FAU_SAR)

Comportement de la famille

111 La présente famille définit les exigences pour des outils d'audit qui devraient être mis à la disposition d'utilisateurs autorisés afin de les assister dans la revue des données d'audit.

Classement des composants



112 Le composant "FAU_SAR.1 Revue d'audit" offre la capacité de lire des informations à partir des enregistrements d'audit.

113 Le composant "FAU_SAR.2 Revue d'audit restreinte" exige qu'il n'y ait pas d'autres utilisateurs qui puissent lire les informations, à l'exception de ceux qui ont été identifiés dans le composant FAU_SAR.1.

114 Le composant "FAU_SAR.3 Revue d'audit sélective" exige que des outils de revue d'audit sélectionnent, à partir de critères, les données d'audit à examiner.

Administration : FAU_SAR.1

115 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la maintenance (suppression, modification, addition) du groupe d'utilisateurs ayant le droit d'accès en lecture aux enregistrements d'audit.

Administration : FAU_SAR.2, FAU_SAR.3

116 Il n'y a pas d'activités d'administration prévues.

Audit : FAU_SAR.1

117 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : lecture d'informations à partir des enregistrements d'audit.

Audit : FAU_SAR.2

118 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : essais infructueux de lecture d'informations à partir des enregistrements d'audit.

Audit : FAU_SAR.3

119 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Détaillé : les paramètres utilisés pour la visualisation.

FAU_SAR.1 Revue d'audit

120 Le présent composant fournit aux utilisateurs autorisés la capacité d'obtenir et d'interpréter les informations. Dans le cas où il s'agit d'utilisateurs humains (de personnes), ces informations doivent être présentées sous une forme qui leur soit compréhensible. Dans le cas où il s'agit d'entités TI externes, les informations doivent être présentées sans ambiguïté sous un format électronique.

Hiérarchique à : aucun autre composant.

FAU_SAR.1.1 La TSF doit offrir à [affectation : *utilisateurs autorisés*] la capacité de lire [affectation : *liste des informations d'audit*] à partir des enregistrements d'audit.

FAU_SAR.1.2 La TSF doit présenter les enregistrements d'audit d'une façon permettant à l'utilisateur de les interpréter.

Dépendances : **FAU_GEN.1 Génération de données d'audit**

FAU_SAR.2 Revue d'audit restreinte

Hiérarchique à : aucun autre composant.

FAU_SAR.2.1 La TSF doit interdire à tous les utilisateurs le droit d'accès en lecture aux enregistrements d'audit, à l'exception de ceux à qui l'on a accordé un droit de lecture explicite.

Dépendances : **FAU_SAR.1 Revue d'audit**

FAU_SAR.3 Revue d'audit sélective

Hiérarchique à : aucun autre composant.

FAU_SAR.3.1 **La TSF doit offrir l'aptitude d'effectuer des [sélection : *recherches, tris, ordonnancements*] des données d'audit en fonction de [affectation : *critères liés logiquement*].**

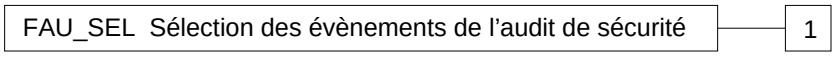
Dépendances : **FAU_SAR.1 Revue d'audit**

3.5 Sélection des évènements de l'audit de sécurité (FAU_SEL)

Comportement de la famille

121 La présente famille définit les exigences pour sélectionner les événements à auditer pendant le fonctionnement de la TOE. Elle définit des exigences pour inclure ou exclure des événements de l'ensemble des événements auditables

Classement des composants



122 Le composant "FAU_SEL.1 Audit sélectif" exige l'aptitude d'inclure ou d'exclure des événements de l'ensemble des événements audités en fonction d'attributs devant être spécifiés par l'auteur du PP ou de la ST.

Administration : FAU_SEL.1

123 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la maintenance des droits de lecture ou de modification des événements d'audit.

Audit : FAU_SEL.1

124 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : toutes les modifications de la configuration d'audit qui ont lieu pendant que les fonctions qui effectuent le recueil des données d'audit sont actives.

FAU_SEL.1 Audit sélectif

Hiérarchique à : aucun autre composant.

FAU_SEL.1.1 La TSF doit pouvoir inclure ou exclure des événements auditables de l'ensemble des événements audités en fonction des attributs suivants :

a) [sélection : *identité de l'objet, identité de l'utilisateur, identité du sujet, identité de l'hôte, type d'événement*]

b) [affectation : *liste des attributs supplémentaires sur lesquels se base la sélectivité de l'audit*].

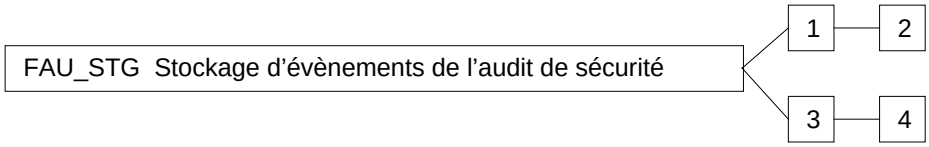
Dépendances : **FAU_GEN.1 Génération de données d'audit**
FMT_MTD.1 Administration des données de la TSF

3.6 Stockage d'évènements de l'audit de sécurité (FAU_STG)

Comportement de la famille

125 La présente famille définit les exigences pour que la TSF soit capable de créer et de maintenir une trace d'audit sûre.

Classement des composants



126 Dans le composant "FAU_STG.1 Stockage protégé de la trace d'audit", des exigences sont définies pour la trace d'audit. Elle sera protégée contre une suppression ou une modification non autorisée.

127 Le composant "FAU_STG.2 Garanties de disponibilité des données d'audit" spécifie les garanties que la TSF maintient sur les données d'audit malgré l'apparition d'une condition non souhaitée.

128 Le composant "FAU_STG.3 Action en cas de perte possible de données d'audit" spécifie les actions à entreprendre dans le cas où un seuil relatif à la trace d'audit est dépassé.

129 Le composant "FAU_STG.4 Prévention des pertes de données d'audit" spécifie les actions à entreprendre dans le cas où la trace d'audit est pleine.

Administration : FAU_STG.1

130 Il n'y a pas d'activités d'administration prévues.

Administration : FAU_STG.2

131 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la maintenance des paramètres qui contrôlent la capacité de stockage de l'audit.

Administration : FAU_STG.3

132 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la maintenance du seuil ;

b) la maintenance (suppression, modification, addition) des actions à entreprendre dans le cas d'une défaillance imminente du stockage de l'audit.

Administration : FAU_STG.4

133 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la maintenance (suppression, modification, addition) des actions à entreprendre dans le cas d'une défaillance du stockage de l'audit.

Audit : FAU_STG.1, FAU_STG.2

134 Il n'y a pas d'actions identifiées qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

Audit : FAU_STG.3

135 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : actions entreprises à la suite du dépassement d'un seuil.

Audit : FAU_STG.4

136 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : actions entreprises à la suite d'une défaillance dans le stockage de l'audit.

FAU_STG.1 Stockage protégé de la trace d'audit

Hiérarchique à : aucun autre composant.

FAU_STG.1.1 La TSF doit protéger les enregistrements d'audit stockés contre une suppression non autorisée.

FAU_STG.1.2 La TSF doit pouvoir [sélection : *empêcher, détecter*] les modifications effectuées sur les enregistrements d'audit.

Dépendances : **FAU_GEN.1 Génération de données d'audit**

FAU_STG.2 Garanties de disponibilité des données d'audit

Hiéarchique à : FAU_STG.1

FAU_STG.2.1 La TSF doit protéger les enregistrements d'audit stockés contre une suppression non autorisée.

FAU_STG.2.2 La TSF doit pouvoir [sélection : *empêcher, détecter*] les modifications effectuées sur les enregistrements d'audit.

FAU_STG.2.3 **La TSF doit garantir que [affectation : *métrique pour sauvegarder les enregistrements d'audit*] des enregistrements d'audit sera maintenue quand les conditions suivantes apparaîtront : [sélection : *dépassement de capacité du stockage de l'audit, défaillance, attaque*].**

Dépendances : FAU_GEN.1 Génération de données d'audit

FAU_STG.3 Action en cas de perte possible de données d'audit

Hiérarchique à : aucun autre composant.

FAU_STG.3.1 **La TSF doit entreprendre [affectation : *actions à entreprendre en cas de défaillance possible du stockage de l'audit*] si la trace d'audit dépasse [affectation : *limite pré-définie*].**

Dépendances : **FAU_STG.1 Stockage protégé de la trace d'audit**

FAU_STG.4 Prévention des pertes de données d'audit

Hiéarchique à : FAU_STG.3

FAU_STG.4.1 **Si la trace d'audit est pleine, la TSF doit [sélection : *'ignorer les événements auditables', 'empêcher les événements auditables, autres que ceux provoqués par l'utilisateur autorisé bénéficiant de droits spéciaux', 'écraser les enregistrements d'audit les plus anciennement stockés'*] et [affectation : *autres actions à entreprendre en cas de défaillance du stockage de l'audit*].**

Dépendances : FAU_STG.1 Stockage protégé de la trace d'audit

4 Classe FCO : Communication

137 Cette classe propose deux familles traitant l'assurance de l'identité d'une partie participant à un échange de données. Ces familles concernent l'assurance de l'identité de l'émetteur des informations transmises (preuve de l'origine) et de l'identité du destinataire des informations transmises (preuve de la réception). Ces familles garantissent que l'émetteur ne peut pas nier avoir envoyé le message, tout comme le destinataire ne peut pas nier l'avoir reçu.

138 La figure 4.1 montre la décomposition de la présente classe en ses composants constitutifs.

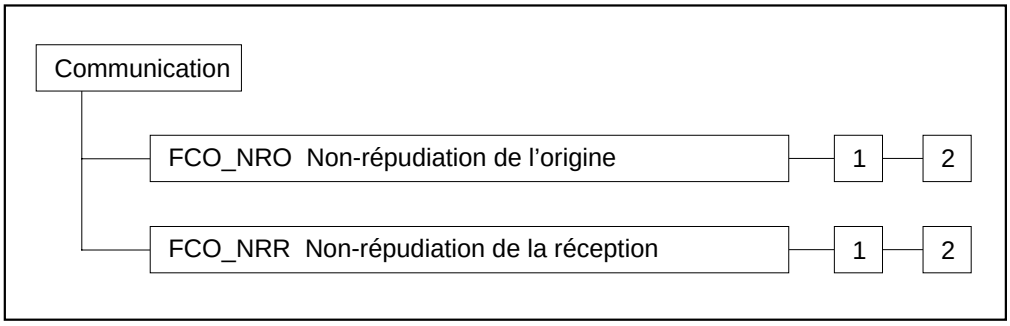


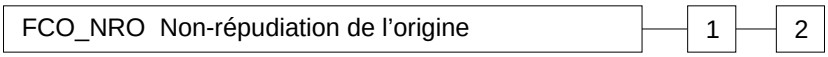
Figure 4.1 - Décomposition de la classe "Communication"

4.1 Non-répudiation de l'origine (FCO_NRO)

Comportement de la famille

139 La famille "Non-répudiation de l'origine" garantit que l'émetteur d'informations ne peut pas réussir à nier avoir envoyé les informations. Cette famille exige que la TSF fournisse une méthode pour garantir qu'un sujet qui reçoit des informations lors d'un échange de données dispose de la preuve de l'origine des informations. Cette preuve peut ensuite être vérifiée soit par le sujet lui-même, soit par d'autres sujets.

Classement des composants



140 Le composant "FCO_NRO.1 Preuve sélective de l'origine" exige que la TSF donne la capacité aux sujets de demander la preuve de l'origine des informations.

141 Le composant "FCO_NRO.2 Preuve systématique de l'origine" exige que la TSF génère systématiquement la preuve de l'origine des informations transmises.

Administration : FCO_NRO.1, FCO_NRO.2

142 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) l'administration des changements des types d'informations, des champs, des attributs de l'émetteur et des destinataires des preuves.

Audit : FCO_NRO.1

143 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : l'identité de l'utilisateur qui a demandé la preuve de l'origine devrait être générée.

b) Minimal : le recours au service de non-répudiation.

c) Elémentaire : l'identification des informations, de leur destination et une copie de la preuve fournie.

d) Détaillé : l'identité de l'utilisateur qui a demandé une vérification de la preuve.

Audit : FCO_NRO.2

144 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : le recours au service de non-répudiation.

b) Elémentaire : l'identification des informations, de leur destination et une copie de la preuve fournie.

c) Détaillé : l'identité de l'utilisateur qui a demandé une vérification de la preuve.

FCO_NRO.1 Preuve sélective de l'origine

Hiérarchique à : aucun autre composant.

FCO_NRO.1.1 **La TSF doit pouvoir générer la preuve de l'origine des [affectation : *liste des types d'informations*] transmis à la demande de [sélection : *émetteur, destinataire,* [affectation : *liste des tierces parties*]].**

FCO_NRO.1.2 **La TSF doit pouvoir établir un lien entre les [affectation : *liste des attributs*] de l'émetteur des informations et les [affectation : *liste des champs d'information*] des informations auxquelles la preuve s'applique.**

FCO_NRO.1.3 **La TSF doit fournir à [sélection : *émetteur, destinataire,* [affectation : *liste des tierces parties*]] la capacité de vérifier la preuve de l'origine des informations, étant donné [affectation : *limitations relatives à la preuve de l'origine*].**

Dépendances : **FIA_UID.1 Programmation de l'identification**

FCO_NRO.2 Preuve systématique de l'origine

Hiéarchique à : FCO_NRO.1

FCO_NRO.2.1 La TSF doit **mettre en œuvre la génération de** la preuve de l'origine à tout moment pour [affectation : *liste des types d'informations*] transmis.

FCO_NRO.2.2 La TSF doit pouvoir établir un lien entre les [affectation : *liste des attributs*] de l'émetteur des informations et les [affectation : *liste des champs d'information*] des informations auxquels la preuve s'applique.

FCO_NRO.2.3 La TSF doit fournir à [sélection : *émetteur, destinataire,* [affectation : *liste des tierces parties*]] la capacité de vérifier la preuve de l'origine des informations étant donné [affectation : *limitations relatives à la preuve de l'origine*].

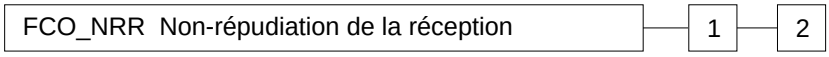
Dépendances : **FIA_UID.1 Programmation de l'identification**

4.2 Non-répudiation de la réception (FCO_NRR)

Comportement de la famille

145 La famille “Non-répudiation de la réception” garantit que le destinataire des informations ne peut pas réussir à nier avoir reçu les informations. Cette famille exige que la TSF fournisse une méthode pour garantir qu’un sujet qui transmet des informations lors d’un échange de données dispose de la preuve de la réception des informations. Cette preuve peut ensuite être vérifiée soit par ce sujet lui-même soit par d’autres sujets.

Classement des composants



146 Le composant “FCO_NRR.1 Preuve sélective de la réception” exige que la TSF donne aux sujets la capacité de demander la preuve de la réception des informations.

147 Le composant “FCO_NRR.2 Preuve systématique de la réception” exige que la TSF génère systématiquement la preuve de la réception pour les informations reçues.

Administration : FCO_NRR.1, FCO_NRR.2

148 Les actions suivantes pourraient être prises en compte pour les fonctions d’administration de la classe FMT :

a) l’administration des changements des types d’informations, des champs, des attributs de l’émetteur et des tierces parties destinataires des preuves.

Audit : FCO_NRR.1

149 Les actions suivantes devraient être auditables dans le cas où la famille “FAU_GEN Génération des données de l’audit de sécurité” est incluse dans le PP ou la ST :

a) Minimal : l’identité de l’utilisateur qui demande une vérification de la preuve devrait être générée.

b) Minimal : le recours au service de non-répudiation.

c) Elémentaire : l’identification des informations, de leur destination et une copie de la preuve fournie.

d) Détaillé : l’identité de l’utilisateur qui a demandé une vérification de la preuve.

Audit : FCO_NRR.2

150 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : le recours au service de non-répudiation ;

b) Elémentaire : l'identification des informations, de leur destination et une copie de la preuve fournie ;

c) Détaillé : l'identité de l'utilisateur qui a demandé une vérification de la preuve.

FCO_NRR.1 Preuve sélective de la réception

Hiérarchique à : aucun autre composant.

FCO_NRR.1.1 **La TSF doit pouvoir générer la preuve de la réception pour [affectation : *liste des types d'informations*] reçus, à la demande de [sélection : *émetteur, destinataire,* [affectation : *liste des tierces parties*]].**

FCO_NRR.1.2 **La TSF doit pouvoir établir un lien entre les [affectation : *liste des attributs*] du destinataire des informations et les [affectation : *liste des champs d'information*] des informations auxquelles la preuve s'applique.**

FCO_NRR.1.3 **La TSF doit fournir à [sélection : *émetteur, destinataire,* [affectation : *liste des tierces parties*]] la capacité de vérifier la preuve de la réception des informations étant donné [affectation : *limitations relatives à la preuve de la réception*].**

Dépendances : **FIA_UID.1 Programmation de l'identification**

FCO_NRR.2 Preuve systématique de la réception

Hiéarchique à : FCO_NRR.1

FCO_NRR.2.1 La TSF doit **mettre en œuvre la génération de** la preuve de la réception pour les [affectation : *liste des types d'informations*] reçus.

FCO_NRR.2.2 La TSF doit pouvoir établir un lien entre les [affectation : *liste des attributs*] du destinataire des informations et les [affectation : *liste des champs d'information*] des informations auxquelles la preuve s'applique.

FCO_NRR.2.3 La TSF doit fournir à [sélection : *émetteur*, *destinataire,* [affectation : *liste des tierces parties*]] la capacité de vérifier la preuve de la réception des informations étant donné [affectation : *limitations relatives à la preuve de la réception*].

Dépendances : **FIA_UID.1 Programmation de l'identification**

5 Classe FCS : Support cryptographique

151 La TSF peut utiliser des fonctionnalités cryptographiques pour contribuer à satisfaire à plusieurs objectifs de sécurité de haut niveau. Ces derniers comprennent entre autres : l'identification et l'authentification, la non-répudiation, le chemin de confiance, le canal de confiance et la séparation des données. La présente classe est utilisée dans le cas où la TOE implémente des fonctions cryptographiques dans du matériel, des micro-programmes ou du logiciel.

152 La classe FCS est composée de deux familles : "FCS_CKM Gestion de clés cryptographiques" et "FCS_COP Opération cryptographique". La famille FCS_CKM traite des aspects de la gestion de clés cryptographiques, tandis que la famille FCS_COP concerne l'utilisation opérationnelle de ces clés cryptographiques.

153 La figure 5.1 montre la décomposition de cette classe dans ses composants constitutifs.

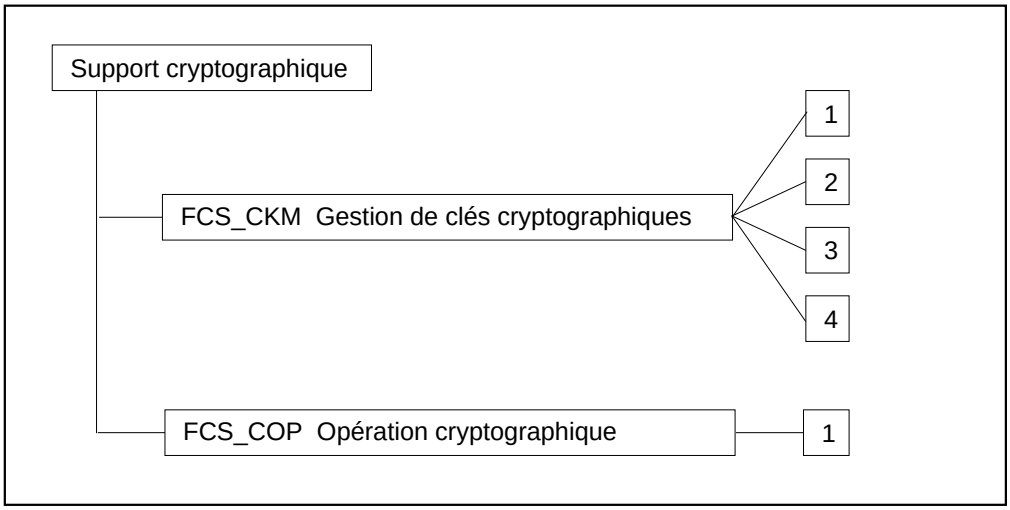


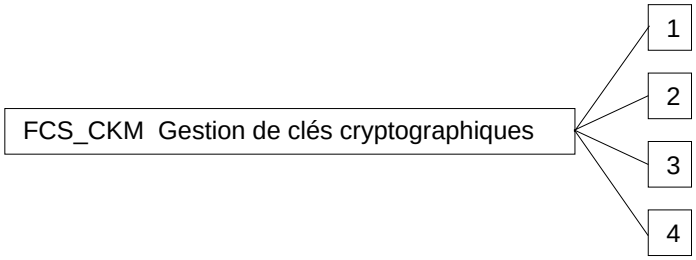
Figure 5.1 - Décomposition de la classe "Support cryptographique"

5.1 Gestion de clés cryptographiques (FCS_CKM)

Comportement de la famille

154 Les clés cryptographiques doivent être gérées tout au long de leur cycle de vie. La présente famille est destinée à contribuer à ce cycle de vie, et définit par conséquent les exigences concernant les activités suivantes : génération de clés cryptographiques, distribution de clés cryptographiques, accès aux clés cryptographiques et destruction de clés cryptographiques. Cette famille devrait être incluse chaque fois qu'il existe des exigences fonctionnelles pour la gestion des clés cryptographiques.

Classement des composants



155 Le composant "FCS_CKM.1 Génération de clés cryptographiques" exige que les clés cryptographiques soient générées conformément à un algorithme et des tailles de clés spécifiés qui peuvent être basés sur une norme identifiée.

156 Le composant "**FCS_CKM.2 Distribution de clés cryptographiques**" exige que les clés cryptographiques soient distribuées conformément à une méthode de distribution spécifiée qui peut être basée sur une norme identifiée.

157 Le composant "FCS_CKM.3 Accès aux clés cryptographiques" exige que les accès aux clés cryptographiques soient effectués conformément à une méthode d'accès spécifiée qui peut être basée sur une norme identifiée.

158 Le composant "FCS_CKM.4 Destruction de clés cryptographiques" exige que les clés cryptographiques soient détruites conformément à une méthode de destruction spécifiée qui peut être basée sur une norme identifiée.

Administration : FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4

159 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) l'administration des modifications des attributs d'une clé cryptographique. De tels attributs comprennent par exemple l'utilisateur, le type de la clé (e.g. publique, privée, secrète), sa période de validité et son utilisation (e.g. signature numérique, chiffrement de clé, négociation de clé, chiffrement de données).

Audit : FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4

160 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : réussite et échec de l'activité.

b) Elémentaire : le ou les attribut(s) de l'objet et la ou les valeur(s) de l'objet à l'exclusion de toute information sensible (e.g. clés secrètes ou privées).

FCS_CKM.1 Génération de clés cryptographiques

Hiérarchique à : aucun autre composant.

FCS_CKM.1.1 La TSF doit générer les clés cryptographiques conformément à un algorithme de génération de clés cryptographiques spécifié [affectation : *algorithme de génération de clés cryptographiques*] et à des tailles de clés cryptographiques spécifiées [affectation : *tailles des clés cryptographiques*] qui satisfont à ce qui suit : [affectation : *liste des normes*].

Dépendances : [**FCS_CKM.2 Distribution de clés cryptographiques**

ou

FCS_COP.1 Opération cryptographique]

FCS_CKM.4 Destruction de clés cryptographiques

FMT_MSA.2 Attributs de sécurité sûrs

FCS_CKM.2 Distribution de clés cryptographiques

Hiérarchique à : aucun autre composant.

FCS_CKM.2.1 La TSF doit distribuer les clés cryptographiques conformément à une méthode de distribution de clés cryptographiques spécifiée [affectation : *méthode de distribution de clés cryptographiques*] qui satisfait à ce qui suit : [affectation : *liste des normes*].

Dépendances : [**FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité**

ou

FCS_CKM.1 Génération de clés cryptographiques]

FCS_CKM.4 Destruction de clés cryptographiques

FMT_MSA.2 Attributs de sécurité sûrs

FCS_CKM.3 Accès aux clés cryptographiques

Hiérarchique à : aucun autre composant.

FCS_CKM.3.1 **La TSF doit réaliser [affectation : *type d'accès aux clés cryptographiques*] conformément à une méthode d'accès aux clés cryptographiques spécifiée [affectation : *méthode d'accès aux clés cryptographiques*] qui satisfait à ce qui suit : [affectation : *liste des normes*].**

Dépendances : [**FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité**

ou

FCS_CKM.1 Génération de clés cryptographiques]

FCS_CKM.4 Destruction de clés cryptographiques

FMT_MSA.2 Attributs de sécurité sûrs

FCS_CKM.4 Destruction de clés cryptographiques

Hiérarchique à : aucun autre composant.

FCS_CKM.4.1 **La TSF doit détruire les clés cryptographiques conformément à une méthode de destruction de clés cryptographiques spécifiée [affectation : *méthode de destruction de clés cryptographiques*] qui satisfait à ce qui suit : [affectation : *liste des normes*].**

Dépendances : [**FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité**

ou

FCS_CKM.1 Génération de clés cryptographiques]

FMT_MSA.2 Attributs de sécurité sûrs

5.2 Opération cryptographique (FCS_COP)

Comportement de la famille

161 Pour qu'une opération cryptographique fonctionne correctement, elle doit être exécutée conformément à un algorithme spécifié et avec une clé cryptographique d'une taille spécifiée. La présente famille devrait être incluse chaque fois qu'il existe des exigences pour que soient réalisées des opérations cryptographiques.

162 Les opérations cryptographiques typiques comprennent le chiffrement ou le déchiffrement de données, la génération ou la vérification de signatures numériques, la génération d'un code d'intégrité de message cryptographique pour des besoins d'intégrité ou pour la vérification d'un code d'intégrité, le hachage sécurisé (condensat de message), le chiffrement ou le déchiffrement de clés cryptographiques et la négociation de clés cryptographiques.

Classement des composants

163 Le composant "FCS_COP.1 Opération cryptographique" exige qu'une opération cryptographique soit exécutée conformément à un algorithme spécifié et avec une clé cryptographique dont la taille peut prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée.

Administration : FCS_COP.1

164 Il n'y a pas d'activités d'administration prévues pour ces composants.

Audit : FCS_COP.1

165 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : réussite et échec, ainsi que le type de l'opération cryptographique.

b) Elémentaire : tout mode d'opération cryptographique applicable, les attributs du sujet et les attributs de l'objet.

FCS_COP.1 Opération cryptographique

Hiérarchique à : aucun autre composant.

FCS_COP.1.1 **La TSF doit exécuter [affectation : *liste des opérations cryptographiques*] conformément à un algorithme cryptographique [affectation : *algorithme cryptographique*] et avec des tailles de clés cryptographiques [affectation : *tailles des clés cryptographiques*] spécifiés qui satisfont à ce qui suit : [affectation : *liste des normes*].**

Dépendances : [**FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité**

ou

FCS_CKM.1 Génération de clés cryptographiques]

FCS_CKM.4 Destruction de clés cryptographiques

FMT_MSA.2 Attributs de sécurité sûrs

6 Classe FDP : Protection des données de l'utilisateur

166 La présente classe contient des familles qui spécifient des exigences pour les fonctions de sécurité de la TOE et pour les politiques des fonctions de sécurité portant sur la protection des données de l'utilisateur. La classe FDP est découpée en quatre groupes de familles (énumérées ci-dessous) qui concernent les données de l'utilisateur dans une TOE, au cours de leur importation, de leur exportation et de leur stockage, ainsi que les attributs de sécurité qui ont un lien direct avec les données de l'utilisateur.

167 Les familles de cette classe sont organisées en quatre groupes :

a) Politiques de la fonction de sécurité assurant la protection des données de l'utilisateur :

- FDP_ACC Politique de contrôle d'accès;
- FDP_IFC Politique de contrôle de flux d'information.

Les composants de ces familles permettent à l'auteur du PP ou de la ST de nommer les politiques des fonctions de sécurité assurant la protection des données de l'utilisateur et de définir le domaine d'application de la politique nécessaire à la couverture des objectifs de sécurité. Les noms de ces politiques sont destinés à être utilisés pour les composants fonctionnels qui nécessitent une opération d'affectation ou de sélection d'une "SFP de contrôle d'accès" ou d'une "SFP de contrôle de flux d'information". Les règles permettant de définir les fonctionnalités des SFP de contrôle d'accès ou de contrôle de flux d'information citées seront définies respectivement dans les familles FDP_ACF et FDP_IFF.

b) Types de protection des données de l'utilisateur :

- FDP_ACF Fonctions de contrôle d'accès;
- FDP_IFF Fonctions de contrôle de flux d'information;
- FDP_ITT Transfert interne à la TOE;
- FDP_RIP Protection des informations résiduelles;
- FDP_ROL Annulation;
- FDP_SDI Intégrité des données stockées.

c) Stockage hors ligne, importation et exportation :

- FDP_DAU Authentification de données;
- FDP_ETC Exportation vers une zone hors du contrôle de la TSF;
- FDP_ITC Importation depuis une zone hors du contrôle de la TSF.

Les composants de ces familles concernent le transfert de confiance en direction ou en provenance du TSC.

d) Communication Inter-TSF :

- FDP_UCT Protection de la confidentialité des données de l'utilisateur lors d'un transfert inter-TSF;
- FDP_UIT Protection de l'intégrité des données de l'utilisateur lors d'un transfert inter-TSF.

Les composants de ces familles concernent la communication entre la TSF de la TOE et un autre produit TI de confiance.

Les figures 6.1 et 6.2 montrent la décomposition de cette classe en ses composants constitutifs.

Classe FDP

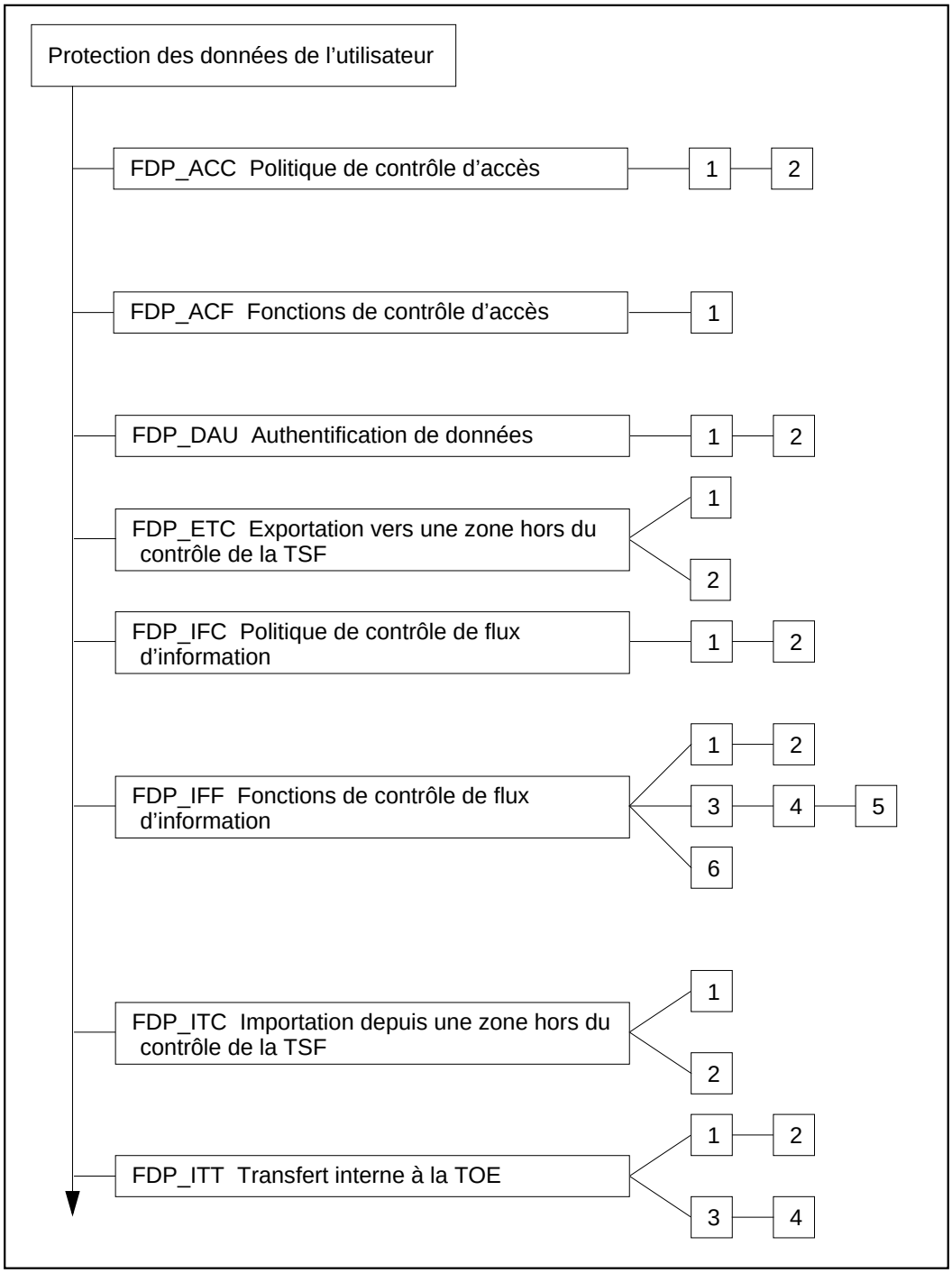


Figure 6.1 - Décomposition de la classe "Protection des données de l'utilisateur"

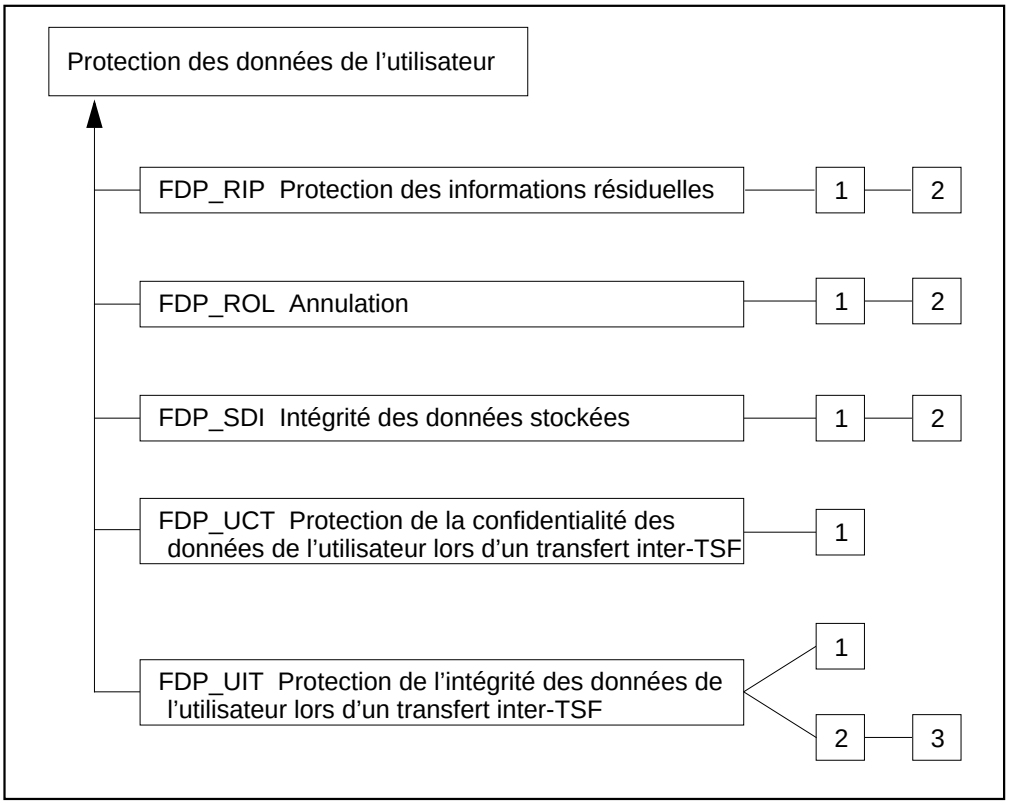


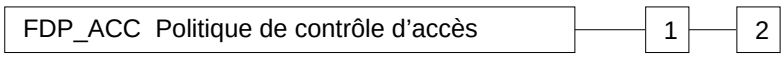
Figure 6.2 - Décomposition de la classe "Protection des données de l'utilisateur" (suite)

6.1 Politique de contrôle d'accès (FDP_ACC)

Comportement de la famille

168 La présente famille identifie les SFP de contrôle d'accès (par leur nom) et définit le domaine d'application des politiques qui forment la partie identifiée du contrôle d'accès de la TSP. Ce domaine d'application est composé de trois ensembles : les sujets contrôlés par la politique, les objets contrôlés par la politique et les opérations concernant les sujets et les objets contrôlés par la politique. Les critères autorisent l'existence de plusieurs politiques, chacune ayant un nom unique. Ceci est réalisé en itérant les composants de cette famille, pour chaque politique de contrôle d'accès citée. Les règles définissant les fonctionnalités d'une SFP de contrôle d'accès seront données par d'autres familles telles que FDP_ACF et FDP_SDI. Les noms des SFP de contrôle d'accès identifiées dans FDP_ACC sont destinés à être utilisés dans les composants fonctionnels qui nécessitent une opération d'affectation ou de sélection d'une "SFP de contrôle d'accès."

Classement des composants



169 Le composant "FDP_ACC.1 Contrôle d'accès partiel" exige que chaque SFP de contrôle d'accès identifiée soit mise en place pour un sous-ensemble des opérations qu'il est possible d'effectuer sur un sous-ensemble des objets de la TOE.

170 Le composant "FDP_ACC.2 Contrôle d'accès complet" exige que chaque SFP de contrôle d'accès identifiée s'applique à toutes les opérations sur les sujets et objets couverts par cette SFP. Il exige de plus que tous les objets et toutes les opérations sur le TSC soient couverts par au moins une SFP de contrôle d'accès identifiée.

Administration : FDP_ACC.1, FDP_ACC.2

171 Il n'y a pas d'activités d'administration prévues pour ce composant.

Audit : FDP_ACC.1, FDP_ACC.2

172 Il n'y a pas d'événements identifiés qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FDP_ACC.1 Contrôle d'accès partiel

Hiérarchique à : aucun autre composant.

FDP_ACC.1.1 La TSF doit appliquer la [affectation : *SFP de contrôle d'accès*] aux [affectation : *liste des sujets, objets et opérations sur les sujets et objets couverts par la SFP*].

Dépendances : **FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité**

FDP_ACC.2 Contrôle d'accès complet

Hiéarchique à : FDP_ACC.1

FDP_ACC.2.1 La TSF doit appliquer la [affectation : *SFP de contrôle d'accès*] aux [affectation : *liste des sujets et objets*] **et à toutes les opérations sur les sujets et objets couverts par la SFP.**

FDP_ACC.2.2 **La TSF doit garantir que toutes les opérations entre tout sujet du TSC et tout objet du TSC sont couvertes par une SFP de contrôle d'accès.**

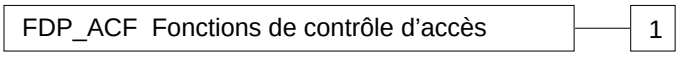
Dépendances : **FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité**

6.2 Fonctions de contrôle d'accès (FDP_ACF)

Comportement de la famille

173 La présente famille décrit les règles relatives aux fonctions spécifiques qui peuvent implémenter une politique de contrôle d'accès citée dans FDP_ACC. FDP_ACC spécifie le domaine d'application de la politique.

Classement des composants



174 Cette famille traite de l'utilisation des attributs de sécurité et des caractéristiques des politiques. Le composant de cette famille est destiné à être utilisé pour décrire les règles relatives à la fonction qui implémente la SFP telle qu'elle est identifiée dans FDP_ACC. L'auteur du PP ou de la ST peut également itérer ce composant pour couvrir plusieurs politiques dans la TOE.

175 Le composant "**FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité**" permet à la TSF de mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. De plus, la TSF peut offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.

Administration : FDP_ACF.1

176 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) administration des attributs utilisés pour prendre les décisions d'autoriser ou de refuser explicitement un accès.

Audit : FDP_ACF.1

177 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : demandes réussies d'exécution d'une opération sur un objet couvert par la SFP;

b) Elémentaire : toutes les demandes d'exécution d'une opération sur un objet couvert par la SFP;

c) Détaillé : les attributs de sécurité spécifiques utilisés pour vérifier un accès.

FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité

Hiérarchique à : aucun autre composant.

FDP_ACF.1.1 **La TSF doit appliquer la [affectation : *SFP de contrôle d'accès*] aux objets en se basant sur [affectation : *attributs de sécurité, groupes d'attributs de sécurité désignés*].**

FDP_ACF.1.2 **La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée : [affectation : *règles qui régissent les accès aux sujets contrôlés et aux objets contrôlés utilisant des opérations contrôlées sur des objets contrôlés*].**

FDP_ACF.1.3 **La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : [affectation : *règles basées sur les attributs de sécurité, qui autorisent explicitement l'accès de sujets à des objets*].**

FDP_ACF.1.4 **La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de [affectation : *règles basées sur les attributs de sécurité, qui interdisent explicitement l'accès de sujets à des objets*].**

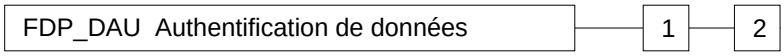
Dépendances : **FDP_ACC.1 Contrôle d'accès partiel**
FMT_MSA.3 Initialisation statique d'attribut

6.3 Authentification de données (FDP_DAU)

Comportement de la famille

178 L'authentification de données permet à une entité d'accepter la responsabilité de l'authenticité d'informations (e.g., en les signant numériquement). La présente famille fournit une méthode qui apporte la garantie de la validité d'une partie spécifique des données, qui peut ensuite être utilisée pour vérifier que le contenu des informations n'a pas été falsifié ni modifié frauduleusement. Contrairement à la classe FCO, cette famille est destinée à être appliquée à des données "statiques" plutôt qu'à des données devant être transférées.

Classement des composants



179 Le composant "FDP_DAU.1 Authentification de données élémentaire" exige que la TSF soit capable de générer une garantie de l'authenticité des informations contenues dans des objets (e.g. des documents).

180 Le composant "FDP_DAU.2 Authentification de données avec identité du garant" exige en complément que la TSF soit capable d'établir l'identité du sujet qui a apporté la garantie d'authenticité.

Administration : FDP_DAU.1, FDP_DAU.2

181 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) l'affectation ou la modification des objets pour lesquels l'authentification de données peut s'appliquer, pourrait être configurable dans le système.

Audit : FDP_DAU.1

182 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

a) Minimal : génération réussie d'une preuve de validité;

b) Elémentaire : génération infructueuse d'une preuve de validité;

c) Détaillé : l'identité du sujet qui a demandé la preuve.

Audit : FDP_DAU.2

183 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

a) Minimal : génération réussie d'une preuve de validité;

b) Elémentaire : génération infructueuse d'une preuve de validité;

c) Détaillé : l'identité du sujet qui a demandé la preuve;

d) Détaillé : l'identité du sujet qui a généré la preuve.

FDP_DAU.1 Authentification de données élémentaire

Hiérarchique à : aucun autre composant.

FDP_DAU.1.1 **La TSF doit offrir une capacité de générer une preuve pouvant être utilisée comme garantie de la validité de [affectation : *liste des objets ou types d'informations*]**.

FDP_DAU.1.2 **La TSF doit offrir aux [affectation : *liste des sujets*] l'aptitude de vérifier la preuve de la validité des informations indiquées**.

Dependencies: No dependencies

FDP_DAU.2 Authentification de données avec identité du garant

Hiéarchique à : FDP_DAU.1

FDP_DAU.2.1 La TSF doit offrir une capacité de générer une preuve pouvant être utilisée comme garantie de la validité de [affectation : *liste des objets ou types d'informations*].

FDP_DAU.2.2 La TSF doit offrir aux [affectation : *liste des sujets*] l'aptitude de vérifier la preuve de la validité des informations indiquées **et l'identité de l'utilisateur qui a généré la preuve.**

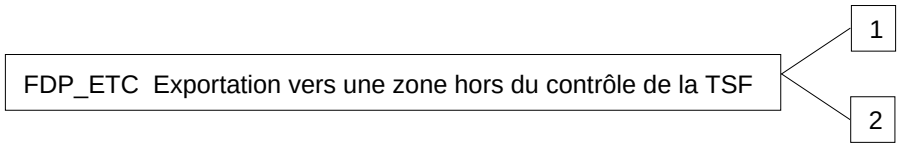
Dépendances : **FIA_UID.1 Programmation de l'identification**

6.4 Exportation vers une zone hors du contrôle de la TSF (FDP_ETC)

Comportement de la famille

184 La présente famille définit les fonctions d'exportation depuis la TOE de données de l'utilisateur, de telle sorte que leurs attributs de sécurité et leur protection puissent soit être explicitement préservés, soit être ignorés, après que les données ont été exportées. Cette famille concerne les limitations relatives à l'exportation ainsi que l'association des attributs de sécurité avec les données de l'utilisateur exportées.

Classement des composants



185 Le composant "FDP_ETC.1 Exportation de données de l'utilisateur sans attributs de sécurité" exige que la TSF applique les SFP appropriées lors de l'exportation de données de l'utilisateur à l'extérieur de la TSF. Les données de l'utilisateur exportées par cette fonction sont exportées sans les attributs de sécurité qui leur sont associés.

186 Le composant "FDP_ETC.2 Exportation de données de l'utilisateur avec attributs de sécurité" exige que la TSF applique les SFP appropriées en utilisant une fonction qui associe précisément et sans ambiguïté les attributs de sécurité avec les données de l'utilisateur qui sont exportées.

Administration : FDP_ETC.1

187 Il n'y a pas d'activités d'administration prévues pour ce composant.

Administration : FDP_ETC.2

188 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) les règles complémentaires de contrôle de l'exportation pourraient être configurables par un utilisateur ayant un rôle défini.

Audit : FDP_ETC.1, FDP_ETC.2

189 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

a) Minimal : exportation réussie d'informations;

b) Elémentaire : toutes les tentatives d'exportation d'informations.

FDP_ETC.1 Exportation de données de l'utilisateur sans attributs de sécurité

Hiérarchique à : aucun autre composant.

FDP_ETC.1.1 **La TSF doit appliquer la ou les [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] lors de l'exportation de données de l'utilisateur, contrôlées par la ou les SFP, vers l'extérieur du TSC.**

FDP_ETC.1.2 **La TSF doit exporter les données de l'utilisateur sans les attributs de sécurité associés aux données de l'utilisateur.**

Dépendances : [**FDP_ACC.1 Contrôle d'accès partiel**, **ou**
FDP_IFC.1 Contrôle de flux d'information partiel]

FDP_ETC.2 Exportation de données de l'utilisateur avec attributs de sécurité

Hiérarchique à : aucun autre composant.

FDP_ETC.2.1 **La TSF doit appliquer la ou les SFP [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] lors de l'exportation de données de l'utilisateur, contrôlées par la ou les SFP, vers l'extérieur du TSC.**

FDP_ETC.2.2 **La TSF doit exporter les données de l'utilisateur avec les attributs de sécurité qui leur sont associés.**

FDP_ETC.2.3 **La TSF doit garantir que les attributs de sécurité, lorsqu'ils sont exportés vers l'extérieur du TSC, sont associés sans ambiguïté aux données de l'utilisateur qui sont exportées.**

FDP_ETC.2.4 **La TSF doit appliquer les règles suivantes lors de l'exportation de données de l'utilisateur en provenance du TSC : [affectation : *règles complémentaires de contrôle d'exportation*].**

Dépendances : [**FDP_ACC.1 Contrôle d'accès partiel**, **ou**
FDP_IFC.1 Contrôle de flux d'information partiel]

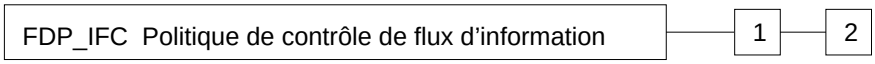
6.5 Politique de contrôle de flux d'information (FDP_IFC)

Comportement de la famille

190 La présente famille identifie les SFP de contrôle de flux d'information (par leur nom) et définit le domaine d'application des politiques qui constituent la partie identifiée du contrôle de flux d'information de la TSP. Ce domaine d'application est caractérisé par trois ensembles : les sujets contrôlés par la politique, les informations contrôlées par la politique et les opérations couvertes par la politique qui déclenchent le transfert d'informations contrôlées vers et en provenance de sujets contrôlés. Les critères permettent l'existence de multiples politiques ayant chacune un nom unique. Ceci est réalisé en utilisant de façon itérative les composants de la présente famille pour chacune des politiques de contrôle de flux d'information désignées. Les règles définissant les fonctionnalités d'une SFP de contrôle de flux d'information sont définies dans d'autres familles telles que FDP_IFF et FDP_SDI. Les noms des SFP de contrôle de flux d'information identifiés dans FDP_IFC sont destinés à être utilisés dans tous les composants fonctionnels qui nécessitent une opération d'affectation ou de sélection d'une "SFP de contrôle de flux d'information."

191 Le mécanisme de la TSF contrôle le flux d'information conformément à la SFP de contrôle de flux d'information. Les opérations qui modifieraient les attributs de sécurité des informations ne sont en général pas autorisées car cela constituerait une violation d'une SFP de contrôle de flux d'information. Cependant, de telles opérations peuvent être autorisées en tant qu'exceptions à la SFP de contrôle de flux d'information, si cela est spécifié explicitement.

Classement des composants



192 Le composant "**FDP_IFC.1 Contrôle de flux d'information partiel**" exige que chaque SFP de contrôle de flux d'information identifiée soit mise en place pour un sous-ensemble des opérations possibles sur un sous-ensemble des flux d'information dans la TOE.

193 Le composant "FDP_IFC.2 Contrôle de flux d'information complet" exige que chaque SFP de contrôle de flux d'information identifiée traite toutes les opérations sur les sujets et les informations couvertes par cette SFP. Il exige de plus que tous les flux d'information et toutes les opérations sur le TSC soient couverts par au moins une SFP de contrôle de flux d'information identifiée. Conjointement avec le composant FPT_RVM.1, ceci correspond à l'aspect "systématiquement appelé" d'un moniteur de référence.

Administration : FDP_IFC.1, FDP_IFC.2

194 Il n'y a pas d'activités d'administration prévues pour ce composant.

Audit : FDP_IFC.1, FDP_IFC.2

195 Il n'y a pas d'actions identifiées qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FDP_IFC.1 Contrôle de flux d'information partiel

Hiérarchique à : aucun autre composant.

FDP_IFC.1.1 **La TSF doit appliquer la [affectation : *SFP de contrôle de flux d'information*] aux [affectation : *liste des sujets, des informations et des opérations couvertes par la SFP qui déclenchent le transfert d'informations contrôlées vers et en provenance de sujets contrôlés*].**

Dépendances : **FDP_IFF.1 Attributs de sécurité simples**

FDP_IFC.2 Contrôle de flux d'information complet

Hiéarchique à : FDP_IFC.1

FDP_IFC.2.1 La TSF doit appliquer la [affectation : *SFP de contrôle de flux d'information*] aux [affectation : *liste des sujets* et *informations*] et **toutes les opérations couvertes par la SFP qui déclenchent le transfert de ces informations vers et en provenance des sujets.**

FDP_IFC.2.2 **La TSF doit garantir que toutes les opérations qui déclenchent le transfert d'une information quelconque du TSC vers et en provenance de tout sujet du TSC sont couvertes par une SFP de contrôle de flux d'information.**

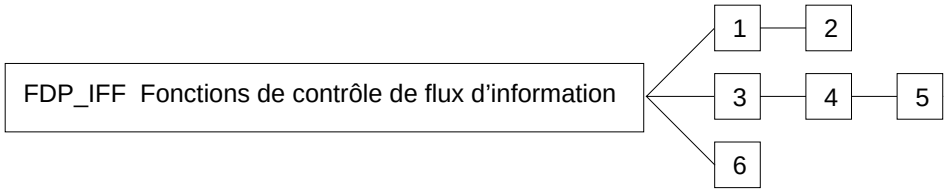
Dépendances : **FDP_IFF.1 Attributs de sécurité simples**

6.6 Fonctions de contrôle de flux d'information (FDP_IFF)

Comportement de la famille

196 La présente famille décrit les règles concernant les fonctions spécifiques qui peuvent implémenter les SFP de contrôle de flux d'information citées dans FDP_IFC, qui spécifie également le domaine d'application de la politique. Cette famille est constituée de deux types d'exigences : le premier concerne les problèmes communs aux fonctions traitant de flux d'information et le second concerne les flux d'information illicites (i.e. des canaux cachés). Cette distinction vient du fait que les problèmes relatifs aux flux d'information illicites sont, en quelque sorte, orthogonaux au reste de la SFP de contrôle de flux d'information. Par leur nature, ils contournent la SFP de contrôle de flux d'information, ce qui aboutit à une violation de cette politique. En tant que tels, ils nécessitent des fonctions spéciales qui permettent soit de limiter, soit d'éviter leur apparition.

Classement des composants



197 Le composant "**FDP_IFF.1 Attributs de sécurité simples**" impose des attributs de sécurité aux informations, aux sujets qui déclenchent le transfert de ces informations ainsi qu'aux sujets qui reçoivent ces informations. Ce composant spécifie les règles qui doivent être appliquées par la fonction et décrit comment les attributs de sécurité sont choisis par la fonction.

198 Le composant "FDP_IFF.2 Attributs de sécurité hiérarchiques" développe les exigences du composant "**FDP_IFF.1 Attributs de sécurité simples**" en exigeant que toutes les SFP de contrôle de flux d'information dans la TSP utilisent des attributs de sécurité hiérarchiques qui forment un treillis.

199 Le composant "FDP_IFF.3 Flux d'information illicites limités" exige que la SFP couvre les flux d'information illicites mais ne les élimine pas nécessairement.

200 Le composant "FDP_IFF.4 Élimination partielle des flux d'information illicites" exige que la SFP couvre l'élimination de certains flux d'information illicites (mais pas nécessairement de tous).

201 Le composant "FDP_IFF.5 Aucun flux d'information illicite" exige que la SFP couvre l'élimination de tous les flux d'information illicites.

202 Le composant "FDP_IFF.6 Contrôle des flux d'information illicites" exige que la SFP contrôle les flux d'information illicites par rapport à des capacités maximum spécifiées.

Administration : FDP_IFF.1, FDP_IFF.2

203 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) l'administration des attributs utilisés pour prendre les décisions d'accès explicites.

Administration : FDP_IFF.3, FDP_IFF.4, FDP_IFF.5

204 Il n'y a pas d'activités d'administration prévues pour ces composants.

Administration : FDP_IFF.6

205 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) l'activation ou la désactivation de la fonction de contrôle;

b) la modification de la capacité maximum pour laquelle le contrôle s'effectue.

Audit : FDP_IFF.1, FDP_IFF.2, FDP_IFF.5

206 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : décisions d'autoriser les flux d'information demandés ;

b) Elémentaire : toutes les décisions relatives aux demandes de flux d'information ;

c) Détaillé : les attributs de sécurité spécifiques utilisés pour décider de la mise en oeuvre d'un flux d'information;

d) Détaillé : certains sous-ensembles spécifiques d'informations qui ont circulé conformément aux objectifs de la politique (e.g. audit de matériels en configuration dégradée).

Audit : FDP_IFF.3, FDP_IFF.4, FDP_IFF.6

207 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : décisions d'autoriser les flux d'information demandés ;

b) Elémentaire : toutes les décisions relatives aux demandes de flux d'information;

c) Elémentaire : l'utilisation de canaux de flux d'information illicites identifiés;

d) Détaillé : les attributs de sécurité spécifiques utilisés pour décider de la mise en œuvre d'un flux d'information;

e) Détaillé : certains sous-ensembles spécifiques d'informations qui ont circulé conformément aux objectifs de la politique (e.g. audit de matériels en configuration dégradée);

f) Audit détaillé : l'utilisation de canaux de flux d'information illicites identifiés avec une capacité maximum estimée dépassant une valeur spécifiée.

FDP_IFF.1 Attributs de sécurité simples

Hiérarchique à : aucun autre composant.

FDP_IFF.1.1 **La TSF doit appliquer la [affectation : *SFP de contrôle de flux d'information*] en fonction des types suivants d'attributs de sécurité de sujets et d'informations : [affectation : *le nombre minimum et le type des attributs de sécurité*].**

FDP_IFF.1.2 **La TSF doit autoriser un flux d'information entre un sujet contrôlé et des informations contrôlées par l'intermédiaire d'une opération contrôlée si les règles suivantes s'appliquent : [affectation : *pour chaque opération, les relations basées sur les attributs de sécurité qui doivent exister entre les attributs de sécurité du sujet et les attributs de sécurité des informations*].**

FDP_IFF.1.3 **La TSF doit appliquer les [affectation : *règles complémentaires de la SFP de contrôle de flux d'information*].**

FDP_IFF.1.4 **La TSF doit fournir ce qui suit [affectation : *liste des capacités complémentaires de la SFP*].**

FDP_IFF.1.5 **La TSF doit autoriser explicitement un flux d'information en fonction des règles suivantes : [affectation : *règles basées sur les attributs de sécurité, qui autorisent explicitement les flux d'information*].**

FDP_IFF.1.6 **La TSF doit interdire explicitement un flux d'information en fonction des règles suivantes : [affectation : *règles basées sur les attributs de sécurité, qui interdisent explicitement les flux d'information*].**

Dépendances : **FDP_IFC.1 Contrôle de flux d'information partiel**

FMT_MSA.3 Initialisation statique d'attribut

FDP_IFF.2 Attributs de sécurité hiérarchiques

Hiéarchique à : FDP_IFF.1

FDP_IFF.2.1 La TSF doit appliquer la [affectation : *SFP de contrôle de flux d'information*] sur la base des types suivants d'attributs de sécurité du sujet et des informations : [affectation : *le nombre minimum et le type des attributs de sécurité*].

FDP_IFF.2.2 La TSF doit autoriser un flux d'information entre un sujet contrôlé et des informations contrôlées par l'intermédiaire d'une opération contrôlée si les règles suivantes, **basées sur les relations ordonnées entre les attributs de sécurité** s'appliquent : [affectation : *pour chaque opération, les relations basées sur les attributs de sécurité qui doivent exister entre les attributs de sécurité du sujet et les attributs de sécurité des informations*].

FDP_IFF.2.3 La TSF doit appliquer la [affectation : *règles complémentaires de la SFP de contrôle de flux d'information*].

FDP_IFF.2.4 La TSF doit fournir les [affectation : *liste des capacités complémentaires de la SFP*].

FDP_IFF.2.5 La TSF doit autoriser explicitement un flux d'information sur la base des règles suivantes : [affectation : *règles, basées sur les attributs de sécurité, qui autorisent explicitement les flux d'information*].

FDP_IFF.2.6 La TSF doit interdire explicitement un flux d'information sur la base des règles suivantes : [affectation : *règles, basées sur les attributs de sécurité, qui interdisent explicitement les flux d'information*].

FDP_IFF.2.7 **La TSF doit appliquer les relations suivantes pour chaque paire valide d'attributs de sécurité de contrôle de flux d'information :**

a) il existe une fonction d'ordonnancement qui, étant donnés deux attributs de sécurité valides, détermine si les attributs de sécurité sont identiques, si un des attribut de sécurité est supérieur à l'autre ou si les attributs de sécurité ne sont pas comparables ; et

b) il existe un "plus petit majorant" dans l'ensemble des attributs de sécurité, tel que, étant donnée n'importe quelle paire d'attributs de sécurité valides, il existe un attribut de sécurité qui est supérieur ou égal aux deux attributs de sécurité valides ; et

c) il existe un "plus grand minorant" dans l'ensemble des attributs de sécurité, tel que, étant donnée n'importe quelle paire d'attributs de sécurité valides, il existe un attribut de sécurité qui n'est pas supérieur aux deux attributs de sécurité valides.

Dépendances : **FDP_IFC.1 Contrôle de flux d'information partiel**
FMT_MSA.3 Initialisation statique d'attribut

FDP_IFF.3 Flux d'information illicites limités

Hiérarchique à : aucun autre composant.

FDP_IFF.3.1 **La TSF doit appliquer la [affectation : *SFP de contrôle de flux d'information*] pour limiter la capacité de [affectation : *types de flux d'information illicites*] à [affectation : *capacité maximum*].**

Dépendances : **AVA_CCA.1 Analyse des canaux cachés**
FDP_IFC.1 Contrôle de flux d'information partiel

FDP_IFF.4 Élimination partielle des flux d'information illicites

Hiéarchique à : FDP_IFF.3

FDP_IFF.4.1 La TSF doit appliquer la [affectation : *SFP de contrôle de flux d'information*] pour limiter la capacité de [affectation : *types de flux d'information illicites*] à [affectation : *capacité maximum*].

FDP_IFF.4.2 **La TSF doit empêcher [affectation : *types de flux d'information illicites*].**

Dépendances : AVA_CCA.1 Analyse des canaux cachés
FDP_IFC.1 Contrôle de flux d'information partiel

FDP_IFF.5 Aucun flux d'information illicite

Hiéarchique à : FDP_IFF.4

FDP_IFF.5.1 **La TSF doit garantir qu'aucun flux d'information illicite n'existe pour contourner [affectation : *nom de la SFP de contrôle de flux d'information*].**

Dépendances : **AVA_CCA.3 Analyse exhaustive des canaux cachés**
FDP_IFC.1 Contrôle de flux d'information partiel

FDP_IFF.6 Contrôle des flux d'information illicites

Hiérarchique à : aucun autre composant.

FDP_IFF.6.1 **La TSF doit appliquer la [affectation : *SFP de contrôle de flux d'information*] pour surveiller [affectation : *types de flux d'information illicites*] quand elle dépasse [affectation : *capacité maximum*].**

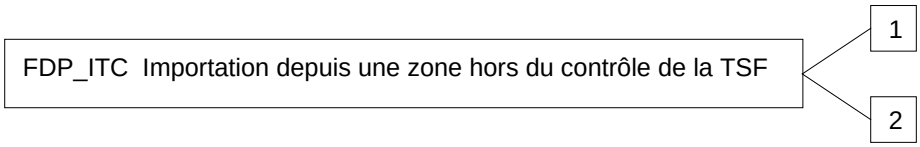
Dépendances : **AVA_CCA.1 Analyse des canaux cachés**
FDP_IFC.1 Contrôle de flux d'information partiel

6.7 Importation depuis une zone hors du contrôle de la TSF (FDP_ITC)

Comportement de la famille

208 La présente famille définit le mécanisme permettant l'introduction de données de l'utilisateur dans la TOE, de telle sorte qu'elles possèdent des attributs de sécurité appropriés et qu'elles soient correctement protégées. Elle concerne les limitations d'importation, la détermination des attributs de sécurité souhaités et l'interprétation des attributs de sécurité associés avec les données de l'utilisateur.

Classement des composants



209 Cette famille contient deux composants destinés à la préservation des attributs de sécurité de données de l'utilisateur importées à des fins de contrôle d'accès et pour des politiques de contrôle d'informations.

210 Le composant "**FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité**" exige que les attributs de sécurité représentent correctement les données de l'utilisateur et soient fournis séparément de l'objet.

211 Le composant "FDP_ITC.2 Importation de données de l'utilisateur avec attributs de sécurité" exige que les attributs de sécurité représentent correctement les données de l'utilisateur et soient associés de façon précise et non ambiguë avec les données de l'utilisateur importées en provenance de l'extérieur du TSC.

Administration : FDP_ITC.1, FDP_ITC.2

212 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) la modification des règles complémentaires de contrôle utilisées pour l'importation.

Audit : FDP_ITC.1, FDP_ITC.2

213 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : importation réussie de données de l'utilisateur, y compris tout attribut de sécurité;

b) Elémentaire : toutes les tentatives d'importation de données de l'utilisateur, y compris tout attribut de sécurité;

c) Détaillé : la spécification des attributs de sécurité associés aux données de l'utilisateur importées qui sont fournis par un utilisateur autorisé.

FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité

Hiérarchique à : aucun autre composant.

FDP_ITC.1.1 **La TSF doit appliquer la [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] lors de l'importation de données de l'utilisateur contrôlées par la SFP en provenance de l'extérieur du TSC.**

FDP_ITC.1.2 **La TSF doit ignorer tout attribut de sécurité associé aux données de l'utilisateur lorsqu'elles sont importées depuis l'extérieur du TSC.**

FDP_ITC.1.3 **La TSF doit appliquer les règles suivantes lors de l'importation de données de l'utilisateur contrôlées par la SFP en provenance de l'extérieur du TSC : [affectation : *règles complémentaires de contrôle d'importation*].**

Dépendances : [**FDP_ACC.1 Contrôle d'accès partiel**, **ou**
FDP_IFC.1 Contrôle de flux d'information partiel]
FMT_MSA.3 Initialisation statique d'attribut

FDP_ITC.2 Importation de données de l'utilisateur avec attributs de sécurité

Hiérarchique à : aucun autre composant.

FDP_ITC.2.1 **La TSF doit appliquer la [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] lors de l'importation de données de l'utilisateur contrôlées par la SFP en provenance de l'extérieur du TSC.**

FDP_ITC.2.2 **La TSF doit utiliser les attributs de sécurité associés aux données de l'utilisateur importées.**

FDP_ITC.2.3 **La TSF doit garantir que le protocole utilisé permet d'associer de façon non ambiguë les attributs de sécurité aux données de l'utilisateur reçues.**

FDP_ITC.2.4 **La TSF doit garantir que l'interprétation des attributs de sécurité des données de l'utilisateur importées est celle prévue par l'émetteur des données de l'utilisateur.**

FDP_ITC.2.5 **La TSF doit appliquer les règles suivantes lors de l'importation de données de l'utilisateur en provenance de l'extérieur du TSC, qui sont contrôlées par la SFP : [affectation : *règles complémentaires de contrôle d'importation*].**

Dépendances : [**FDP_ACC.1 Contrôle d'accès partiel**, **ou**
FDP_IFC.1 Contrôle de flux d'information partiel]
[**FTP_ITC.1 Canal de confiance inter-TSF**, **ou**
FTP_TRP.1 Chemin de confiance]
FPT_TDC.1 Cohérence élémentaire des données de la TSF inter-TSF

6.8 Transfert interne à la TOE (FDP_ITT)

Comportement de la famille

214 La présente famille fournit des exigences qui concernent la protection des données de l'utilisateur lorsqu'elles sont transférées entre des parties de la TOE par un canal interne. Elle peut différer des familles FDP_UCT et FDP_UIT qui permettent la protection des données de l'utilisateur lorsqu'elles sont transférées entre des TSF distinctes par un canal externe, et des familles FDP_ETC et FDP_ITC qui concernent le transfert de données vers ou depuis une zone hors de contrôle de la TSF.

Classement des composants

215 Le composant "FDP_ITT.1 Protection élémentaire d'un transfert interne" exige que les données de l'utilisateur soient protégées lorsqu'elles sont transmises entre des parties de la TOE.

216 Le composant "FDP_ITT.2 Séparation de données au cours d'une transmission en fonction d'attributs" exige, en complément au premier composant, une séparation des données basée sur la valeur des attributs relatifs à la SFP.

217 Le composant "FDP_ITT.3 Contrôle de l'intégrité" exige que la SF contrôle les données de l'utilisateur transmises entre des parties de la TOE afin de détecter des erreurs d'intégrité identifiées.

218 Le composant "FDP_ITT.4 Contrôle de l'intégrité basé sur des attributs" complète le troisième composant en autorisant que le type de contrôle d'intégrité soit différent en fonction de l'attribut relatif à la SFP.

Administration : FDP_ITT.1, FDP_ITT.2

219 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Adminstration" :

a) quand la TSF offre plusieurs méthodes pour protéger les données de l'utilisateur au cours de leur transmission entre des parties de la TOE physiquement séparées, la TSF pourrait fournir à un rôle prédéfini l'aptitude de sélectionner la méthode qui sera utilisée.

Administration : FDP_ITT.3, FDP_ITT.4

220 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) La spécification des actions à entreprendre en cas de détection d'une erreur d'intégrité pourrait être configurable.

Audit : FDP_ITT.1, FDP_ITT.2

221 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : transferts réussis de données de l'utilisateur, ainsi que l'identification de la méthode de protection utilisée;

b) Elémentaire : toute tentative de transfert de données de l'utilisateur, ainsi que la méthode de protection utilisée et toutes les erreurs qui sont survenues.

Audit : FDP_ITT.3, FDP_ITT.4

222 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : transferts réussis de données de l'utilisateur, ainsi que l'identification de la méthode de protection de l'intégrité utilisée;

b) Elémentaire : toute tentative de transfert de données de l'utilisateur, ainsi que la méthode de protection de l'intégrité utilisée et toutes les erreurs qui sont survenues;

c) Elémentaire : tentatives non autorisées pour changer de méthode de protection de l'intégrité;

d) Détaillé : les actions entreprises en cas de détection d'une erreur d'intégrité.

FDP_ITT.1 Protection élémentaire d'un transfert interne

Hiérarchique à : aucun autre composant.

FDP_ITT.1.1 **La TSF doit appliquer la ou les [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] pour empêcher la [sélection : *divulgation, modification ou perte d'utilisation*] de données de l'utilisateur au cours de leur transmission entre des parties de la TOE physiquement séparées.**

Dépendances : [**FDP_ACC.1 Contrôle d'accès partiel**, **ou**
FDP_IFC.1 Contrôle de flux d'information partiel]

FDP_ITT.2 Séparation de données au cours d'une transmission en fonction d'attributs

Hiérarchique à : FDP_ITT.1

FDP_ITT.2.1 La TSF doit appliquer la ou les [affectation : SFP de contrôle d'accès ou SFP de contrôle de flux d'information] pour empêcher la [sélection : divulgation, modification ou perte d'utilisation] de données de l'utilisateur au cours de leur transmission entre des parties de la TOE physiquement séparées.

FDP_ITT.2.2 **La TSF doit séparer les données contrôlées par la ou les SFP au cours de leur transmission entre des parties de la TOE physiquement séparées, en fonction de la valeur de ce qui suit : [affectation : *attributs de sécurité qui exigent une séparation*].**

Dépendances : [FDP_ACC.1 Contrôle d'accès partiel, ou
FDP_IFC.1 Contrôle de flux d'information partiel]

FDP_ITT.3 Contrôle de l'intégrité

Hiérarchique à : aucun autre composant.

FDP_ITT.3.1 **La TSF doit appliquer la ou les [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] pour contrôler les données de l'utilisateur au cours de leur transmission entre des parties de la TOE physiquement séparées, pour détecter les erreurs suivantes : [affectation : *erreurs d'intégrité*].**

FDP_ITT.3.2 **En cas de détection d'erreur d'intégrité de données, la TSF doit [affectation : *spécifier l'action à entreprendre en cas d'erreur d'intégrité*].**

Dépendances : [**FDP_ACC.1 Contrôle d'accès partiel**, **ou**
FDP_IFC.1 Contrôle de flux d'information partiel]
FDP_ITT.1 Protection élémentaire d'un transfert interne

FDP_ITT.4 Contrôle de l'intégrité basé sur des attributs

Hiérarchique à : FDP_ITT.3

FDP_ITT.4.1 La TSF doit appliquer la ou les [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] pour contrôler les données de l'utilisateur au cours de leur transmission entre des parties de la TOE physiquement séparées pour détecter les erreurs suivantes : [affectation : *erreurs d'intégrité*], **en fonction des attributs suivants : [affectation : *attributs de sécurité qui exigent des canaux de transmission séparés*].**

FDP_ITT.4.2 En cas de détection d'une erreur d'intégrité de données, la TSF doit [affectation : *spécifier l'action à entreprendre en cas d'erreur d'intégrité*].

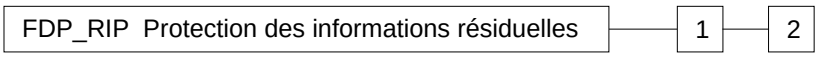
Dépendances : [FDP_ACC.1 Contrôle d'accès partiel, ou
FDP_IFC.1 Contrôle de flux d'information partiel]
FDP_ITT.2 Séparation de données au cours d'une transmission en fonction d'attributs

6.9 Protection des informations résiduelles (FDP_RIP)

Comportement de la famille

223 La présente famille répond au besoin de garantir que les informations détruites ne seront plus accessibles et que des objets nouvellement créés ne contiennent pas d'informations qui ne devraient pas être accessibles. Cette famille exige une protection des informations qui ont été logiquement supprimées ou effacées mais qui pourraient être encore présentes dans la TOE.

Classement des composants



224 Le composant "FDP_RIP.1 Protection partielle des informations résiduelles" exige que la TSF garantisse que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour un sous-ensemble défini des objets du TSC lors de l'allocation ou de la désallocation de la ressource.

225 Le composant "FDP_RIP.2 Protection totale des informations résiduelles" exige que la TSF garantisse que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour tous les objets du TSC lors de l'allocation ou de la désallocation de la ressource.

Administration : FDP_RIP.1, FDP_RIP.2

226 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) le choix de l'instant de la mise en œuvre de la protection des informations résiduelles (i.e. lors de l'allocation ou de la désallocation) pourrait être rendu configurable au sein de la TOE.

Audit : FDP_RIP.1, FDP_RIP.2

227 Il n'y a pas d'événements identifiés qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FDP_RIP.1 Protection partielle des informations résiduelles

Hiérarchique à : aucun autre composant.

FDP_RIP.1.1 La TSF doit garantir que toute information contenue précédemment dans une ressource est rendue indisponible lors de [sélection : l'*allocation de la ressource aux*, la *désallocation de la ressource des*] objets suivants : [affectation : *liste des objets*].

Dependencies: No dependencies

FDP_RIP.2 Protection totale des informations résiduelles

FDP_RIP.2.1 La TSF doit garantir que toute information contenue précédemment dans une ressource est rendue indisponible lors de [sélection : *l'allocation de la ressource à, la désallocation de la ressource de*] **tous les objets**.

Dependencies: No dependencies

6.10 Annulation (FDP_ROL)

Comportement de la famille

228 L’opération d’annulation consiste à annuler la dernière opération effectuée ou une série d’opérations effectuées, dans une limite donnée, comme par exemple une période de temps donnée, et de retourner à un état précédent connu. La famille "Annulation" offre l’aptitude d’annuler les effets d’une opération ou d’une série d’opérations afin de préserver l’intégrité des données de l’utilisateur.

Classement des composants

229 Le composant "FDP_ROL.1 Annulation élémentaire" répond au besoin d’annulation d’un nombre limité d’opérations effectuées dans les limites définies.

230 Le composant "FDP_ROL.2 Annulation avancée" répond au besoin d’annulation de toutes les opérations effectuées dans les limites définies.

Administration : FDP_ROL.1, FDP_ROL.2

231 Les actions suivantes pourraient être prises en compte pour les fonctions d’administration de la classe "FMT Administration" :

a) les limites dans lesquelles l’annulation peut être réalisée pourraient être un élément configurable au sein de la TOE;

b) la permission de procéder à une opération d’annulation pourrait être restreinte à un rôle bien défini.

Audit : FDP_ROL.1, FDP_ROL.2

232 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l’audit de sécurité" est spécifiée dans le PP ou la ST :

a) Minimal : toutes les opérations réussies d’annulation;

b) Elémentaire : toutes les tentatives de procéder à des opérations d’annulation;

c) Détaillé : toutes les tentatives de procéder à des opérations d’annulation, ainsi que l’identification des types d’opérations annulés.

FDP_ROL.1 Annulation élémentaire

Hiérarchique à : aucun autre composant.

FDP_ROL.1.1 **La TSF doit appliquer la ou les [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] pour autoriser l'annulation des [affectation : *liste des opérations*] sur les [affectation : *liste des objets*].**

FDP_ROL.1.2 **La TSF doit autoriser l'annulation des opérations dans les [affectation : *limites dans lesquelles l'annulation peut être effectuée*].**

Dépendances : [**FDP_ACC.1 Contrôle d'accès partiel**, **ou**
FDP_IFC.1 Contrôle de flux d'information partiel]

FDP_ROL.2 Annulation avancée

Hiéarchique à : FDP_ROL.1

FDP_ROL.2.1 La TSF doit appliquer la ou les [affectation : S*FP de contrôle d'accès ou SFP de contrôle de flux d'information*] pour autoriser l'annulation de **toutes les opérations** sur les [affectation : *liste des objets*].

FDP_ROL.2.2 La TSF doit autoriser l'annulation pour les opérations dans les [affectation : *limites dans lesquelles l'annulation peut être effectuée*].

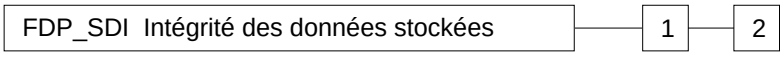
Dépendances : [FDP_ACC.1 Contrôle d'accès partiel, ou
FDP_IFC.1 Contrôle de flux d'information partiel]

6.11 Intégrité des données stockées (FDP_SDI)

Comportement de la famille

233 La présente famille fournit des exigences qui concernent la protection de données de l'utilisateur lorsqu'elles sont stockées au sein du TSC. Les erreurs d'intégrité peuvent affecter les données de l'utilisateur stockées en mémoire ou dans un dispositif de stockage. Cette famille diffère de la famille "FDP_ITT Transfert interne à la TOE" qui protège les données de l'utilisateur des erreurs d'intégrité lors de leur transfert au sein de la TOE.

Classement des composants



234 Le composant "FDP_SDI.1 Contrôle de l'intégrité des données stockées" exige que la SF contrôle les données de l'utilisateur stockées au sein du TSC pour rechercher des erreurs d'intégrité identifiées.

235 Le composant "FDP_SDI.2 Contrôle de l'intégrité des données stockées et action à entreprendre" complète le premier composant en autorisant des actions à entreprendre suite à la détection d'une erreur.

Administration : FDP_SDI.1

236 Il n'y a pas d'activités d'administration prévues pour ce composant.

Administration : FDP_SDI.2

237 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) les actions à entreprendre en cas de détection de toute erreur d'intégrité pourraient être configurables.

Audit : FDP_SDI.1

238 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : tentatives réussies de vérification de l'intégrité des données de l'utilisateur, ainsi qu'une indication du résultat de la vérification;

b) Elémentaire : toutes les tentatives de vérification de l'intégrité des données de l'utilisateur, ainsi qu'une indication du résultat de la vérification dans le cas où elle a été effectuée;

c) Détaillé : le type d'erreur d'intégrité survenue.

Audit : FDP_SDI.2

239 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : tentatives réussies de vérification de l'intégrité des données de l'utilisateur, ainsi qu'une indication du résultat de la vérification;

b) Elémentaire : toutes les tentatives de vérification de l'intégrité des données de l'utilisateur, ainsi qu'une indication du résultat de la vérification dans le cas où elle a été effectuée;

c) Détaillé : le type d'erreur d'intégrité survenue;

d) Détaillé : l'action entreprise en cas de détection d'une erreur d'intégrité.

FDP_SDI.1 Contrôle de l'intégrité des données stockées

Hiérarchique à : aucun autre composant.

FDP_SDI.1.1 La TSF doit contrôler les données de l'utilisateur stockées au sein du TSC à la recherche des [affectation : *erreurs d'intégrité*] sur tous les objets, en fonction des attributs suivants : [affectation : *attributs des données de l'utilisateur*].

Dependencies: No dependencies

FDP_SDI.2 Contrôle de l'intégrité des données stockées et action à entreprendre

Hiéarchique à : FDP_SDI.1

FDP_SDI.2.1 La TSF doit contrôler les données de l'utilisateur stockées au sein du TSC à la recherche [affectation : *erreurs d'intégrité*] sur tous les objets, en fonction des attributs suivants : [affectation : *attributs des données de l'utilisateur*].

FDP_SDI.2.2 En cas de détection d'une erreur d'intégrité, la TSF doit [affectation : *action à entreprendre*].

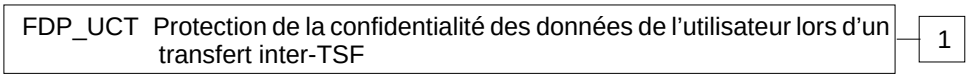
Dependencies: No dependencies

6.12 Protection de la confidentialité des données de l'utilisateur lors d'un transfert inter-TSF (FDP_UCT)

Comportement de la famille

240 La présente famille définit les exigences pour garantir la confidentialité des données de l'utilisateur lorsqu'elles sont transférées en utilisant un canal externe entre deux TOE distinctes ou entre des utilisateurs de TOE distinctes.

Classement des composants



241 Le composant "FDP_UCT.1 Confidentialité élémentaire lors d'un échange de données" a pour but de fournir une protection vis-à-vis de la divulgation de données de l'utilisateur lorsqu'elles sont transférées.

Administration : FDP_UCT.1

242 Il n'y a pas d'activités d'administration prévues pour ce composant.

Audit : FDP_UCT.1

243 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

a) Minimal : l'identité de tout utilisateur ou sujet utilisant les mécanismes d'échange de données;

b) Elémentaire : l'identité de tout utilisateur ou sujet non autorisé qui essaye d'utiliser les mécanismes d'échange de données;

c) Elémentaire : une référence aux noms ou à toute autre information utile pour identifier les données de l'utilisateur qui ont été transmises ou reçues. Ceci pourrait inclure les attributs de sécurité associés aux informations.

FDP_UCT.1 Confidentialité élémentaire lors d'un échange de données

Hiérarchique à : aucun autre composant.

FDP_UCT.1.1 La TSF doit appliquer la ou les [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] afin de pouvoir [sélection : *transmettre, recevoir*] des objets d'une façon qui les protège d'une divulgation non autorisée.

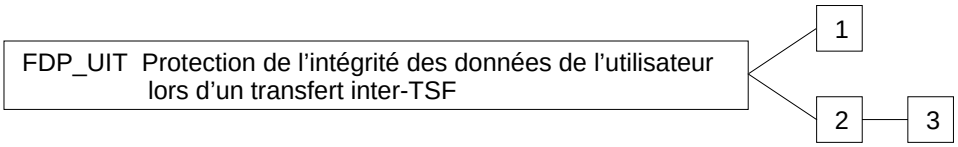
Dépendances : [**FTP_ITC.1 Canal de confiance inter-TSF**, **ou**
FTP_TRP.1 Chemin de confiance]
[**FDP_ACC.1 Contrôle d'accès partiel**, **ou**
FDP_IFC.1 Contrôle de flux d'information partiel]

6.13 Protection de l'intégrité des données de l'utilisateur lors d'un transfert inter-TSF (FDP_UIT)

Comportement de la famille

244 La présente famille définit les exigences pour assurer l'intégrité des données de l'utilisateur en transit entre la TSF et un autre produit TI de confiance et pour reconstituer les données à partir des erreurs détectables. Au minimum, cette famille contrôle l'intégrité des données de l'utilisateur contre des modifications. De plus, cette famille couvre différents moyens de corriger les erreurs d'intégrité détectées.

Classement des composants



245 Le composant "FDP_UIT.1 Intégrité lors d'un échange de données" concerne la détection d'erreurs liées à des modifications, suppressions, insertions et rejeux des données de l'utilisateur transmises.

246 Le composant "FDP_UIT.2 Reconstitution grâce à l'émetteur lors d'un échange de données" concerne la reconstitution des données originales de l'utilisateur par la TSF destinataire avec l'aide du produit TI de confiance à l'origine de l'émission.

247 Le composant "FDP_UIT.3 Reconstitution par le destinataire lors d'un échange de données" concerne la reconstitution des données originales de l'utilisateur par la TSF destinataire par ses propres moyens sans aucune aide du produit TI de confiance à l'origine de l'émission.

Administration : FDP_UIT.1, FDP_UIT.2, FDP_UIT.3

248 Il n'y a pas d'activités d'administration prévues pour ce composant.

Audit : FDP_UIT.1

249 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : l'identité de tout utilisateur ou sujet utilisant les mécanismes d'échange de données;

b) Elémentaire : l'identité de tout utilisateur ou sujet qui essaye d'utiliser les mécanismes d'échange de données, sans y être autorisé;

c) Elémentaire : une référence au nom ou à toute autre information utile pour identifier les données de l'utilisateur qui ont été transmises ou

reçues. Ceci pourrait inclure les attributs de sécurité associés aux informations;

d) Elémentaire : toute tentative identifiée de bloquer la transmission de données de l'utilisateur;

e) Détaillé : les types ou les effets de toute modification détectée des données de l'utilisateur qui ont été transmises.

Audit : FDP_UIT.2, FDP_UIT.3

250 Les événements suivants devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : l'identité de tout utilisateur ou sujet utilisant les mécanismes d'échange de données;

b) Minimal : reconstitution réussie après erreurs, ainsi que le type d'erreur qui a été détecté;

c) Elémentaire : l'identité de tout utilisateur ou sujet qui essaye d'utiliser les mécanismes d'échange de données, sans y être autorisé;

d) Elémentaire : une référence aux noms ou à toute autre information utile pour identifier les données de l'utilisateur qui ont été transmises ou reçues. Ceci pourrait inclure les attributs de sécurité associés aux informations;

e) Elémentaire : toute tentative identifiée de bloquer la transmission de données de l'utilisateur;

f) Détaillé : les types ou les effets de toute modification détectée des données de l'utilisateur qui ont été transmises.

FDP_UIT.1 Intégrité lors d'un échange de données

Hiérarchique à : aucun autre composant.

FDP_UIT.1.1 **La TSF doit appliquer la ou les [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] afin de pouvoir [sélection : *transmettre, recevoir*] des données de l'utilisateur d'une façon qui les protège d'erreurs de [sélection : *modification, suppression, insertion, rejeu*].**

FDP_UIT.1.2 **La TSF doit pouvoir déterminer lors de la réception des données de l'utilisateur si [sélection : une *modification*, une *suppression*, une *insertion*, *un rejeu*] a eu lieu.**

Dépendances : [**FDP_ACC.1 Contrôle d'accès partiel**, **ou**
FDP_IFC.1 Contrôle de flux d'information partiel]
[**FTP_ITC.1 Canal de confiance inter-TSF**, **ou**
FTP_TRP.1 Chemin de confiance]

FDP_UIT.2 Reconstitution grâce à l'émetteur lors d'un échange de données

Hiérarchique à : aucun autre composant.

FDP_UIT.2.1 **La TSF doit appliquer la ou les [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] afin de pouvoir reconstituer les données à partir de [affectation : *liste des erreurs compatibles avec une reconstitution*] avec l'aide du produit TI de confiance à l'origine de l'émission.**

Dépendances : [FDP_ACC.1 Contrôle d'accès partiel, ou
FDP_IFC.1 Contrôle de flux d'information partiel]
FDP_UIT.1 Intégrité lors d'un échange de données
FTP_ITC.1 Canal de confiance inter-TSF

FDP_UIT.3 Reconstitution par le destinataire lors d'un échange de données

Hiéarchique à : FDP_UIT.2

FDP_UIT.3.1 La TSF doit appliquer la ou les [affectation : *SFP de contrôle d'accès ou SFP de contrôle de flux d'information*] afin de pouvoir reconstituer les données à partir de [affectation : *liste des erreurs permettant une reconstitution*] **sans aucune aide du produit TI de confiance à l'origine de l'émission.**

Dépendances : [FDP_ACC.1 Contrôle d'accès partiel, ou
FDP_IFC.1 Contrôle de flux d'information partiel]
FDP_UIT.1 Intégrité lors d'un échange de données
FTP_ITC.1 Canal de confiance inter-TSF

7 Classe FIA : Identification et authentification

251 Les familles de la présente classe traitent des exigences pour que des fonctions établissent et contrôlent l'identité annoncée d'un utilisateur.

252 L'identification et l'authentification sont exigées pour garantir que sont associés aux utilisateurs les attributs de sécurité corrects (e.g. identité, groupes, rôles, niveaux de sécurité ou d'intégrité).

253 L'identification non ambiguë d'utilisateurs autorisés et l'association correcte d'attributs de sécurité à des utilisateurs et à des sujets sont critiques pour l'application des politiques de sécurité prévues. Les familles de cette classe couvrent la détermination et la vérification de l'identité d'utilisateurs, la détermination de leur droit à interagir avec la TOE et l'association correcte d'attributs de sécurité à chaque utilisateur autorisé. D'autres classes d'exigences (e.g. protection des données de l'utilisateur, audit de sécurité) dépendent de l'identification et de l'authentification correctes des utilisateurs pour être efficaces.

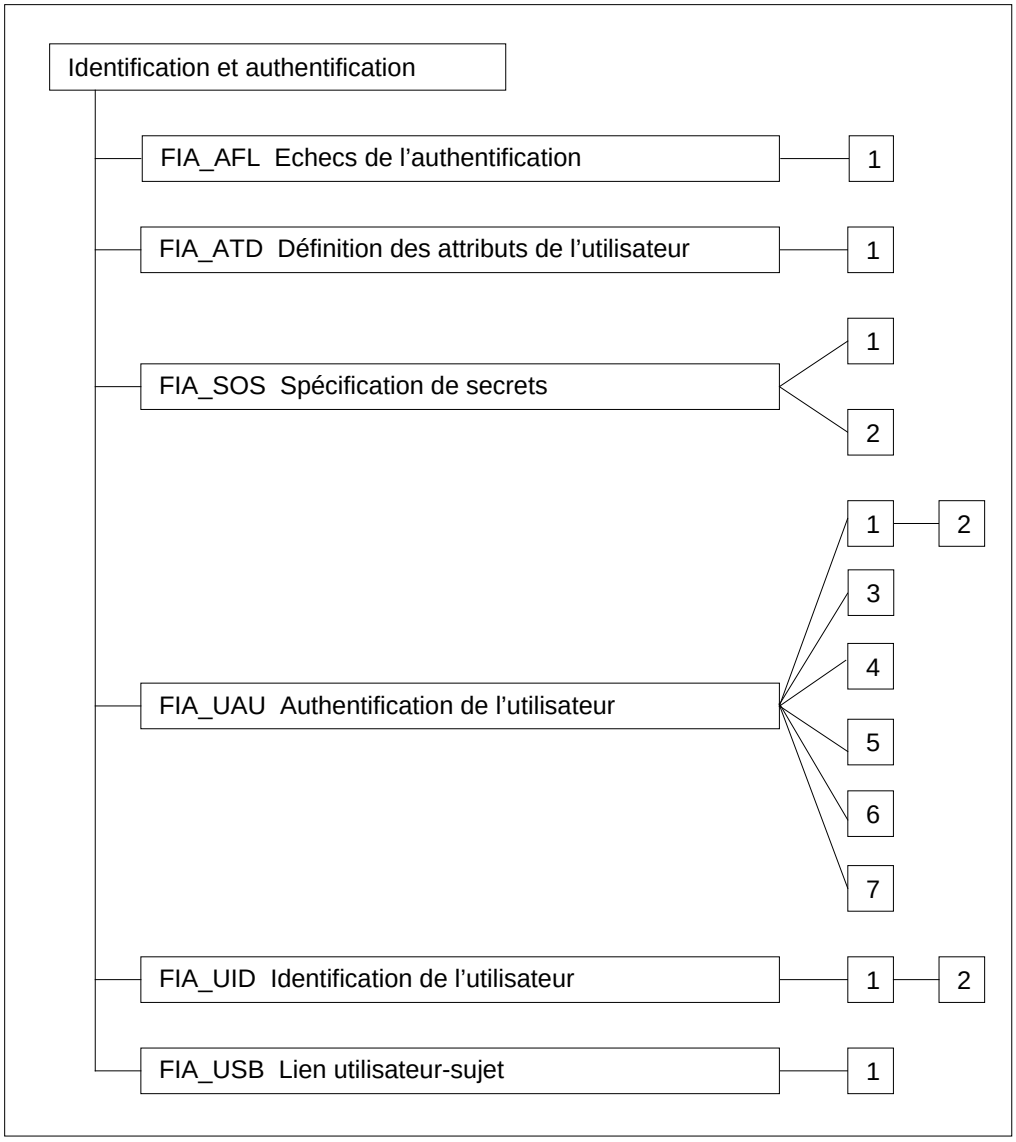


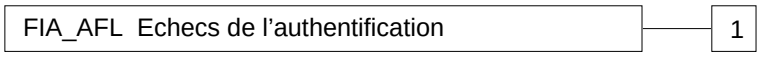
Figure 7.1 - Décomposition de la classe "Identification et authentification"

7.1 Echecs de l'authentification (FIA_AFL)

Comportement de la famille

254 La présente famille contient des exigences pour définir des paramètres pour un certain nombre de tentatives d'authentification infructueuses et les actions de la TSF en cas d'échecs de tentatives d'authentification. Les paramètres comprennent entre autres le nombre de tentatives d'authentification qui ont échoué et des seuils de durée.

Classement des composants



255 Le composant FIA_AFL.1 exige que la TSF soit capable d'arrêter le processus d'établissement d'une session après un nombre spécifié de tentatives d'authentification infructueuses d'un utilisateur. Il exige aussi que, après la clôture du processus d'établissement d'une session, la TSF soit capable de désactiver le compte de l'utilisateur ou le point d'entrée (e.g. station de travail) à partir duquel les tentatives ont été faites jusqu'à ce qu'une condition définie par un administrateur se réalise.

Administration : FIA_AFL.1

256 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) l'adminstration du seuil de tentatives d'authentification infructueuses ;

b) l'administration des actions à entreprendre dans le cas d'un échec de l'authentification.

Audit : FIA_AFL.1

257 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : l'atteinte du seuil de tentatives d'authentification infructueuses, les actions entreprises (e.g. désactivation d'un terminal) et la restauration qui s'en suit, quand cela est approprié, de l'état normal (e.g. réactivation d'un terminal).

FIA_AFL.1 Gestion d'un échec de l'authentification

Hiérarchique à : aucun autre composant.

FIA_AFL.1.1 **La TSF doit détecter quand [affectation : *nombre*] tentatives d'authentification infructueuses ont eu lieu en relation avec [affectation : *liste d'événements liés à l'authentification*].**

FIA_AFL.1.2 **Quand le nombre spécifié de tentatives d'authentification infructueuses a été atteint ou dépassé, la TSF doit [affectation : *liste d'actions*].**

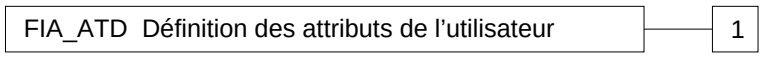
Dépendances : **FIA_UAU.1 Programmation de l'authentification**

7.2 Définition des attributs de l'utilisateur (FIA_ATD)

Comportement de la famille

258 Tous les utilisateurs autorisés peuvent avoir un ensemble d'attributs de sécurité, autres que l'identité de l'utilisateur, qui est utilisé pour appliquer la TSP. La présente famille définit les exigences pour associer les attributs de sécurité aux utilisateurs, dans la mesure où cela est nécessaire pour contribuer à l'application de la TSP.

Classement des composants



259 Le composant "FIA_ATD.1 Définition des attributs de l'utilisateur" autorise que des attributs de sécurité de l'utilisateur soient maintenus individuellement pour chaque utilisateur.

Administration : FIA_ATD.1

260 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) si cela est indiqué dans l'affectation, l'administrateur autorisé devrait être capable de définir des attributs de sécurité supplémentaires pour les utilisateurs.

Audit : FIA_ATD.1

261 Il n'y a pas d'actions identifiées qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FIA_ATD.1 Définition des attributs de l'utilisateur

Hiérarchique à : aucun autre composant.

FIA_ATD.1.1 La TSF doit maintenir la liste suivante d'attributs de sécurité appartenant à des utilisateurs individuels : [affectation : *liste d'attributs de sécurité*].

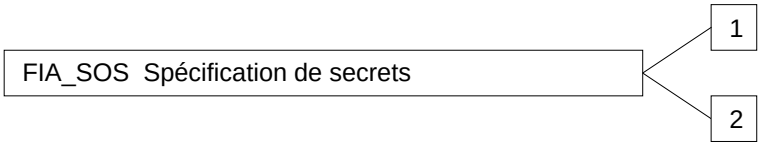
Dependencies: No dependencies

7.3 Spécification de secrets (FIA_SOS)

Comportement de la famille

262 La présente famille définit des exigences pour les mécanismes qui appliquent des métriques de qualité définies aux secrets fournis et qui génèrent des secrets répondant à la métrique définie.

Classement des composants



263 Le composant “FIA_SOS.1 Vérification de secrets” exige que la TSF vérifie que les secrets répondent à des métriques de qualité définies.

264 Le composant “FIA_SOS.2 Génération de secrets par la TSF” exige que la TSF soit capable de générer des secrets qui répondent à des métriques de qualité définies.

Administration : FIA_SOS.1

265 Les actions suivantes pourraient être prises en compte pour les fonctions d’administration de la classe FMT :

a) l’administration des métriques utilisées pour contrôler les secrets.

Administration : FIA_SOS.2

266 Les actions suivantes pourraient être prises en compte pour les fonctions d’administration de la classe FMT :

a) l’administration des métriques utilisées pour générer les secrets.

Audit : FIA_SOS.1, FIA_SOS.2

267 Les actions suivantes devraient être auditables dans le cas où la famille “FAU_GEN Génération des données de l’audit de sécurité” est incluse dans le PP ou la ST :

a) Minimal : rejet par la TSF de tout secret testé ;

b) Elémentaire : rejet ou acceptation par la TSF de tout secret testé ;

c) Détaillé : identification de tout changement des métriques de qualité définies.

FIA_SOS.1 Vérification de secrets

Hiérarchique à : aucun autre composant.

FIA_SOS.1.1 La TSF doit offrir un mécanisme pour contrôler que les secrets répondent à [affectation : *une métrique de qualité définie*].

Dependencies: No dependencies

FIA_SOS.2 Génération de secrets par la TSF

Hiérarchique à : aucun autre composant.

FIA_SOS.2.1 La TSF doit offrir un mécanisme pour générer des secrets qui répondent à [affectation : *une métrique de qualité définie*].

FIA_SOS.2.2 La TSF doit être capable de rendre obligatoire l'utilisation de secrets qu'elle a générés pour [affectation : *liste de fonctions de la TSF*].

Dependencies: No dependencies

7.4 Authentification de l'utilisateur (FIA_UAU)

Comportement de la famille

268 La présente famille définit les types de mécanismes d'authentification de l'utilisateur gérés par la TSF. Cette famille définit également les attributs nécessaires sur lesquels doivent être basés les mécanismes d'authentification de l'utilisateur.

Classement des composants

269 Le composant "**FIA_UAU.1 Programmation de l'authentification**" autorise un utilisateur à exécuter certaines actions avant que son identité ne soit authentifiée.

270 Le composant "FIA_UAU.2 Authentification de l'utilisateur avant toute action" exige que les utilisateurs s'authentifient eux-mêmes avant que toute action ne soit autorisée par la TSF.

271 Le composant "FIA_UAU.3 Authentification infalsifiable" exige que le mécanisme d'authentification soit capable de détecter et d'empêcher l'utilisation de données d'authentification qui ont été contrefaites ou copiées.

272 Le composant "FIA_UAU.4 Mécanismes d'authentification à usage unique" exige un mécanisme d'authentification qui fonctionne avec des données d'authentification à usage unique.

273 Le composant "FIA_UAU.5 Mécanismes d'authentification multiple" exige que différents mécanismes d'authentification soient fournis et utilisés pour authentifier les identités d'un utilisateur pour des événements spécifiques.

274 Le composant "FIA_UAU.6 Réauthentification" exige l'aptitude de spécifier des événements pour lesquels l'utilisateur doit être réauthentifié.

275 Le composant “FIA_UAU.7 Authentification avec retours protégés” exige que seules des informations limitées soient retournées à l’utilisateur pendant l’authentification.

Administration : FIA_UAU.1

276 Les actions suivantes pourraient être prises en compte pour les fonctions d’administration de la classe FMT :

a) l’administration des données d’authentification par un administrateur ;

b) l’administration des données d’authentification par l’utilisateur associé ;

c) l’administration de la liste des actions qui peuvent être entreprises avant que l’utilisateur ne soit authentifié.

Administration : FIA_UAU.2

277 Les actions suivantes pourraient être prises en compte pour les fonctions d’administration de la classe FMT :

a) l’adminsitration des données d’authentification par un administrateur ;

b) l’administration des données d’authentification par l’utilisateur associé à ces données.

Administration : FIA_UAU.3, FIA_UAU.4, FIA_UAU.7

278 Il n’y a pas d’activités d’administration prévues.

Administration : FIA_UAU.5

279 Les actions suivantes pourraient être prises en compte pour les fonctions d’administration de la classe FMT :

a) l’administration des mécanismes d’authentification ;

b) l’administration des règles d’authentification.

Administration : FIA_UAU.6

280 Les actions suivantes pourraient être prises en compte pour les fonctions d’administration de la classe FMT :

a) dans le cas où un administrateur autorisé pourrait demander une nouvelle authentification, l’administration inclut une demande de réauthentification.

Audit : FIA_UAU.1

281 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : utilisation infructueuse du mécanisme d'authentification ;

b) Elémentaire : toute utilisation du mécanisme d'authentification ;

c) Détaillé : toutes les actions transitant par la TSF effectuées avant l'authentification de l'utilisateur.

Audit : FIA_UAU.2

282 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : utilisation infructueuse du mécanisme d'authentification ;

b) Elémentaire : toute utilisation du mécanisme d'authentification.

Audit : FIA_UAU.3

283 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : détection de données d'authentification frauduleuses ;

b) Elémentaire : toutes les mesures immédiates prises et les résultats des vérifications effectuées sur les données frauduleuses.

Audit : FIA_UAU.4

284 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : tentatives de réutilisation de données d'authentification.

Audit : FIA_UAU.5

285 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : la décision finale sur l'authentification ;

b) Elémentaire : le résultat de chaque mécanisme activé ainsi que la décision finale.

Audit : FIA_UAU.6

286 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : échec de réauthentification ;

b) Elémentaire : toutes les tentatives de réauthentification.

Audit : FIA_UAU.7

287 Il n'y a pas d'événements auditables prévus.

FIA_UAU.1 Programmation de l'authentification

Hiérarchique à : aucun autre composant.

FIA_UAU.1.1 **La TSF doit autoriser que [affectation : *liste d'actions transitant par la TSF*] pour le compte de l'utilisateur soient effectuées avant qu'il ne soit authentifié.**

FIA_UAU.1.2 **La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.**

Dépendances : **FIA_UID.1 Programmation de l'identification**

FIA_UAU.2 Authentification de l'utilisateur avant toute action

Hiéarchique à : FIA_UAU.1

FIA_UAU.2.1 La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser **toute autre action transitant par la TSF** pour le compte de cet utilisateur.

Dépendances : **FIA_UID.1 Programmation de l'identification**

FIA_UAU.3 Authentification infalsifiable

Hiérarchique à : aucun autre composant.

FIA_UAU.3.1 **La TSF doit [sélection : *détecter, empêcher*] l'utilisation de données d'authentification qui ont été contrefaites par un utilisateur quelconque de la TSF.**

FIA_UAU.3.2 **La TSF doit [sélection : *détecter, empêcher*] l'utilisation de données d'authentification qui ont été copiées par tout autre utilisateur de la TSF.**

Dependencies: No dependencies

FIA_UAU.4 Mécanismes d'authentification à usage unique

Hiérarchique à : aucun autre composant.

FIA_UAU.4.1 **La TSF doit empêcher la réutilisation des données d'authentification liées à [affectation : *mécanisme(s) d'authentification identifié(s)*].**

Dependencies: No dependencies

FIA_UAU.5 Mécanismes d'authentification multiple

Hiérarchique à : aucun autre composant.

FIA_UAU.5.1 **La TSF doit fournir [affectation : *liste de mécanismes d'authentification multiple*] pour contribuer à l'authentification de l'utilisateur.**

FIA_UAU.5.2 **La TSF doit authentifier l'identité annoncée de tout utilisateur selon [affectation : *règles décrivant comment les mécanismes d'authentification multiple procurent l'authentification*].**

Dependencies: No dependencies

FIA_UAU.6 Réauthentification

Hiérarchique à : aucun autre composant.

FIA_UAU.6.1 **La TSF doit réauthentifier l'utilisateur dans les conditions suivantes [affectation : *liste des conditions pour lesquelles une réauthentification est exigée*].**

Dependencies: No dependencies

FIA_UAU.7 Authentification avec retours protégés

Hiérarchique à : aucun autre composant.

FIA_UAU.7.1 **La TSF ne doit fournir que [affectation : *liste des informations retournées*] à l'utilisateur pendant que l'authentification est en cours.**

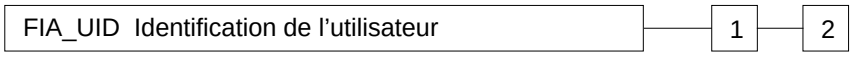
Dépendances : **FIA_UAU.1 Programmation de l'authentification**

7.5 Identification d'un utilisateur (FIA_UID)

Comportement de la famille

288 La présente famille définit les conditions pour lesquelles il est exigé que les utilisateurs s'identifient avant d'effectuer tout autre action devant transiter par la TSF qui nécessite l'identification de l'utilisateur.

Classement des composants



289 Le composant "**FIA_UID.1 Programmation de l'identification**" autorise les utilisateurs à effectuer certaines actions avant d'être identifiés par la TSF.

290 Le composant "FIA_UID.2 Identification de l'utilisateur avant toute action" exige que les utilisateurs s'identifient avant qu'une action quelconque ne soit autorisée par la TSF.

Administration : FIA_UID.1

291 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) l'administration de l'identité de l'utilisateur ;

b) l'administration des listes d'actions, dans le cas où un administrateur autorisé peut changer les actions autorisées avant une identification.

Administration : FIA_UID.2

292 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) l' administration de l'identité de l'utilisateur.

Audit : FIA_UID.1, FIA_UID.2

293 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : utilisation infructueuse du mécanisme d'identification de l'utilisateur, avec l'identité de l'utilisateur fournie ;

b) Elémentaire : toute utilisation du mécanisme d'identification de l'utilisateur, avec l'identité de l'utilisateur fournie.

FIA_UID.1 Programmation de l'identification

Hiérarchique à : aucun autre composant.

FIA_UID.1.1 **La TSF doit autoriser que [affectation : *liste d'actions transitant par la TSF*] pour le compte de l'utilisateur soient effectuées avant qu'il ne soit identifié.**

FIA_UID.1.2 **La TSF doit exiger que chaque utilisateur soit identifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.**

Dependencies: No dependencies

FIA_UID.2 Identification de l'utilisateur avant toute action

Hiéarchique à : FIA_UID.1

FIA_UID.2.1 La TSF doit exiger que chaque utilisateur soit identifié avec succès avant d'autoriser **toute autre action transitant par la TSF** pour le compte de cet utilisateur.

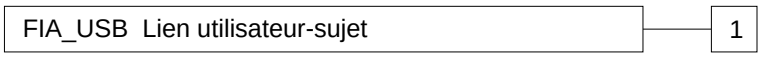
Dependencies: No dependencies

7.6 Lien utilisateur-sujet (FIA_USB)

Comportement de la famille

294 Un utilisateur authentifié active habituellement un sujet afin d'utiliser la TOE. Les attributs de sécurité de l'utilisateur sont associés (en totalité ou en partie) à ce sujet. La présente famille définit des exigences pour créer et maintenir la relation entre les attributs de sécurité de l'utilisateur et un sujet agissant pour le compte de cet utilisateur.

Classement des composants



295 Le composant "FIA_USB.1 Lien utilisateur-sujet" exige la maintenance de la relation entre les attributs de sécurité de l'utilisateur et un sujet agissant pour le compte de cet utilisateur.

Administration : FIA_USB.1

296 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) un administrateur autorisé peut définir des attributs de sécurité du sujet par défaut.

Audit : FIA_USB.1

297 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : établissement infructueux de lien entre les attributs de sécurité de l'utilisateur et un sujet (e.g. création d'un sujet) ;

b) Elémentaire : réussite et échec de l'établissement de lien entre les attributs de sécurité de l'utilisateur et un sujet (e.g. réussite et échec de la création d'un sujet).

FIA_USB.1 Lien utilisateur-sujet

Hiérarchique à : aucun autre composant.

FIA_USB.1.1 **La TSF doit relier les attributs de sécurité appropriés de l'utilisateur avec les sujets agissant pour le compte de cet utilisateur.**

Dépendances : **FIA_ATD.1 Définition des attributs de l'utilisateur**

8 Classe FMT : Administration de la sécurité

298 La présente classe est destinée à définir l'administration de plusieurs aspects de la TSF : attributs de sécurité, données et fonctions de la TSF. Les différents rôles d'administration et leurs interactions, comme par exemple la séparation des privilèges, peuvent être spécifiés.

299 Cette classe a plusieurs objectifs :

a) l'administration des données de la TSF qui inclut par exemple les messages aux utilisateurs ;

b) l'administration des attributs de sécurité qui inclut par exemple les listes de contrôle d'accès et les listes de privilèges ;

c) l'administration des fonctions de la TSF qui inclut par exemple la sélection des fonctions et les règles ou les conditions qui influencent le comportement de la TSF ;

d) la définition des rôles de sécurité.

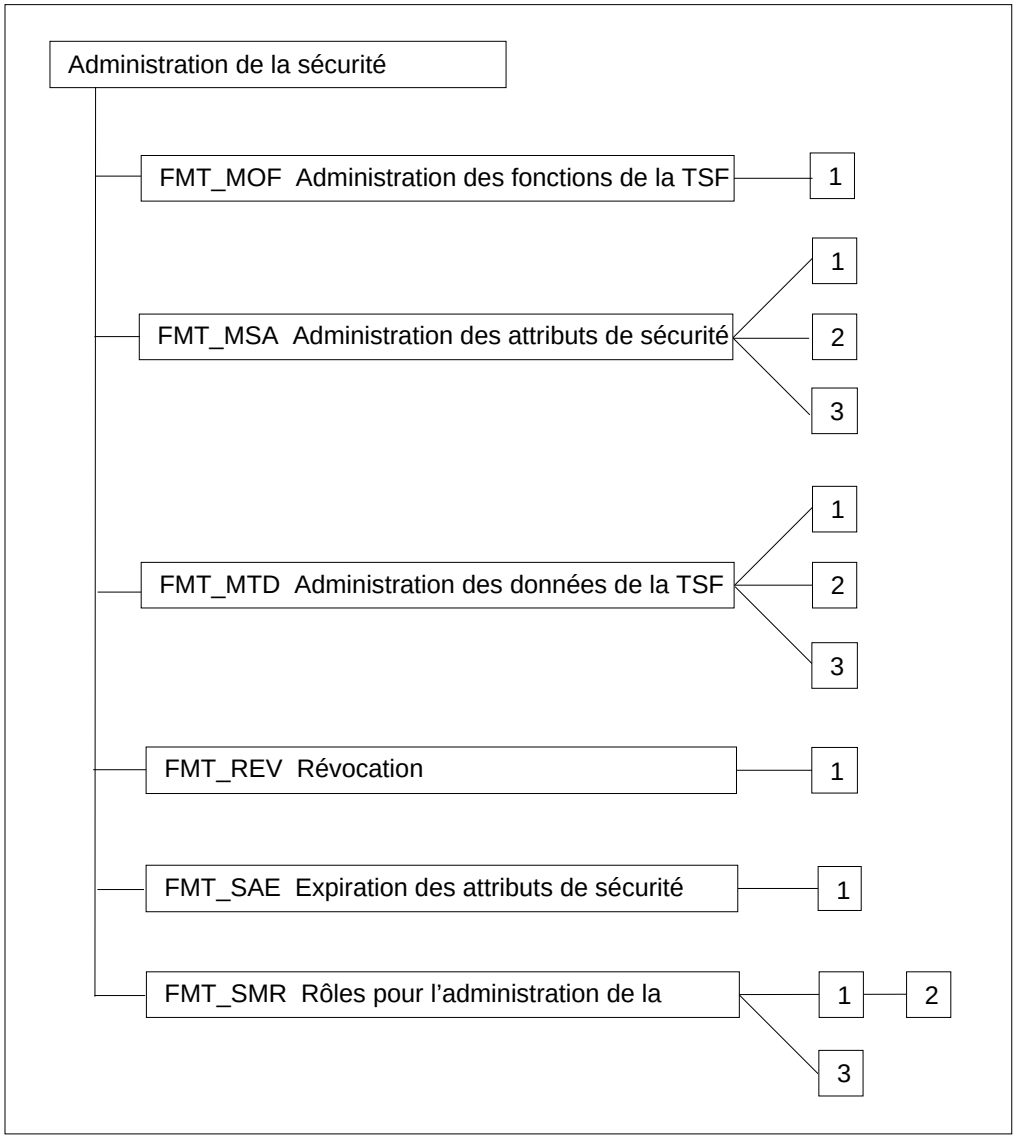


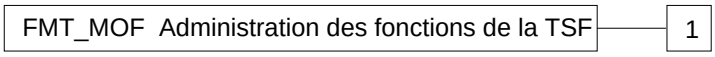
Figure 8.1 - Décomposition de la classe "Administration de la sécurité"

8.1 Administration des fonctions dans la TSF (FMT_MOF)

Comportement de la famille

300 La présente famille permet à des utilisateurs autorisés de contrôler l'administration de fonctions dans la TSF. Les fonctions d'audit et les fonctions d'authentification multiple sont des exemples de fonctions de la TSF.

Classement des composants



301 Le composant "FMT_MOF.1 Administration du comportement des fonctions de sécurité" permet à des utilisateurs autorisés (rôles) de gérer le comportement des fonctions dans la TSF qui utilisent des règles ou ont des conditions spécifiées susceptibles d'être gérées.

Administration : FMT_MOF.1

302 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) l'administration du groupe de rôles qui peuvent interagir avec les fonctions dans la TSF.

Audit : FMT_MOF.1

303 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : toutes les modifications dans le comportement des fonctions dans la TSF.

FMT_MOF.1 Administration du comportement des fonctions de sécurité

Hiérarchique à : aucun autre composant.

FMT_MOF.1.1 La TSF doit restreindre l'aptitude de [sélection : *déterminer le comportement, désactiver, activer, modifier le comportement*] des fonctions [affectation : *liste des fonctions*] aux [affectation : *rôles autorisés identifiés*].

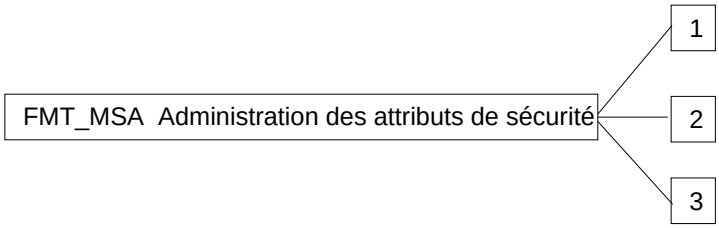
Dépendances : **FMT_SMR.1 Rôles de sécurité**

8.2 Administration des attributs de sécurité (FMT_MSA)

Comportement de la famille

304 La présente famille permet aux utilisateurs autorisés de contrôler l'administration des attributs de sécurité. Cette administration pourrait inclure les capacités de visualiser et modifier les attributs de sécurité.

Classement des composants



305 Le composant "FMT_MSA.1 Administration des attributs de sécurité" permet aux utilisateurs autorisés (rôles) de gérer les attributs de sécurité spécifiés.

306 Le composant "**FMT_MSA.2 Attributs de sécurité sûrs**" garantit que les valeurs assignées aux attributs de sécurité sont valides par rapport à l'état sûr.

307 Le composant "**FMT_MSA.3 Initialisation statique d'attribut**" garantit que les valeurs par défaut des attributs de sécurité sont de façon appropriée de nature soit permissive soit restrictive.

Administration : FMT_MSA.1

308 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) l'administration du groupe de rôles qui peut interagir avec les attributs de sécurité.

Administration : FMT_MSA.2

309 Il n'y a pas d'actions d'administration supplémentaires prévues pour ce composant.

Administration : FMT_MSA.3

310 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) l'administration du groupe de rôles qui peut spécifier les valeurs initiales ;

b) l'administration de l'attribution du caractère permissif ou restrictif aux valeurs par défaut pour une SFP de contrôle d'accès donnée.

Audit : FMT_MSA.1

311 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : toutes les modifications des valeurs des attributs de sécurité.

Audit : FMT_MSA.2

312 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : toutes les valeurs proposées et rejetées pour un attribut de sécurité ;

b) Détaillé : toutes les valeurs sûres proposées et acceptées pour un attribut de sécurité.

Audit : FMT_MSA.3

313 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : les modifications de l'attribution par défaut des règles permissives ou restrictives ;

b) Elémentaire : toutes les modifications des valeurs initiales des attributs de sécurité.

FMT_MSA.1 Administration des attributs de sécurité

Hiérarchique à : aucun autre composant.

FMT_MSA.1.1 La TSF doit mettre en œuvre la ou les [affectation : *SFP de contrôle d'accès, SFP de contrôle de flux d'informations*] pour restreindre aux [affectation : *les rôles autorisés identifiés*] l'aptitude de [sélection : *changer la valeur par défaut, interroger, modifier, supprimer,* [affectation : *autres opérations*]] les attributs de sécurité [affectation : *liste des attributs de sécurité*].

Dépendances : [**FDP_ACC.1 Contrôle d'accès partiel ou**
FDP_IFC.1 Contrôle de flux d'information partiel]
FMT_SMR.1 Rôles de sécurité

FMT_MSA.2 Attributs de sécurité sûrs

Hiérarchique à : aucun autre composant.

FMT_MSA.2.1 **La TSF doit garantir que seules des valeurs sûres sont acceptées pour les attributs de sécurité.**

Dépendances : **ADV_SPM.1 Modèle informel de politique de sécurité de la TOE**

[**FDP_ACC.1 Contrôle d'accès partiel ou**

FDP_IFC.1 Contrôle de flux d'information partiel]

FMT_MSA.1 Administration des attributs de sécurité

FMT_SMR.1 Rôles de sécurité

FMT_MSA.3 Initialisation statique d'attribut

Hiérarchique à : aucun autre composant.

FMT_MSA.3.1 **La TSF doit mettre en œuvre la ou les [affectation : *SFP de contrôle d'accès, SFP de contrôle de flux d'informations*] afin de fournir des valeurs par défaut [sélection : *restrictives, permissives, autres propriétés*] pour les attributs de sécurité qui sont utilisés pour appliquer la *SFP*.**

FMT_MSA.3.2 **La TSF doit permettre aux [affectation : *les rôles autorisés identifiés*] de spécifier des valeurs initiales alternatives pour remplacer les valeurs par défaut lorsqu'un objet ou une information est créé.**

Dépendances : **FMT_MSA.1 Administration des attributs de sécurité**

FMT_SMR.1 Rôles de sécurité

8.3 Administration des données de la TSF (FMT_MTD)

Comportement de la famille

314 La présente famille permet aux utilisateurs autorisés (rôles) de contrôler l' administration des données de la TSF. Les informations d'audit, les données de l'horloge, les paramètres de configuration du système et les autres paramètres de configuration de la TSF sont des exemples de données de la TSF.

Classement des composants

315 Le composant "**FMT_MTD.1 Administration des données de la TSF**" permet aux utilisateurs autorisés de gérer les données de la TSF.

316 Le composant "FMT_MTD.2 Administration des valeurs limites des données de la TSF" spécifie l'action à entreprendre lorsque les valeurs limites des données de la TSF sont atteintes ou dépassées.

317 Le composant "FMT_MTD.3 Données sûres de la TSF" garantit que les valeurs allouées aux données de la TSF sont valides par rapport à l'état sûr.

Administration : FMT_MTD.1

318 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) l'administration du groupe de rôles qui peut interagir avec les données de la TSF.

Administration : FMT_MTD.2

319 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) l'administration du groupe de rôles qui peut interagir avec les valeurs limites des données de la TSF.

Administration : FMT_MTD.3

320 Il n'y a pas d'actions d'administration supplémentaires prévues pour ce composant.

Audit : FMT_MTD.1

321 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : toutes les modifications des valeurs des données de la TSF.

Audit : FMT_MTD.2

322 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : toutes les modifications des valeurs limites des données de la TSF ;

b) Elémentaire : toutes les modifications des actions à entreprendre en cas de violation des valeurs limites.

Audit : FMT_MTD.3

323 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : Toutes les valeurs rejetées pour les données de la TSF.

FMT_MTD.1 Administration des données de la TSF

Hiérarchique à : aucun autre composant.

FMT_MTD.1.1 La TSF doit restreindre l'aptitude de [sélection : *changer une valeur par défaut, interroger, modifier, supprimer, effacer* [affectation : *autres opérations*]] les [affectation : *liste des données de la TSF*] aux [affectation : *les rôles autorisés identifiés*].

Dépendances : **FMT_SMR.1 Rôles de sécurité**

FMT_MTD.2 Administration des valeurs limites des données de la TSF

Hiérarchique à : aucun autre composant.

FMT_MTD.2.1 La TSF doit restreindre la spécification des valeurs limites des [affectation : *liste des données de la TSF*] aux [affectation : *les rôles autorisés identifiés*].

FMT_MTD.2.2 La TSF doit entreprendre les actions suivantes lorsque les données de la TSF atteignent les valeurs limites indiquées ou les dépassent : [affectation : *actions à entreprendre*].

Dépendances : **FMT_MTD.1 Administration des données de la TSF**

FMT_SMR.1 Rôles de sécurité

FMT_MTD.3 Données sûres de la TSF

Hiérarchique à : aucun autre composant.

FMT_MTD.3.1 La TSF doit garantir que seules des valeurs sûres sont acceptées pour les données de la TSF.

Dépendances : **ADV_SPM.1 Modèle informel de politique de sécurité de la TOE**

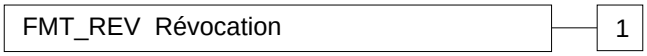
FMT_MTD.1 Administration des données de la TSF

8.4 Révocation (FMT_REV)

Comportement de la famille

324 Cette famille couvre la révocation des attributs de sécurité pour diverses entités dans une TOE.

Classement des composants



325 Le composant “FMT_REV.1 Révocation” permet d’appliquer la révocation d’attributs de sécurité à un certain moment.

Administration : FMT_REV.1

326 Les actions suivantes pourraient être prises en compte pour les fonctions d’administration de la classe “FMT Administration” :

a) l’administration du groupe de rôles qui peut demander la révocation des attributs de sécurité ;

b) l’administration de la liste des utilisateurs, des sujets, objets et autres ressources pour lesquels la révocation est possible ;

c) l’administration des règles de révocation.

Audit : FMT_REV.1

327 Les actions suivantes devraient être auditables dans le cas où la famille “FAU_GEN Génération des données de l’audit de sécurité” est incluse dans le PP ou la ST :

a) Minimal : révocation infructueuse d’attributs de sécurité ;

b) Elémentaire : toutes les tentatives de révocation d’attributs de sécurité.

FMT_REV.1 Révocation

Hiérarchique à : aucun autre composant.

FMT_REV.1.1 La TSF doit restreindre aux [affectation : *les rôles autorisés identifiés*] l’aptitude de révoquer les attributs de sécurité associés aux [sélection : *utilisateurs, sujets, objets, autres ressources complémentaires*] au sein du TSC.

FMT_REV.1.2 La TSF doit mettre en œuvre les règles [affectation : *spécification des règles de révocation*].

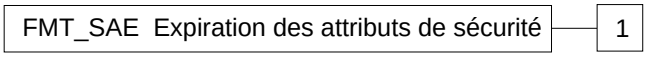
Dépendances : **FMT_SMR.1 Rôles de sécurité**

8.5 Expiration des attributs de sécurité (FMT_SAE)

Comportement de la famille

328 Cette famille couvre la capacité d'appliquer des limites temporelles à la validité d'attributs de sécurité.

Classement des composants



329 Le composant "FMT_SAE.1 Autorisation limitée dans le temps" offre la capacité pour un utilisateur autorisé de définir une date d'expiration pour des attributs de sécurité spécifiés.

Administration : FMT_SAE.1

330 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) administration de la liste des attributs de sécurité pour lesquels l'expiration doit s'appliquer ;

b) les actions à entreprendre si la date d'expiration est dépassée.

Audit : FMT_SAE.1

331 Les actions suivantes devraient être auditables dans le cas où la famille "FAU Audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : spécification de la date d'expiration pour un attribut ;

b) Elémentaire : action entreprise à la suite de l'expiration d'un attribut.

FMT_SAE.1 Autorisation limitée dans le temps

Hiérarchique à : aucun autre composant.

FMT_SAE.1.1 La TSF doit restreindre aux [affectation : *les rôles autorisés identifiés*] la capacité de spécifier une date d'expiration pour [affectation : *liste des attributs de sécurité pour lesquels l'expiration doit s'appliquer*].

FMT_SAE.1.2 Pour chacun de ces attributs de sécurité, la TSF doit être capable de [affectation : *liste des actions à entreprendre pour chaque attribut de sécurité*] après que la date d'expiration de l'attribut de sécurité soit passée.

Dépendances : **FMT_SMR.1 Rôles de sécurité**
FPT_STM.1 Horodatage fiable

8.6 Rôles pour l'administration de la sécurité (FMT_SMR)

Comportement de la famille

332 La présente famille est destinée au contrôle de l'affectation de différents rôles aux utilisateurs. Les droits associés à chaque rôle par rapport à l'administration de la sécurité sont décrits dans les autres familles de cette classe.

Classement des composants

333 Le composant "**FMT_SMR.1 Rôles de sécurité**" spécifie les rôles par rapport à la sécurité que la TSF reconnaît.

334 Le composant "FMT_SMR.2 Restrictions sur les rôles de sécurité" spécifie que, en complément de la spécification des rôles, certaines règles contrôlent les relations entre les rôles.

335 Le composant "FMT_SMR.3 Prise en charge des rôles" exige qu'une demande explicite soit formulée à la TSF pour la prise en charge d'un rôle.

Administration : FMT_SMR.1

336 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe "FMT Administration" :

a) l'administration du groupe des utilisateurs correspondant à un rôle.

Administration : FMT_SMR.2

337 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) l'administration du groupe des utilisateurs correspondant à un rôle ;

b) l'administration des conditions que le rôle doit satisfaire.

Administration : FMT_SMR.3

338 Il n'y a pas d'actions d'administration supplémentaires prévues pour ce composant.

Audit : FMT_SMR.1

339 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : les modifications du groupe des utilisateurs correspondant à un rôle ;

b) Détaillé : chaque utilisation des droits associés à un rôle.

Audit : FMT_SMR.2

340 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : les modifications du groupe des utilisateurs correspondant à un rôle ;

b) Minimal : les tentatives infructueuses d'utiliser un rôle résultant des conditions associées à ce rôle ;

c) Détaillé : chaque utilisation des droits associés à un rôle.

Audit : FMT_SMR.3

341 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : demande explicite pour la prise en charge d'un rôle.

FMT_SMR.1 Rôles de sécurité

Hiérarchique à : aucun autre composant.

FMT_SMR.1.1 **La TSF doit tenir à jour les rôles [affectation : *les rôles autorisés identifiés*].**

FMT_SMR.1.2 **La TSF doit être capable d'associer des utilisateurs à des rôles.**

Dépendances : **FIA_UID.1 Programmation de l'identification**

FMT_SMR.2 Restrictions sur les rôles de sécurité

Hiéarchique à : FMT_SMR.1

FMT_SMR.2.1 La TSF doit tenir à jour les rôles : [affectation : *les rôles autorisés identifiés*].

FMT_SMR.2.2 La TSF doit être capable d'associer des utilisateurs à des rôles.

FMT_SMR.2.3 **La TSF doit garantir que les conditions [affectation : *conditions associées aux différents rôles*] sont satisfaites.**

Dépendances : **FIA_UID.1 Programmation de l'identification**

FMT_SMR.3 Prise en charge des rôles

Hiérarchique à : aucun autre composant.

FMT_SMR.3.1 **La TSF doit exiger une demande explicite pour la prise en charge des rôles suivants : [affectation : *les rôles*].**

Dépendances : **FMT_SMR.1 Rôles de sécurité**

9 Classe FPR : Protection de la vie privée

342 La présente classe contient des exigences relatives à la protection de la vie privée. Ces exigences fournissent à un utilisateur une protection contre la découverte et le mauvais usage de son identité par d'autres utilisateurs.

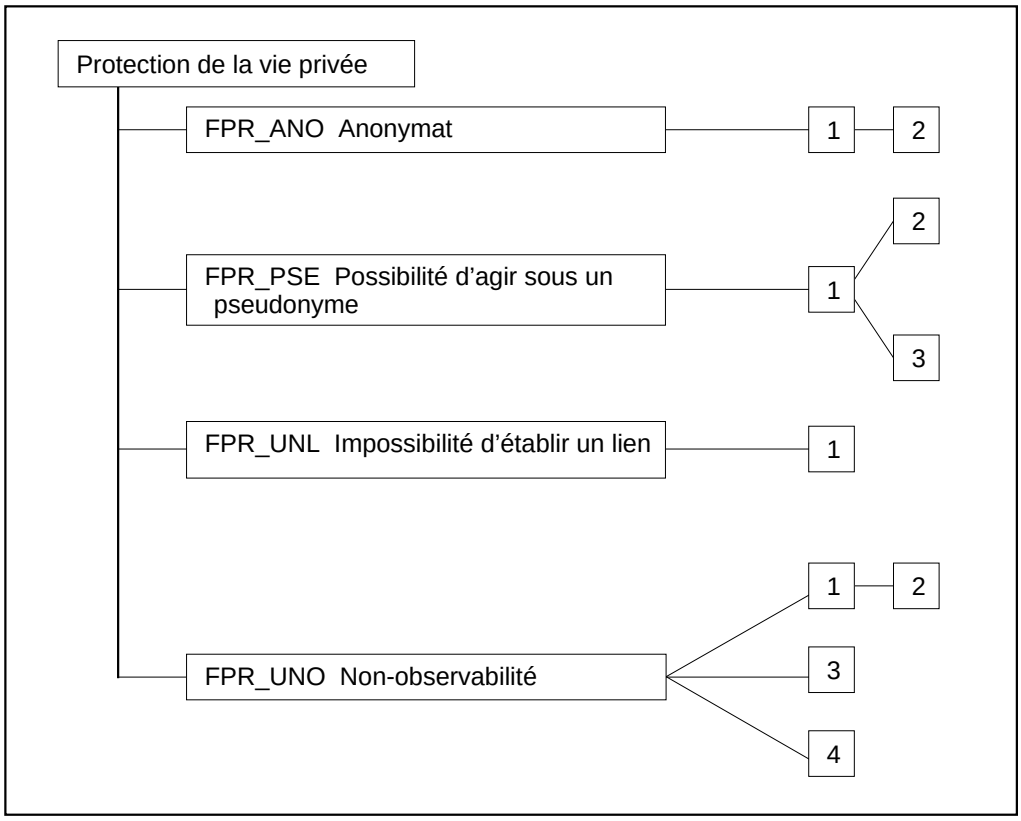


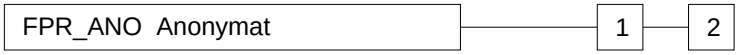
Figure 9.1 - Décomposition de la classe "Protection de la vie privée"

9.1 Anonymat (FPR_ANO)

Comportement de la famille

343 La présente famille garantit qu'un utilisateur peut utiliser une ressource ou un service sans révéler son identité d'utilisateur. Les exigences de la famille "Anonymat" permettent une protection de l'identité d'un utilisateur. Cette famille n'est pas prévue pour protéger l'identité d'un sujet.

Classement des composants



344 Le composant "**FPR_ANO.1 Anonymat**" exige que d'autres utilisateurs ou sujets soient incapables de déterminer l'identité d'un utilisateur associé à un sujet ou à une opération.

345 Le composant "FPR_ANO.2 Anonymat sans demande d'informations" étend les exigences de FPR_ANO.1 en garantissant que la TSF ne réclame pas l'identité de l'utilisateur.

Administration : FPR_ANO.1, FPR_ANO.2

346 Il n'y a pas d'activités d'administration prévues pour ces composants.

Audit : FPR_ANO.1, FPR_ANO.2

347 Les actions suivantes doivent être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : l'appel du mécanisme d'anonymat.

FPR_ANO.1 Anonymat

Hiérarchique à : aucun autre composant.

FPR_ANO.1.1 La TSF doit garantir que [affectation : *ensemble d'utilisateurs ou de sujets*] sont incapables de déterminer le véritable nom de l'utilisateur associé à [affectation : *liste de sujets, d'opérations ou d'objets*].

Dependencies: No dependencies

FPR_ANO.2 Anonymat sans demande d'informations

Hiéarchique à : FPR_ANO.1

FPR_ANO.2.1 La TSF doit garantir que [affectation : *ensemble d'utilisateurs ou de sujets*] sont incapables de déterminer le véritable nom de l'utilisateur associé à [affectation : *liste de sujets, d'opérations ou d'objets*].

FPR_ANO.2.2 **La TSF doit fournir [affectation : *liste de services*] à [affectation : *liste de sujets*] sans solliciter une quelconque référence au véritable nom de l'utilisateur.**

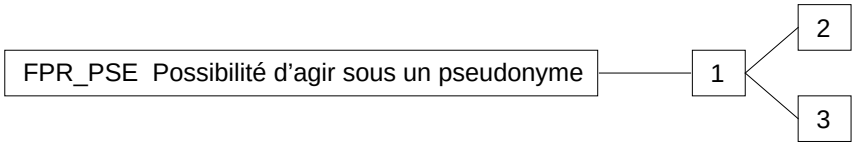
Dependencies: No dependencies

9.2 Possibilité d'agir sous un pseudonyme (FPR_PSE)

Comportement de la famille

348 La présente famille garantit qu'un utilisateur peut utiliser une ressource ou un service sans révéler son identité d'utilisateur, mais peut quand même avoir à répondre de cette utilisation.

Classement des composants



349 Le composant "**FPR_PSE.1 Possibilité d'agir sous un pseudonyme**" exige qu'un ensemble d'utilisateurs ou de sujets soit incapable de déterminer l'identité d'un utilisateur associé à un sujet ou à une opération, mais que cet utilisateur réponde quand même de ses actions.

350 Le composant "FPR_PSE.2 Utilisation réversible de pseudonymes" exige que la TSF fournisse la capacité de déterminer l'identité originelle de l'utilisateur à partir d'un alias fourni.

351 Le composant "FPR_PSE.3 Possibilité d'agir sous un pseudonyme en utilisant un alias" exige que la TSF suive certaines règles de construction pour l'alias de l'identité de l'utilisateur.

Administration : FPR_PSE.1, FPR_PSE.2, FPR_PSE.3

352 Il n'y a pas d'activités d'administration prévues pour ces composants.

Audit : FPR_PSE.1, FPR_PSE.2, FPR_PSE.3

353 Les actions suivantes doivent être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : le sujet ou l'utilisateur qui demande la résolution de l'identité de l'utilisateur devrait être audité.

FPR_PSE.1 Possibilité d'agir sous un pseudonyme

Hiérarchique à : aucun autre composant.

FPR_PSE.1.1 La TSF doit garantir que [affectation : *ensemble d'utilisateurs ou de sujets*] sont incapables de déterminer le véritable nom de l'utilisateur associé à [affectation : *liste de sujets, opérations ou objets*].

FPR_PSE.1.2 **La TSF doit être capable de fournir [affectation : *nombre d'alias*] alias du véritable nom de l'utilisateur à [affectation : *liste de sujets*].**

FPR_PSE.1.3 **La TSF doit [sélection : *déterminer un alias pour un utilisateur, accepter l'alias de l'utilisateur*] et contrôler qu'il est conforme à la [affectation : *métrique relative aux alias*].**

Dependencies: No dependencies

FPR_PSE.2 Utilisation réversible de pseudonymes

Hiéarchique à : FPR_PSE.1

FPR_PSE.2.1 La TSF doit garantir que [affectation : *ensemble d'utilisateurs ou de sujets*] sont incapables de déterminer le véritable nom de l'utilisateur associé à [affectation : *liste de sujets, opérations ou objets*].

FPR_PSE.2.2 La TSF doit être capable de fournir [affectation : *nombre d'alias*] alias du véritable nom de l'utilisateur à [affectation : *liste de sujets*].

FPR_PSE.2.3 La TSF doit [sélection : *déterminer un alias pour un utilisateur, accepter l'alias de l'utilisateur*] et contrôler qu'il est conforme à la [affectation : *métrique relative aux alias*].

FPR_PSE.2.4 **La TSF doit fournir à [sélection : *un utilisateur autorisé,* [affectation : *liste de sujets de confiance*]] une capacité de déterminer l'identité de l'utilisateur à partir de l'alias fourni, uniquement sous les conditions suivantes [affectation : *liste de conditions*].**

Dépendances : **FIA_UID.1 Programmation de l'identification**

FPR_PSE.3 Possibilité d'agir sous un pseudonyme en utilisant un alias

Hiéarchique à : FPR_PSE.1

FPR_PSE.3.1 La TSF doit garantir que [affectation : *ensemble d'utilisateurs ou de sujets*] sont incapables de déterminer le véritable nom de l'utilisateur associé à [affectation : *liste de sujets, opérations ou objets*].

FPR_PSE.3.2 La TSF doit être capable de fournir [affectation : *nombre d'alias*] alias du véritable nom de l'utilisateur à [affectation : *liste de sujets*].

FPR_PSE.3.3 La TSF doit [sélection : *déterminer un alias pour un utilisateur, accepter l'alias de l'utilisateur*] et contrôler qu'il est conforme à la [affectation : *métrique relative aux alias*].

FPR_PSE.3.4 **La TSF doit fournir un alias pour le véritable nom de l'utilisateur qui doit être identique à un alias fourni précédemment sous les conditions suivantes [affectation : *liste de conditions*] ; dans le cas contraire l'alias fourni doit être sans relation avec les alias précédemment fournis.**

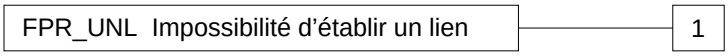
Dependencies: No dependencies

9.3 Impossibilité d'établir un lien (FPR_UNL)

Comportement de la famille

354 La présente famille garantit qu'un utilisateur peut utiliser plusieurs fois des ressources ou des services sans que d'autres soient capables d'établir un lien entre ces utilisations.

Classement des composants



355 Le composant "FPR_UNL.1 Impossibilité d'établir un lien" exige que des utilisateurs ou des sujets soient incapables de déterminer si le même utilisateur a déclenché certaines opérations spécifiques dans le système.

Administration : FPR_UNL.1

356 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) l'administration de la fonction qui empêche d'établir un lien.

Audit : FPR_UNL.1

357 Les actions suivantes doivent être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : l'appel du mécanisme qui empêche d'établir un lien.

FPR_UNL.1 Impossibilité d'établir un lien

Hiérarchique à : aucun autre composant.

FPR_UNL.1.1 **La TSF doit garantir que [affectation : *ensemble d'utilisateurs ou de sujets*] sont incapables de déterminer si [affectation : *liste d'opérations*] [sélection : *ont été déclenchées par le même utilisateur, sont reliées comme suit* [affectation : *liste de relations*]].**

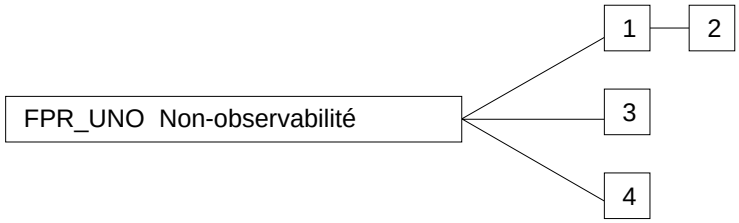
Dependencies: No dependencies

9.4 Non-observabilité (FPR_UNO)

Comportement de la famille

358 La présente famille garantit qu'un utilisateur peut utiliser une ressource ou un service sans que d'autres, en particulier des tierces parties, soient capables d'observer que la ressource ou le service est en cours d'utilisation.

Classement des composants



359 Le composant "FPR_UNO.1 Non-observabilité" exige que des utilisateurs ou des sujets ne puissent pas déterminer si une opération est en cours d'exécution.

360 Le composant "FPR_UNO.2 Allocation des informations ayant un impact sur la non-observabilité" exige que la TSF fournisse des mécanismes spécifiques pour éviter la concentration d'informations relatives à la vie privée au sein de la TOE. De telles concentrations peuvent avoir un impact sur la non-observabilité si une compromission de la sécurité se produit.

361 Le composant "FPR_UNO.3 Non-observabilité sans sollicitation d'informations" exige que la TSF n'essaye pas d'obtenir des informations relatives à la vie privée qui pourraient être utilisées pour compromettre la non-observabilité.

362 Le composant "FPR_UNO.4 Observabilité par un utilisateur autorisé" exige que la TSF offre à un ou plusieurs utilisateurs autorisés la capacité d'observer l'utilisation de ressources ou de services.

Administration : FPR_UNO.1, FPR_UNO.2

363 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) l'administration du comportement de la fonction de non-observabilité.

Administration : FPR_UNO.3

364 Il n'y a pas d'activités d'administration prévues pour ces composants.

Administration : FPR_UNO.4

365 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la liste des utilisateurs autorisés qui sont capables de déterminer l'occurrence d'opérations.

Audit : FPR_UNO.1, FPR_UNO.2

366 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : l'appel du mécanisme de non-observabilité.

Audit : FPR_UNO.3

367 Il n'y a pas d'actions identifiées qui devraient être auditables si "FAU_GEN Génération de données de l'audit de sécurité' est incluse dans le PP ou la ST.

Audit : FPR_UNO.4

368 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : l'observation de l'utilisation d'une ressource ou d'un service par un utilisateur ou un sujet.

FPR_UNO.1 Non-observabilité

Hiérarchique à : aucun autre composant.

FPR_UNO.1.1 **La TSF doit garantir que [affectation : *liste d'utilisateurs ou de sujets*] ne peuvent pas observer l'exécution de [affectation : *liste des opérations*] sur [affectation : *liste des objets*] par [affectation : *liste d'utilisateurs ou de sujets protégés*].**

Dependencies: No dependencies

FPR_UNO.2 Allocation des informations ayant un impact sur la non-observabilité

Hiéarchique à : FPR_UNO.1

FPR_UNO.2.1 La TSF doit garantir que [affectation : *liste d'utilisateurs ou de sujets*] ne peuvent pas observer l'exécution de [affectation : *liste de opérations*] sur [affectation : *liste des objets*] par [affectation : *liste d'utilisateurs ou de sujets protégés*].

FPR_UNO.2.2 **La TSF doit allouer les [affectation : *informations relatives à la non-observabilité*] aux différentes parties de la TOE de telle sorte que les conditions suivantes soient satisfaites pendant la durée de vie des informations : [affectation : *liste de conditions*].**

Dependencies: No dependencies

FPR_UNO.3 Non-observabilité sans sollicitation d'informations

Hiérarchique à : aucun autre composant.

FPR_UNO.3.1 **La TSF doit fournir [affectation : *liste de services*] à [affectation : *liste de sujets*] sans solliciter une quelconque référence à des [affectation : *informations relatives à la vie privée*].**

Dépendances : **FPR_UNO.1 Non-observabilité**

FPR_UNO.4 Observabilité par un utilisateur autorisé

Hiérarchique à : aucun autre composant.

FPR_UNO.4.1 **La TSF doit fournir à [affectation : *ensemble d'utilisateurs autorisés*] la capacité d'observer l'utilisation de [affectation : *liste de ressources ou services*].**

Dependencies: No dependencies

10 Classe FPT : Protection de la TSF

369 La présente classe contient des familles d'exigences fonctionnelles qui se rapportent à l'intégrité et à l'administration des mécanismes qu'offre la TSF (indépendamment des spécificités de la TSP) et à l'intégrité des données de la TSF (indépendamment du contenu spécifique des données de la TSP). Dans une certaine mesure, les familles de cette classe peuvent apparaître comme une duplication des composants de la classe FDP (Protection des données de l'utilisateur) ; elles peuvent même être implémentées en utilisant les mêmes mécanismes. Cependant, la classe FDP porte sur la protection des données de l'utilisateur, tandis que la classe FPT porte sur la protection des données de la TSF. En fait, les composants de la classe FPT sont nécessaires pour fournir les exigences établissant que les SFP de la TOE ne peuvent pas être altérées ou court-circuitées.

370 Du point de vue de cette classe, il y a trois parties importantes pour la TSF :

a) la *machine abstraite* de la TSF, qui est la machine virtuelle ou physique sur laquelle s'exécute l'implémentation spécifique de la TSF en cours d'évaluation ;

b) l'*implémentation* de la TSF, qui s'exécute sur la machine abstraite et implémente les mécanismes qui mettent en œuvre la TSP ;

c) les *données* de la TSF, qui sont les bases de données d'administration qui guident l'application de la TSP.

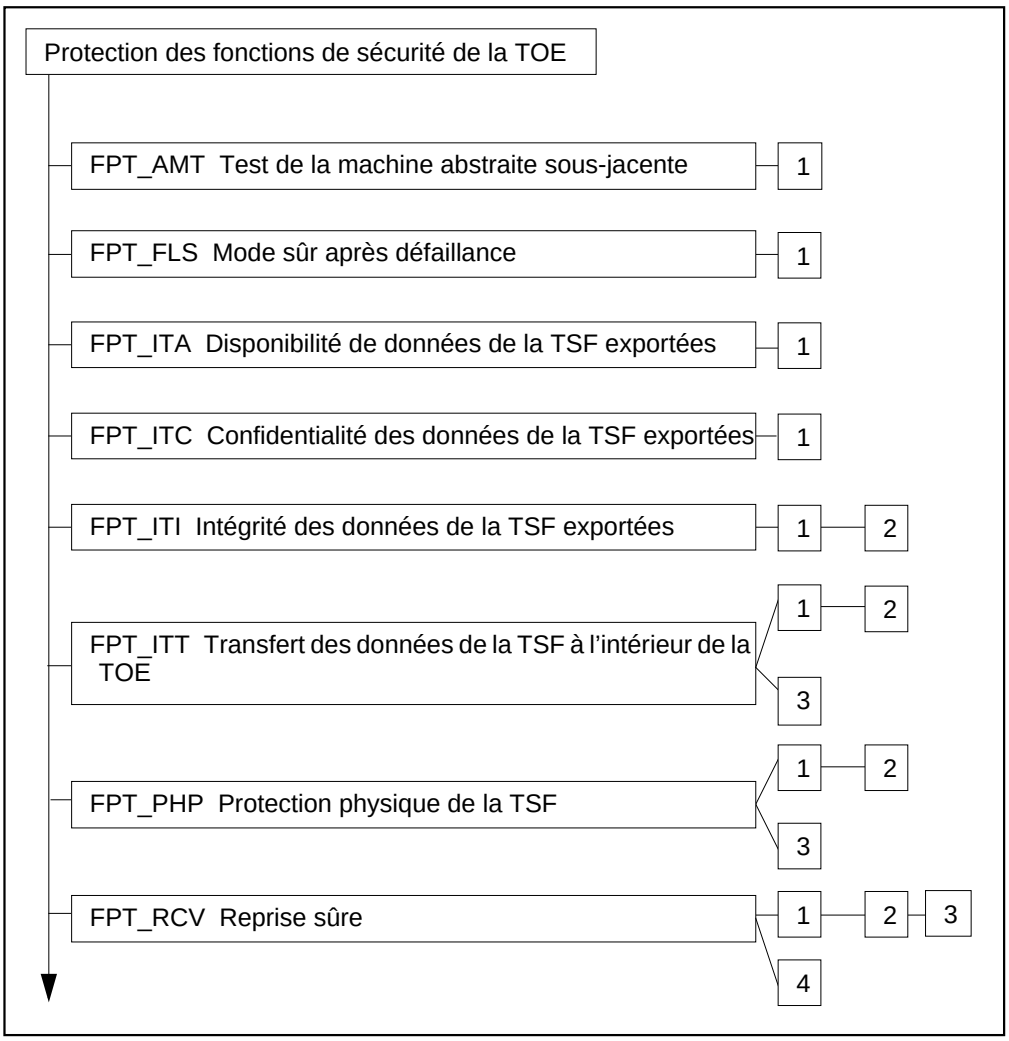


Figure 10.1 - Décomposition de la classe "Protection de la TSF"

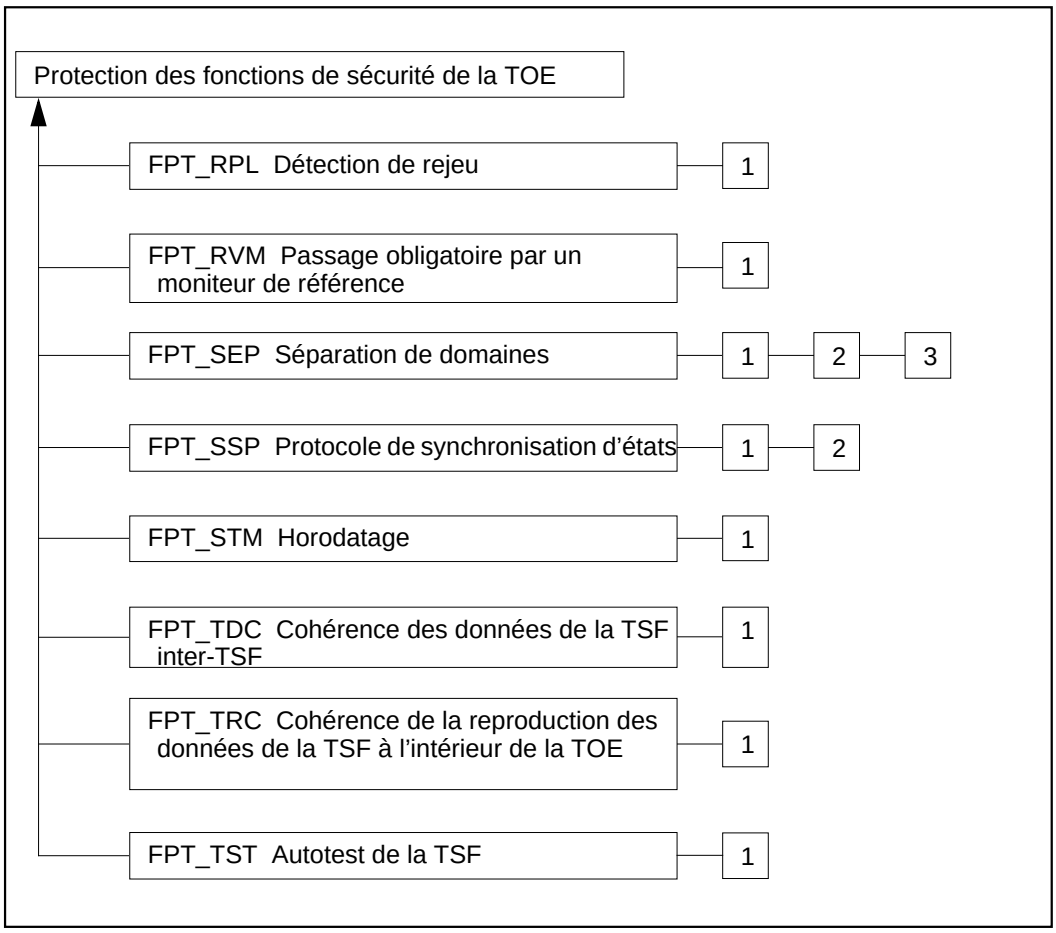


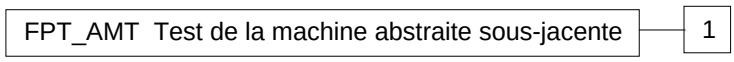
Figure 10.2 - Décomposition de la classe "Protection de la TSF" (suite)

10.1 Test de la machine abstraite sous-jacente (FPT_AMT)

Comportement de la famille

371 La présente famille définit des exigences pour que la TSF exécute des tests pour démontrer les hypothèses de sécurité qui ont été faites au sujet de la machine abstraite sous-jacente sur laquelle la TSF repose. Cette machine "abstraite" pourrait être une plate-forme matérielle ou micro-programmée, ou bien une association connue et testée de matériel et de logiciel se comportant comme une machine virtuelle.

Classement des composants



372 Le composant "FPT_AMT.1 Test de la machine abstraite" définit la façon de tester la machine abstraite sous-jacente.

Administration : FPT_AMT.1

373 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration des conditions dans lesquelles les tests de la machine abstraite ont lieu, comme par exemple pendant le démarrage initial, à des intervalles réguliers ou dans des conditions spécifiées ;

b) administration de l'intervalle de temps le cas échéant.

Audit : FPT_AMT.1

374 Les actions suivantes devraient être auditées dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : exécution des tests de la machine sous-jacente et résultats des tests.

FPT_AMT.1 Test de la machine abstraite

Hiérarchique à : aucun autre composant.

FPT_AMT.1.1 La TSF doit exécuter une suite de tests [sélection : *pendant le démarrage initial, de façon périodique pendant le fonctionnement normal, à la demande d'un utilisateur autorisé, autres conditions*] pour démontrer le fonctionnement correct des hypothèses de sécurité fournies par la machine abstraite sous-jacente à la TSF.

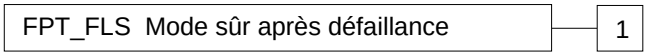
Dependencies: No dependencies

10.2 Mode sûr après défaillance (FPT_FLS)

Comportement de la famille

375 Les exigences de cette famille garantissent que la TOE ne violera pas sa propre TSP dans le cas où se produiraient certaines catégories identifiées de défaillances dans la TSF.

Classement des composants



376 Cette famille n'est constituée que d'un seul composant, "FPT_FLS.1 Défaillance avec préservation d'un état sûr", qui exige que la TSF préserve un état sûr dans le cas de défaillances identifiées.

Administration : FPT_FLS.1

377 Il n'y a pas d'activités d'administration prévues.

Audit : FPT_FLS.1

378 Les actions suivantes devraient être auditées dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : défaillance de la TSF.

FPT_FLS.1 Défaillance avec préservation d'un état sûr

Hiérarchique à : aucun autre composant.

FPT_FLS.1.1 La TSF doit préserver un état sûr quand les types de défaillances suivants se produisent : [affectation : *liste des types de défaillances de la TSF*].

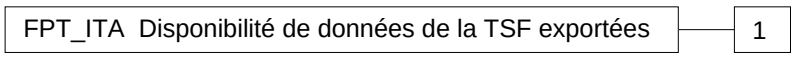
Dépendances : **ADV_SPM.1 Modèle informel de politique de sécurité de la TOE**

10.3 Disponibilité de données de la TSF exportées (FPT_ITA)

Comportement de la famille

379 La présente famille définit les règles pour prévenir la perte de disponibilité des données de la TSF transitant entre la TSF et un produit TI de confiance distant. Ces données pourraient, par exemple, être des données critiques de la TSF telles que des mots de passe, des clés, des données d'audit ou du code exécutable de la TSF.

Classement des composants



380 Cette famille n'est constituée que d'un seul composant, "FPT_ITA.1 Disponibilité inter-TSF dans la limite d'une métrique de disponibilité définie". Ce composant exige que la TSF garantisse, avec un degré de probabilité identifié, la disponibilité de données de la TSF fournies à un produit TI de confiance distant.

Administration : FPT_ITA.1

381 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration de la liste des types de données de la TSF qui doivent être disponibles pour un produit TI de confiance distant.

Audit : FPT_ITA.1

382 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : l'absence de données de la TSF quand elles sont demandées par une TOE.

FPT_ITA.1 Disponibilité inter-TSF dans la limite d'une métrique de disponibilité définie

Hiérarchique à : aucun autre composant.

FPT_ITA.1.1 **La TSF doit garantir la disponibilité [affectation : *liste des types de données de la TSF*] fournies à un produit TI de confiance distant dans le cadre de [affectation : *une métrique de disponibilité définie*] étant donné les conditions suivantes [affectation : *conditions pour garantir la disponibilité*].**

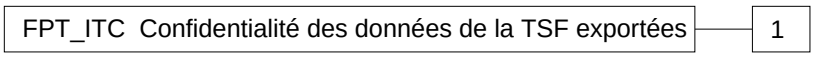
Dependencies: No dependencies

10.4 Confidentialité des données de la TSF exportées (FPT_ITC)

Comportement de la famille

383 La présente famille définit les règles pour la protection des données de la TSF contre une divulgation non autorisée lors de leur transmission entre la TSF et un produit TI de confiance distant. Ces données pourraient, par exemple, être des données critiques pour la TSF telles que des mots de passe, des clés, des données d'audit ou du code exécutable de la TSF.

Classement des composants



384 Cette famille n'est constituée que d'un seul composant, "FPT_ITC.1 Confidentialité inter-TSF pendant une transmission", qui exige que la TSF garantisse que les données transmises entre la TSF et un produit TI de confiance distant soient protégées contre une divulgation pendant leur transit.

Administration : FPT_ITC.1

385 Il n'y a pas d'activités d'administration prévues.

Audit : FPT_ITC.1

386 Il n'y a pas d'actions identifiées qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FPT_ITC.1 Confidentialité inter-TSF pendant une transmission

Hiérarchique à : aucun autre composant.

FPT_ITC.1.1 La TSF doit protéger toutes les données de la TSF transmises depuis la TSF vers un produit TI de confiance distant contre une divulgation non autorisée pendant leur transmission.

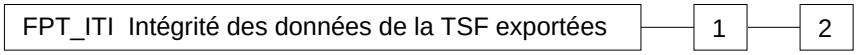
Dependencies: No dependencies

10.5 Intégrité des données de la TSF exportées (FPT_ITI)

Comportement de la famille

387 La présente famille définit les règles pour la protection contre une modification non autorisée des données de la TSF pendant leur transmission entre la TSF et un produit TI de confiance distant. Ces données pourraient, par exemple, être des données critiques de la TSF telles que des mots de passe, des clés, des données d'audit ou du code exécutable de la TSF

Classement des composants



388 Le composant "FPT_ITI.1 Détection inter-TSF d'une modification" offre l'aptitude de détecter une modification des données de la TSF pendant leur transmission entre la TSF et un produit TI de confiance distant, dans l'hypothèse où le produit TI de confiance distant a connaissance du mécanisme utilisé.

389 Le composant "FPT_ITI.2 Détection et correction inter-TSF d'une modification" donne l'aptitude au produit TI de confiance distant non seulement de détecter une modification, mais de corriger des données de la TSF qui ont été modifiées, dans l'hypothèse où le produit TI de confiance distant a connaissance du mécanisme utilisé.

Administration : FPT_ITI.1

390 Il n'y a pas d'activités d'administration prévues.

Administration : FPT_ITI.2

391 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration des types de données de la TSF que la TSF devrait essayer de corriger si elles ont été modifiées pendant leur transit ;

b) administration des types d'actions que la TSF pourrait entreprendre si des données de la TSF étaient modifiées pendant leur transit.

Audit : FPT_ITI.1

392 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : la détection de modification des données de la TSF qui ont été transmises.

b) Elémentaire : l'action entreprise après détection d'une modification des données de la TSF qui ont été transmises.

Audit : FPT_ITI.2

393 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : la détection de modification des données de la TSF qui ont été transmises ;

b) Elémentaire : l'action entreprise après détection d'une modification des données de la TSF qui ont été transmises ;

c) Elémentaire : l'utilisation du mécanisme de correction.

FPT_ITI.1 Détection inter-TSF d'une modification

Hiérarchique à : aucun autre composant.

FPT_ITI.1.1 **La TSF doit offrir la capacité de détecter une modification de toutes les données de la TSF pendant leur transmission entre la TSF et un produit TI de confiance distant dans la limite de la métrique suivante : [affectation : *une métrique de modification définie*].**

FPT_ITI.1.2 **La TSF doit offrir la capacité de contrôler l'intégrité de toutes les données de la TSF transmises entre la TSF et un produit TI de confiance distant et effectuer [affectation : *action à entreprendre*] si des modifications sont détectées.**

Dependencies: No dependencies

FPT_ITI.2 Détection et correction inter-TSF d'une modification

Hiéarchique à : FPT_ITI.1

FPT_ITI.2.1 La TSF doit offrir la capacité de détecter une modification de toutes les données de la TSF pendant leur transmission entre la TSF et un produit TI de confiance distant dans la limite de la métrique suivante : [affectation : *une métrique de modification définie*].

FPT_ITI.2.2 La TSF doit offrir la capacité de contrôler l'intégrité de toutes les données de la TSF transmises entre la TSF et un produit TI de confiance distant et effectuer [affectation : *action à entreprendre*] si des modifications sont détectées.

FPT_ITI.2.3 **La TSF doit offrir la capacité de corriger [affectation : *type de modification*] toutes les données de la TSF transmises entre la TSF et un produit TI de confiance distant.**

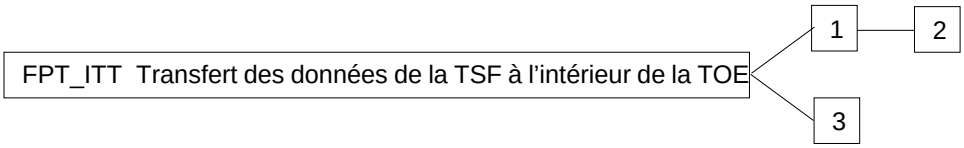
Dependencies: No dependencies

10.6 Transfert des données de la TSF à l'intérieur de la TOE (FPT_ITT)

Comportement de la famille

394 Cette famille fournit des exigences qui traitent de la protection des données de la TSF quand elles sont transférées entre des parties séparées d'une TOE via un canal interne.

Classement des composants



395 Le composant "FPT_ITT.1 Protection élémentaire des données de la TSF lors d'un transfert interne" exige que les données de la TSF soient protégées quand elles sont transmises entre des parties séparées de la TOE.

396 Le composant "FPT_ITT.2 Séparation des données de la TSF pendant un transfert" exige que la TSF sépare les données de l'utilisateur des données de la TSF pendant leur transmission.

397 Le composant "FPT_ITT.3 Contrôle de l'intégrité des données de la TSF" exige que les données de la TSF transmises entre des parties séparées de la TOE soient contrôlées pour détecter des erreurs d'intégrité identifiées.

Administration : FPT_ITT.1

398 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration des types de modification contre lesquels la TSF devrait offrir une protection ;

b) administration du mécanisme utilisé pour fournir la protection des données transitant entre différentes parties de la TSF.

Administration : FPT_ITT.2

399 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration des types de modification contre lesquels la TSF devrait offrir une protection ;

b) administration du mécanisme utilisé pour fournir la protection des données transitant entre différentes parties de la TSF ;

c) administration du mécanisme de séparation.

Administration : FPT_ITT.3

400 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration des types de modification contre lesquels la TSF devrait offrir une protection ;

b) administration du mécanisme utilisé pour fournir la protection des données transitant entre différentes parties de la TSF ;

c) administration des types de modification des données de la TSF que la TSF devrait essayer de détecter ;

d) administration des actions qui seront entreprises.

Audit : FPT_ITT.1, FPT_ITT.2

401 Il n'y a pas d'actions identifiées qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

Audit : FPT_ITT.3

402 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : la détection d'une modification des données de la TSF.

FPT_ITT.1 Protection élémentaire des données de la TSF lors d'un transfert interne

Hiérarchique à : aucun autre composant.

FPT_ITT.1.1 La TSF doit protéger les données de la TSF contre la [sélection : *divulgation, modification*] quand elles sont transmises entre des parties séparées de la TOE.

Dependencies: No dependencies

FPT_ITT.2 Séparation des données de la TSF pendant un transfert

Hiéarchique à : FPT_ITT.1

FPT_ITT.2.1 La TSF doit protéger les données de la TSF contre la [sélection : *divulgation, modification*] quand elles sont transmises entre des parties séparées de la TOE.

FPT_ITT.2.2 **La TSF doit séparer les données de l'utilisateur des données de la TSF quand de telles données sont transmises entre des parties séparées de la TOE.**

Dependencies: No dependencies

FPT_ITT.3 Contrôle de l'intégrité des données de la TSF

Hiérarchique à : aucun autre composant.

FPT_ITT.3.1 **La TSF doit être capable de détecter [sélection : la *modification de données, la substitution de données, le ré-ordonnancement de données, la suppression de données,* [affectation : *autres erreurs d'intégrité*]] pour les données de la TSF transmises entre des parties séparées de la TOE.**

FPT_ITT.3.2 **Dès qu'une erreur d'intégrité sur les données est détectée, la TSF doit entreprendre les actions suivantes : [affectation : *spécifier l'action à entreprendre*].**

Dépendances : **FPT_ITT.1 Protection élémentaire des données de la TSF lors d'un transfert interne**

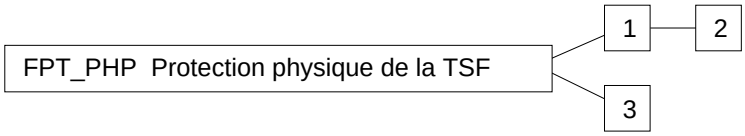
10.7 Protection physique de la TSF (FPT_PHP)

Comportement de la famille

403 Les composants relatifs à la protection physique de la TSF font référence à des restrictions concernant les accès physiques non autorisés à la TSF et à la dissuasion pour prévenir une modification physique non autorisée ou une substitution de la TSF, ou à la résistance à celles-ci.

404 Les exigences des composants de cette famille garantissent que la TSF est protégée contre des intrusions physiques et des interférences. La satisfaction des exigences de ces composants fait que la TSF est conditionnée et utilisée de façon telle que des intrusions physiques soient détectables, ou que la résistance aux intrusions physiques soit effective. Sans ces composants, les fonctions de protection d'une TSF perdent de leur efficacité dans des environnements où les agressions physiques ne peuvent pas être empêchées. Cette famille fournit également des exigences concernant la façon dont la TSF doit répondre à des tentatives d'intrusion physique.

Classement des composants



405 Le composant "FPT_PHP.1 Détection passive d'une attaque physique" fournit des caractéristiques qui indiquent quand un dispositif de la TSF ou un élément de la TSF est l'objet d'une intrusion. Cependant, la notification d'intrusion n'est pas automatique ; un utilisateur autorisé doit faire appel à une fonction de sécurité administrative ou effectuer une inspection manuelle pour déterminer si une intrusion a eu lieu.

406 Le composant "FPT_PHP.2 Notification d'une attaque physique" fournit la notification automatique d'une intrusion pour un sous-ensemble identifié de pénétrations physiques.

407 Le composant "FPT_PHP.3 Résistance à une attaque physique" fournit des caractéristiques qui empêchent ou résistent à une intrusion physique des dispositifs de la TSF ou des éléments de la TSF.

Administration : FPT_PHP.1

408 Il n'y a pas d'activités d'administration prévues.

Administration : FPT_PHP.2

409 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration de l'utilisateur ou du rôle qui se tient informé des intrusions ;

b) administration de la liste des dispositifs qui devraient informer de l'intrusion l'utilisateur ou le rôle indiqué.

Administration : FPT_PHP.3

410 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration des réponses automatiques à une intrusion physique.

Audit : FPT_PHP.1

411 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : si une détection est faite par des moyens TI, détection de l'intrusion.

Audit : FPT_PHP.2,

412 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : détection d'une intrusion.

Audit : FPT_PHP.3

413 Il n'y a aucune action identifiée qui puisse être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FPT_PHP.1 Détection passive d'une attaque physique

Hiérarchique à : aucun autre composant.

FPT_PHP.1.1 La TSF doit détecter de façon non ambiguë une intrusion physique qui pourrait compromettre la TSF.

FPT_PHP.1.2 La TSF doit offrir la capacité de déterminer si une intrusion physique dans les dispositifs de la TSF ou dans les éléments de la TSF a eu lieu.

Dépendances : **FMT_MOF.1 Administration du comportement des fonctions de sécurité**

FPT_PHP.2 Notification d'une attaque physique

Hiéarchique à : FPT_PHP.1

FPT_PHP.2.1 La TSF doit détecter de façon non ambiguë une intrusion physique qui pourrait compromettre la TSF.

FPT_PHP.2.2 La TSF doit offrir la capacité de déterminer si une intrusion physique dans les dispositifs de la TSF ou les éléments de la TSF a eu lieu.

FPT_PHP.2.3 **Pour [affectation : *liste des dispositifs ou des éléments de la TSF pour lesquels une détection active est requise*], la TSF doit contrôler les dispositifs et les éléments et notifier à [affectation : *un utilisateur ou un rôle désigné*] quand une intrusion physique dans les dispositifs de la TSF ou dans les éléments de la TSF a eu lieu.**

Dépendances : FMT_MOF.1 Administration du comportement des fonctions de sécurité

FPT_PHP.3 Résistance à une attaque physique

Hiérarchique à : aucun autre composant.

FPT_PHP.3.1 **La TSF doit résister à [affectation : *scénarios d'intrusions physique*] dans les [affectation : *liste des dispositifs ou des éléments de la TSF*] en répondant automatiquement de telle façon que la TSP ne soit pas violée.**

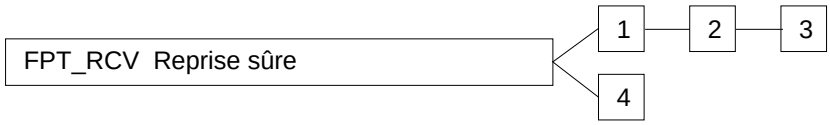
Dependencies: No dependencies

10.8 Reprise sûre (FPT_RCV)

Comportement de la famille

414 Les exigences de cette famille garantissent que la TSF peut déterminer que le démarrage de la TOE a été fait sans compromettre sa protection et qu'elle peut reprendre son fonctionnement à la suite d'une interruption des opérations sans compromettre sa protection. Cette famille est importante parce que l'état au démarrage de la TSF détermine la protection des états suivants.

Classement des composants



415 Le composant "FPT_RCV.1 Reprise manuelle" permet à une TOE de ne fournir que des mécanismes qui impliquent une intervention humaine pour retourner à un état sûr.

416 Le composant "FPT_RCV.2 Reprise automatisée" pourvoit à une reprise dans un état sûr sans intervention humaine, au moins pour un type d'interruption de service ; la reprise à la suite d'autres types d'interruption peut nécessiter le recours à une intervention humaine.

417 Le composant "FPT_RCV.3 Reprise automatisée sans perte indue" pourvoit également à une reprise automatisée, mais renforce les exigences en n'autorisant pas la perte indue d'objets protégés.

418 Le composant "FPT_RCV.4 Reprise de fonction" pourvoit à une reprise au niveau de SF particulières, en garantissant soit la réussite finale, soit un retour des données de la TSF dans un état sûr.

Administration : FPT_RCV.1

419 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration de la personne qui peut accéder au moyen permettant la restauration dans le mode de maintenance.

Administration : FPT_RCV.2, FPT_RCV.3

420 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration de la personne qui peut accéder au moyen permettant la restauration dans le mode de maintenance ;

b) administration de la liste des défaillances ou d'interruptions de service qui seront prises en compte par les procédures automatiques.

Administration : FPT_RCV.4

421 Il n'y a pas d'activités d'administration prévues.

Audit : FPT_RCV.1, FPT_RCV.2, FPT_RCV.3

422 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : le fait qu'une défaillance ou une interruption de service ait eu lieu ;

b) Minimal : reprise du fonctionnement normal ;

c) Elémentaire : type de défaillance ou d'interruption de service.

Audit : FPT_RCV.4

423 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : si possible, l'impossibilité de retourner à un état sûr après défaillance d'une fonction de sécurité ;

b) Elémentaire : si possible, la détection d'une défaillance d'une fonction de sécurité.

FPT_RCV.1 Reprise manuelle

Hiérarchique à : aucun autre composant.

FPT_RCV.1.1 Après une défaillance ou une interruption de service, la TSF doit passer dans un mode de maintenance où l'aptitude de remettre la TOE dans un état sûr est offerte.

Dépendances : **FPT_TST.1 Test de la TSF**

AGD_ADM.1 Guide de l'administrateur

ADV_SPM.1 Modèle informel de politique de sécurité de la TOE

FPT_RCV.2 Reprise automatisée

Hiéarchique à : FPT_RCV.1

FPT_RCV.2.1 **Quand une reprise automatisée à la suite** d'une défaillance ou d'une interruption de service **n'est pas possible**, la TSF doit passer dans un mode de maintenance où l'aptitude de remettre la TOE dans un état sûr est offerte.

FPT_RCV.2.2 **Pour [affectation : *liste de défaillances ou d'interruptions de service*], la TSF doit garantir le retour de la TOE à un état sûr en utilisant des procédures automatisées.**

Dépendances : **FPT_TST.1 Test de la TSF**

AGD_ADM.1 Guide de l'administrateur

ADV_SPM.1 Modèle informel de politique de sécurité de la TOE

FPT_RCV.3 Reprise automatisée sans perte indue

Hiéarchique à : FPT_RCV.2

FPT_RCV.3.1 Quand une reprise automatisée à la suite d'une défaillance ou d'une interruption de service n'est pas possible, la TSF doit passer dans un mode de maintenance où l'aptitude de remettre la TOE dans un état sûr est offerte.

FPT_RCV.3.2 Pour [affectation : liste de défaillances ou d'interruptions de service], la TSF doit garantir le retour de la TOE à un état sûr en utilisant des procédures automatisées.

FPT_RCV.3.3 **Les fonctions fournies par la TSF pour une reprise à la suite d'une défaillance ou d'une interruption de service doivent garantir que l'état initial sûr est restauré sans dépasser [affectation : *quantification*] de perte de données de la TSF ou d'objets dans le TSC.**

FPT_RCV.3.4 **La TSF doit offrir la capacité de déterminer les objets qui ont pu ou n'ont pas pu être récupérés.**

Dépendances : **FPT_TST.1 Test de la TSF**

AGD_ADM.1 Guide de l'administrateur

ADV_SPM.1 Modèle informel de politique de sécurité de la TOE

FPT_RCV.4 Reprise de fonction

Hiérarchique à : aucun autre composant.

FPT_RCV.4.1 **La TSF doit garantir que [affectation : *liste des SF et des scénarios de défaillance*] possèdent la propriété selon laquelle la SF soit accomplit sa tâche avec succès, soit reprend son fonctionnement dans un état cohérent et sûr, pour les scénarios de défaillance indiqués.**

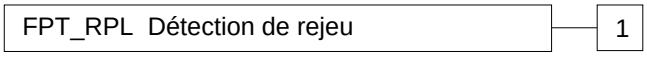
Dépendances : **ADV_SPM.1 Modèle informel de politique de sécurité de la TOE**

10.9 Détection de rejeu (FPT_RPL)

Comportement de la famille

424 Cette famille traite de la détection de rejeu pour divers types d'entités (e.g. messages, requêtes de service, réponses de service) et des actions de correction qui s'ensuivent. Dans le cas où le rejeu peut être détecté, il est efficacement contré.

Classement des composants



425 La famille n'est constituée que d'un seul composant, "FPT_RPL.1 Détection de rejeu", qui exige que la TSF doit être capable de détecter le rejeu d'entités identifiables.

Administration : FPT_RPL.1

426 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de FMT :

a) administration de la liste des entités identifiées pour lesquelles le rejeu doit être détecté ;

b) administration de la liste des actions qui doivent être entreprises dans le cas d'un rejeu.

Audit : FPT_RPL.1

427 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : attaques de rejeu, qui ont été détectées ;

b) Détaillé : action à entreprendre parmi les actions spécifiques.

FPT_RPL.1 Détection de rejeu

Hiérarchique à : aucun autre composant.

FPT_RPL.1.1 La TSF doit détecter le rejeu pour les entités suivantes : [affectation : *liste des entités identifiées*].

FPT_RPL.1.2 La TSF doit exécuter [affectation : *liste des actions spécifiques*] quand le rejeu est détecté.

Dependencies: No dependencies

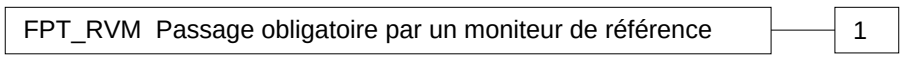
10.10 Passage obligatoire par un moniteur de référence (FPT_RVM)

Comportement de la famille

428 Les exigences de cette famille couvrent l'aspect "appel systématique" à un moniteur de référence traditionnel. Le but de cette famille est de garantir, par rapport à une SFP donnée, que toutes les actions exigeant l'application de la politique sont validées par la TSF vis-à-vis de cette SFP. Si la partie de la TSF qui met en œuvre la SFP satisfait également aux exigences des composants appropriés de la famille FPT_SEP (Séparation de domaines) et de la famille ADV_INT (Parties internes de la TSF), alors cette partie de la TSF fournit un "moniteur de référence" pour cette SFP.

429 Une TSF qui implémente une SFP fournit une protection efficace contre une opération non autorisée, si et seulement si toutes les actions applicables (e.g. accès à des objets) demandées par des sujets non sûrs concernant une partie ou la totalité de cette SFP sont validées par la TSF avant d'aboutir. Si une action applicable par la TSF est appliquée de façon incorrecte ou bien contournée de façon incorrecte, la mise en œuvre globale de la SFP pourrait être compromise. Des sujets pourraient alors contourner la SFP de plusieurs façons non autorisées (e.g. contourner des contrôles d'accès pour certains sujets ou objets, contourner des contrôles pour des objets dont la protection était supposée être assurée par des applications, maintenir des droits d'accès au delà de leur durée de vie prévue, contourner l'audit d'actions auditées, ou contourner l'authentification). Il est à noter qu'on pourrait faire confiance à certains sujets, ceux que l'on nomme "sujets de confiance" par référence à une SFP spécifique, pour qu'ils mettent en œuvre eux-mêmes la SFP, et contourner le passage obligatoire par la SFP.

Classement des composants



430 Cette famille n'est constituée que d'un seul composant, "FPT_RVM.1 Capacité de la TSP à ne pas être contournée", qui exige la capacité à ne pas être contourné pour toute les SFP de la TSP.

Administration : FPT_RVM.1

431 Il n'y a pas d'activités d'administration prévues.

Audit : FPT_RVM.1

432 Il n'y a pas d'actions identifiées qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FPT_RVM.1 Capacité de la TSP à ne pas être contournée

Hiérarchique à : aucun autre composant.

FPT_RVM.1.1 La TSF doit garantir que les fonctions qui mettent en œuvre la TSP sont appelées et s'exécutent avec succès avant que chaque fonction dans le TSC ne soit autorisée à démarrer.

Dependencies: No dependencies

10.11 Séparation de domaines (FPT_SEP)

Comportement de la famille

433 Les composants de cette famille garantissent qu'au moins un domaine de sécurité soit disponible pour l'exécution de la TSF elle-même et que la TSF soit protégée contre des interférences et des intrusions d'origine externes (e.g. par modification du code de la TSF ou des structures de données) par des sujets non sûrs. La satisfaction des exigences de cette famille rend la TSF auto-protectrice, ce qui signifie qu'un sujet non sûr ne peut pas modifier ou endommager la TSF.

434 Cette famille exige que :

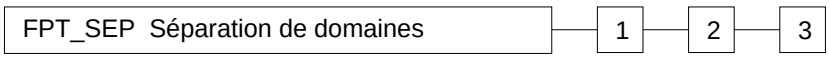
a) les ressources du domaine de sécurité de la TSF ("domaine protégé") et ceux des sujets et des entités libres externes au domaine soient séparés, de telle façon que les entités externes au domaine protégé ne puissent pas observer ou modifier des données de la TSF ou du code de la TSF à l'intérieur du domaine protégé ;

b) les transferts entre domaines soient contrôlés, de telle sorte qu'il ne soit pas possible d'entrer dans le domaine protégé ou d'en sortir de façon arbitraire ;

c) les paramètres de l'utilisateur ou de l'application passés dans le domaine protégé par adresses soient validés en fonction de l'espace adressable du domaine protégé, et ceux passés par valeurs soient validés en fonction des valeurs attendues par le domaine protégé ;

d) les domaines de sécurité des sujets soient distincts sauf pour les parties communes contrôlées via la TSF.

Classement des composants



435 Le composant "FPT_SEP.1 Séparation de domaines pour la TSF" offre un domaine protégé distinct pour la TSF et procure une séparation entre sujets dans le TSC.

436 Le composant "FPT_SEP.2 Séparation de domaines pour la SFP" exige que la TSF soit subdivisée, avec un ou des domaines distincts pour un ensemble identifié de SFP qui agissent comme un moniteur de référence pour leurs politiques, un domaine pour le reste de la TSF, ainsi que des domaines pour les parties de la TOE ne faisant pas partie de la TSF.

437 Le composant "FPT_SEP.3 Moniteur de référence complet" exige qu'il y ait un ou plusieurs domaines distincts pour la mise en œuvre de la TSP, un domaine pour le

reste de la TSF, ainsi que des domaines pour les parties de la TOE ne faisant pas partie de la TSF.

Administration : FPT_SEP.1, FPT_SEP.2, FPT_SEP.3

438 Il n'y a pas d'activités d'administration prévues.

Audit : FPT_SEP.1, FPT_SEP.2, FPT_SEP.3

439 Il n'y a pas d'actions identifiées qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FPT_SEP.1 Séparation de domaines pour la TSF

Hiérarchique à : aucun autre composant.

FPT_SEP.1.1 **La TSF doit maintenir un domaine de sécurité pour sa propre exécution, qui la protège des interférences et des intrusions par des sujets non sûrs.**

FPT_SEP.1.2 **La TSF doit appliquer une séparation entre les domaines de sécurité de sujets dans le TSC.**

Dependencies: No dependencies

FPT_SEP.2 Séparation de domaines pour la SFP

Hiéarchique à : FPT_SEP.1

FPT_SEP.2.1 La **partie non isolée de la TSF** doit maintenir un domaine de sécurité pour sa propre exécution, qui la protège des interférences et des intrusions par des sujets non sûrs.

FPT_SEP.2.2 La TSF doit appliquer une séparation entre les domaines de sécurité de sujets dans le TSC.

FPT_SEP.2.3 **La TSF doit maintenir la partie de la TSF liée à [affectation : *liste des SFP de contrôles d'accès ou des SFP de contrôle de flux d'information*] dans un domaine de sécurité pour leur propre exécution qui les protège des interférences et des intrusions en provenance du reste de la TSF et des sujets non sûrs, relativement à ces SFP.**

Dependencies: No dependencies

FPT_SEP.3 Moniteur de référence complet

Hiéarchique à : FPT_SEP.2

FPT_SEP.3.1 La partie non isolée de la TSF doit maintenir un domaine de sécurité pour sa propre exécution qui la protège des interférences et des intrusions par des sujets non sûrs.

FPT_SEP.3.2 La TSF doit appliquer une séparation entre les domaines de sécurité de sujets dans le TSC.

FPT_SEP.3.3 La TSF doit maintenir **la partie de la TSF qui met en œuvre les SFP de contrôle d'accès ou les SFP de contrôle de flux d'information** dans un domaine de sécurité pour **sa** propre exécution qui **les** protège des interférences et des intrusions en provenance du reste de la TSF et des sujets non sûrs, relativement à **la TSP**.

Dependencies: No dependencies

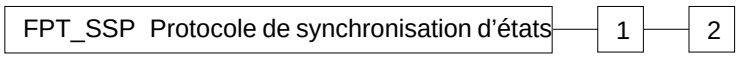
10.12 Protocole de synchronisation d'états (FPT_SSP)

Comportement de la famille

440 Les systèmes distribués peuvent occasionner une complexité supérieure à celle des systèmes monolithiques à cause du potentiel de différence des états entre des parties du système, et à cause de retards dans les communications. Dans la plupart des cas, la synchronisation d'état entre fonctions distribuées implique un protocole d'échange, et non une simple action. Quand la malveillance est présente dans l'environnement distribué de ces protocoles, des protocoles défensifs plus complexes sont exigés.

441 La famille FPT_SSP établit l'exigence pour certaines fonctions de sécurité critiques de la TSF d'utiliser ce protocole de confiance. La famille FPT_SSP garantit que deux parties distribuées de la TOE (e.g. des hôtes) ont synchronisé leurs états après une action touchant à la sécurité.

Classement des composants



442 Le composant "FPT_SSP.1 Accusé de réception de confiance simple" exige seulement un accusé de réception simple par le récipiendaire des données.

443 Le composant "FPT_SSP.2 Accusé de réception de confiance mutuel" exige un accusé de réception mutuel de l'échange de données.

Administration : FPT_SSP.1, FPT_SSP.2

444 Il n'y a pas d'activités d'administration prévues.

Audit : FPT_SSP.1, FPT_SSP.2

445 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : échec dans la réception d'un accusé de réception quand il est attendu.

FPT_SSP.1 Accusé de réception de confiance simple

Hiérarchique à : aucun autre composant.

FPT_SSP.1.1 La TSF doit accuser réception, quand cela est demandé par une autre partie de la TSF, d'une transmission sans modification de données de la TSF.

Dépendances : **FPT_ITT.1 Protection élémentaire des données de la TSF lors d'un transfert interne**

FPT_SSP.2 Accusé de réception de confiance mutuel

Hiéarchique à : FPT_SSP.1

FPT_SSP.2.1 La TSF doit accuser réception, quand cela est demandé par une autre partie de la TSF, d'une transmission sans modification de données de la TSF.

FPT_SSP.2.2 **La TSF doit garantir que les parties concernées de la TSF connaissent le statut exact des données transmises entre ses différentes parties, au moyen d'accusés de réception.**

Dépendances : FPT_ITT.1 Protection élémentaire des données de la TSF lors d'un transfert interne

10.13 Horodatage (FPT_STM)

Comportement de la famille

446 Cette famille traite des exigences pour une fonction d'horodatage fiable dans une TOE.

Classement des composants

447 Cette famille n'est constituée que d'un seul composant, "**FPT_STM.1 Horodatage fiable**", qui exige que la TSF fournisse un horodatage fiable pour les fonctions de la TSF.

Administration : FPT_STM.1

448 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration de la date.

Audit : FPT_STM.1

449 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : modifications de la date ;

b) Détaillé : fourniture d'un horodatage.

FPT_STM.1 Horodatage fiable

Hiérarchique à : aucun autre composant.

FPT_STM.1.1 La TSF doit être capable de fournir un horodatage fiable pour son propre usage.

Dependencies: No dependencies

10.14 Cohérence des données de la TSF inter-TSF (FPT_TDC)

Comportement de la famille

450 Dans l'environnement d'un système distribué ou composé, une TOE peut avoir besoin d'échanger des données de la TSF (e.g. les attributs de la SFP associés à des données, des informations d'audit, des informations d'identification) avec un autre produit TI de confiance. La présente famille définit les exigences pour un partage et une interprétation cohérente de ces attributs entre la TSF de la TOE et celle d'un produit TI de confiance différent.

Classement des composants

FPT_TDC Cohérence des données de la TSF inter-TSF	1

451 Le composant "**FPT_TDC.1 Cohérence élémentaire des données de la TSF inter-TSF**" exige que la TSF offre la capacité de garantir la cohérence des attributs entre des TSF.

Administration : FPT_TDC.1

452 Il n'y a pas d'activités d'administration prévues.

Audit : FPT_TDC.1

453 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : utilisation réussie des mécanismes assurant la cohérence des données de la TSF ;

b) Elémentaire : utilisation des mécanismes assurant la cohérence des données de la TSF ;

c) Elémentaire : identification des données de la TSF qui ont été interprétées ;

d) Elémentaire : détection des données de la TSF qui ont été modifiées.

FPT_TDC.1 Cohérence élémentaire des données de la TSF inter-TSF

Hiérarchique à : aucun autre composant.

FPT_TDC.1.1 La TSF doit offrir la capacité d'interpréter de façon cohérente [affectation : *liste des types de données de la TSF*] quand elles sont partagées entre la TSF et un autre produit TI de confiance.

FPT_TDC.1.2 **La TSF doit utiliser [affectation : *liste des règles d'interprétation à appliquer par la TSF*] pour interpréter les données de la TSF d'un autre produit TI de confiance.**

Dependencies: No dependencies

10.15 Cohérence de la reproduction des données de la TSF à l'intérieur de la TOE (FPT_TRC)

Comportement de la famille

454 Les exigences de cette famille sont nécessaires pour garantir la cohérence des données de la TSF quand de telles données sont reproduites à l'intérieur de la TOE. Celles-ci peuvent devenir incohérentes si le canal interne entre des parties de la TOE devient inopérant. Si la TOE est structurée en interne comme un réseau et si des éléments de connexion du réseau de la TOE sont détruits, cette incohérence peut se produire quand ces parties de la TOE sont déconnectés.

Classement des composants

455 Cette famille n'est constituée que d'un seul composant, "FPT_TRC.1 Cohérence interne de la TSF", qui exige que la TSF garantisse la cohérence des données de la TSF qui sont reproduites à plusieurs endroits.

Administration : FPT_TRC.1

456 Il n'y a pas d'activités d'administration prévues.

Audit : FPT_TRC.1

457 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : restauration de la cohérence à la reconnexion ;

b) Elémentaire : incohérences détectées entre des données de la TSF.

FPT_TRC.1 Cohérence interne de la TSF

Hiérarchique à : aucun autre composant.

FPT_TRC.1.1 La TSF doit garantir que des données de la TSF sont cohérentes quand elles sont reproduites entre des parties de la TOE.

FPT_TRC.1.2 Quand des parties de la TOE contenant des données de la TSF qui ont été reproduites sont déconnectées, la TSF doit garantir la cohérence de ces données à la reconnexion avant de traiter toute demande pour [affectation : *liste des SF dépendant de la cohérence de la reproduction des données de la TSF*].

Dépendances : **FPT_ITT.1 Protection élémentaire des données de la TSF lors d'un transfert interne**

10.16 Autotest de la TSF (FPT_TST)

Comportement de la famille

458 La famille définit les exigences pour l'autotest de la TSF par rapport à un comportement correct attendu. On peut citer comme exemple des interfaces vers des fonctions d'application, et des opérations arithmétiques d'échantillonnage sur des parties critiques de la TOE. Ces tests peuvent être menés au démarrage, de façon périodique, à la demande de l'utilisateur autorisé, ou quand d'autres conditions sont remplies. Les actions à entreprendre par la TOE à la suite de l'autotest sont définies dans d'autres familles.

459 Les exigences de cette famille sont également nécessaires pour détecter l'altération du code exécutable de la TSF (i.e. du logiciel de la TSF) et des données de la TSF dues à diverses défaillances qui ne provoquent pas nécessairement l'arrêt du fonctionnement de la TOE (qui serait pris en compte par d'autres familles). Ces vérifications doivent être effectuées car ces défaillances ne peuvent pas toujours être empêchées. De telles défaillances peuvent survenir soit parce qu'il existe des modes de défaillance non prévus ou des contrôles non prévus associés à ces modes de défaillance dans la conception du matériel, des micro-programmes ou du logiciel, soit à cause de l'altération malveillante de la TSF due à une protection logique ou physique inadaptée.

Classement des composants

460 Le composant "FPT_TST.1 Test de la TSF" offre l'aptitude de tester le fonctionnement correct de la TSF. Ces tests peuvent être effectués au démarrage, de façon périodique, à la demande de l'utilisateur autorisé, ou quand d'autres conditions sont remplies. Il offre aussi l'aptitude de contrôler l'intégrité de données de la TSF et du code exécutable.

Administration : FPT_TST.1

461 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) administration des conditions dans lesquelles l'autotest de la TSF a lieu, comme par exemple au démarrage, à des intervalles réguliers ou dans des conditions spécifiées ;

b) administration de l'intervalle de temps si cela est approprié.

Audit : FPT_TST.1

462 Les actions suivantes devraient être auditées dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Elémentaire : exécution des autotests de la TSF et résultats de ces tests.

FPT_TST.1 Test de la TSF

Hiérarchique à : aucun autre composant.

FPT_TST.1.1 **La TSF doit exécuter une suite d'autotests [sélection :** ***pendant le démarrage initial, de façon périodique pendant le fonctionnement normal, à la demande de l'utilisateur autorisé, dans les conditions*** **[affectation :** ***conditions dans lesquelles l'autotest devrait intervenir*****]] pour démontrer le fonctionnement correct de la TSF.**

FPT_TST.1.2 **La TSF doit fournir aux utilisateurs autorisés la capacité de contrôler l'intégrité de données de la TSF.**

FPT_TST.1.3 **La TSF doit fournir aux utilisateurs autorisés la capacité de contrôler l'intégrité du code exécutable de la TSF stocké.**

Dépendances : **FPT_AMT.1 Test de la machine abstraite**

11 Classe FRU : Utilisation des ressources

463 Cette classe inclut trois familles qui concernent la disponibilité des ressources nécessaires telles que la capacité de calcul ou la capacité de stockage. La famille “Tolérance aux pannes” fournit une protection contre l’indisponibilité de capacités due à une défaillance de la TOE. La famille “Priorité de service” garantit que les ressources seront allouées aux tâches les plus importantes ou dont l’exécution immédiate est critique et ne pourront pas être monopolisées par des tâches de moindre priorité. La famille “Allocation des ressources” fournit des limites à l’utilisation des ressources disponibles, empêchant ainsi les utilisateurs de monopoliser les ressources.

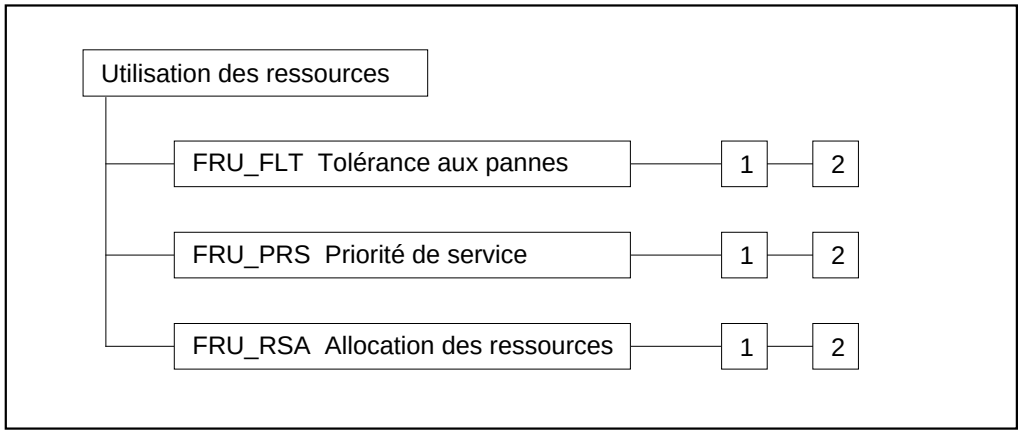


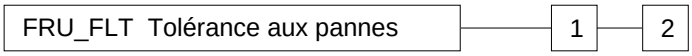
Figure 11.1 - Décomposition de la classe “Utilisation des ressources”

11.1 Tolérance aux pannes (FRU_FLT)

Comportement de la famille

464 Les exigences de cette famille garantissent que la TOE conservera un fonctionnement correct même en cas de défaillances.

Classement des composants



465 Le composant “FRU_FLT.1 Tolérance aux pannes avec mode dégradé” exige que la TOE continue à offrir un fonctionnement correct pour des capacités identifiées en cas de défaillances identifiées.

466 Le composant “FRU_FLT.2 Tolérance aux pannes limitée” exige que la TOE continue à offrir un fonctionnement correct pour toutes ses capacités en cas de défaillances identifiées.

Administration : FRU_FLT.1, FRU_FLT.2

467 Il n’y a pas d’activités d’administration prévues.

Audit : FRU_FLT.1

468 Les actions suivantes devraient être auditables dans le cas où la famille “FAU_GEN Génération des données de l’audit de sécurité” est incluse dans le PP ou la ST :

a) Minimal : toute défaillance détectée par la TSF ;

b) Elémentaire : toutes les capacités de la TOE interrompues à cause d’une défaillance.

Audit : FRU_FLT.2

469 Les actions suivantes devraient être auditables dans le cas où la famille “FAU_GEN Génération des données de l’audit de sécurité” est incluse dans le PP ou la ST :

a) Minimal : toute défaillance détectée par la TSF.

FRU_FLT.1 Tolérance aux pannes avec mode dégradé

Hiérarchique à : aucun autre composant.

FRU_FLT.1.1 **La TSF doit garantir le fonctionnement de [affectation : *liste des capacités de la TOE*] lorsque les défaillances suivantes surviennent : [affectation : *liste des types de défaillance*].**

Dépendances : **FPT_FLS.1 Défaillance avec préservation d'un état sûr**

FRU_FLT.2 Tolérance aux pannes limitée

Hiéarchique à : FRU_FLT.1

FRU_FLT.2.1 La TSF doit garantir le fonctionnement de **toutes les capacités de la TOE** lorsque les défaillances suivantes surviennent : [affectation : *liste des types de défaillance*] .

Dépendances : FPT_FLS.1 Défaillance avec préservation d'un état sûr

11.2 Priorité de service (FRU_PRS)

Comportement de la famille

470 Les exigences de cette famille permettent à la TSF de contrôler l'utilisation de ressources au sein du TSC par des utilisateurs et des sujets de telle sorte que les activités prioritaires au sein du TSC seront toujours exécutées sans interférence ou retard excessifs dus aux activités de faible priorité.

Classement des composants

471 Le composant "FRU_PRS.1 Priorité de service limitée" fournit des priorités pour l'utilisation par un sujet d'un sous-ensemble de ressources au sein du TSC.

472 Le composant "FRU_PRS.2 Priorité de service totale" fournit des priorités pour l'utilisation par un sujet de toutes les ressources au sein du TSC.

Administration : FRU_PRS.1, FRU_PRS.2

473 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) l'affectation des priorités à chaque sujet de la TSF.

Audit : FRU_PRS.1, FRU_PRS.2

474 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : rejet d'une opération basé sur l'utilisation d'une priorité dans le cadre d'une allocation ;

b) Elémentaire : toutes les tentatives d'utilisation de la fonction d'allocation qui touche à la priorité des fonctions de service.

FRU_PRS.1 Priorité de service limitée

Hiérarchique à : aucun autre composant.

FRU_PRS.1.1 La TSF doit affecter une priorité à chaque sujet de la TSF.

FRU_PRS.1.2 La TSF doit garantir que chaque accès à [affectation : *ressources contrôlées*] doit être accordé sur la base de la priorité allouée aux sujets.

Dependencies: No dependencies

FRU_PRS.2 Priorité de service totale

Hiéarchique à : FRU_PRS.1

FRU_PRS.2.1 La TSF doit affecter une priorité à chaque sujet de la TSF.

FRU_PRS.2.2 La TSF doit garantir que chaque accès à **toutes les ressources partageables** doit être accordé sur la base de la priorité allouée aux sujets.

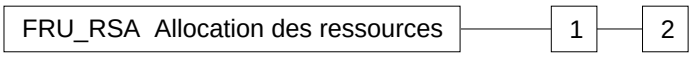
Dependencies: No dependencies

11.3 Allocation des ressources (FRU_RSA)

Comportement de la famille

475 Les exigences de cette famille permettent à la TSF de contrôler l'utilisation des ressources par les utilisateurs et les sujets de telle sorte qu'un déni de service ne pourra survenir du fait de la monopolisation non autorisée de ressources.

Classement des composants



476 Le composant "FRU_RSA.1 Quotas maximums" fournit des exigences pour des mécanismes de quotas qui garantissent que les utilisateurs et les sujets ne monopoliseront pas une ressource contrôlée.

477 Le composant "FRU_RSA.2 Quotas minimums et maximums" fournit des exigences pour des mécanismes de quota qui garantissent que les utilisateurs et les sujets disposeront toujours au moins d'un minimum d'une ressource spécifiée et qu'ils ne seront pas capables de monopoliser une ressource contrôlée.

Administration : FRU_RSA.1

478 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) la spécification par un administrateur des limites maximums pour l'utilisation d'une ressource par des groupes d'utilisateurs, des utilisateurs individuels ou des sujets.

Administration : FRU_RSA.2

479 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) la spécification par un administrateur des limites minimums et maximums pour l'utilisation d'une ressource par des groupes d'utilisateurs, des utilisateurs individuels ou des sujets.

Audit : FRU_RSA.1, FRU_RSA.2

480 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : rejet d'une opération d'allocation dû aux limites d'utilisation des ressources ;

b) Elémentaire : toutes les tentatives d'utilisation des fonctions d'allocation de ressources qui sont sous le contrôle de la TSF.

FRU_RSA.1 Quotas maximums

Hiérarchique à : aucun autre composant.

FRU_RSA.1.1 **La TSF doit appliquer des quotas maximums pour les ressources suivantes : [affectation : *ressources contrôlées*] que [sélection : un *utilisateur individuel, un groupe défini d'utilisateurs, des sujets*] peuvent utiliser [sélection : *simultanément, pendant une période de temps spécifiée*].**

Dependencies: No dependencies

FRU_RSA.2 Quotas minimums et maximums

Hiéarchique à : FRU_RSA.1

FRU_RSA.2.1 La TSF doit appliquer des quotas maximums pour les ressources suivantes [affectation : *ressources contrôlées*] que [sélection : un *utilisateur individuel, un groupe défini d'utilisateurs*] peuvent utiliser [sélection : *simultanément, pendant une période de temps spécifiée*].

FRU_RSA.2.2 **La TSF doit garantir la fourniture d'une quantité minimum de chaque [affectation : *ressource contrôlée*] qui soit disponible pour une utilisation [sélection : *simultanée, pendant une période de temps spécifiée*] par [sélection : *un utilisateur individuel, un groupe défini d'utilisateurs, des sujets*].**

Dependencies: No dependencies

12 Classe FTA : Accès à la TOE

481 La présente classe spécifie des exigences fonctionnelles pour contrôler l'établissement d'une session utilisateur.

482 La figure 12.1 montre la décomposition de cette classe en ses composants constitutifs.

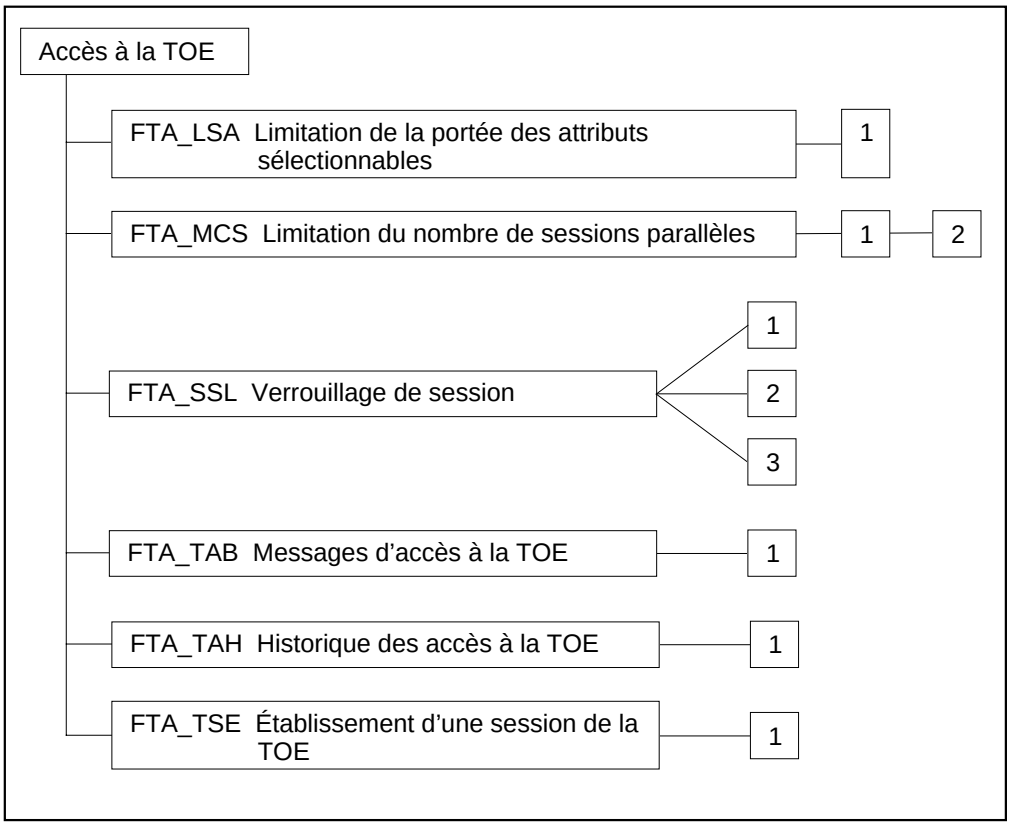


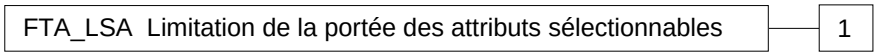
Figure 12.1 - Décomposition de la classe "Accès à la TOE"

12.1 Limitation de la portée des attributs sélectionnables (FTA_LSA)

Comportement de la famille

483 La présente famille définit des exigences pour limiter le portée des attributs de sécurité de session qu'un utilisateur peut sélectionner pour une session.

Classement des composants



484 Le composant "FTA_LSA.1 Limitation de la portée des attributs sélectionnables" fournit les exigences pour qu'une TOE limite la portée des attributs de sécurité de session pendant l'établissement de la session.

Administration : FTA_LSA.1

485 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) l'administration de la portée des attributs de sécurité de session par un administrateur.

Audit : FTA_LSA.1

486 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : toutes les tentatives infructueuses pour sélectionner des attributs de sécurité de session ;

b) Elémentaire : toutes les tentatives pour sélectionner des attributs de sécurité de session ;

c) Détaillé : capture des valeurs de chaque attribut de sécurité de session.

FTA_LSA.1 Limitation de la portée des attributs sélectionnables

Hiérarchique à : aucun autre composant.

FTA_LSA.1.1 La TSF doit limiter la portée des attributs de sécurité de session [affectation : *attributs de sécurité de session*] en fonction de [affectation : *attributs*].

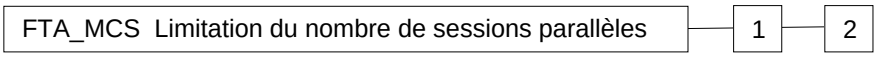
Dependencies: No dependencies

12.2 Limitation du nombre de sessions parallèles (FTA_MCS)

Comportement de la famille

487 La présente famille définit des exigences pour mettre des limites au nombre de sessions parallèles qui appartiennent au même utilisateur.

Classement des composants



488 Le composant "FTA_MCS.1 Limitation élémentaire du nombre de sessions parallèles" fournit des limitations qui s'appliquent à tous les utilisateurs de la TSF.

489 Le composant "FTA_MCS.2 Limitation du nombre de sessions parallèles par les attributs de l'utilisateur" étend les exigences de FTA_MCS.1 en exigeant l'aptitude de spécifier des limitations portant sur le nombre de sessions parallèles, en fonction des attributs de sécurité associés.

Administration : FTA_MCS.1

490 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) l'administration par un administrateur du nombre maximum de sessions utilisateur parallèles autorisées.

Administration : FTA_MCS.2

491 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) l'administration par un administrateur des règles qui régissent le nombre maximum de sessions utilisateur parallèles autorisées.

Audit : FTA_MCS.1, FTA_MCS.2

492 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : rejet d'une nouvelle session en fonction de la limitation du nombre de sessions parallèles ;

b) Détaillé : capture du nombre de sessions utilisateur parallèles en cours et de l'attribut ou des attributs de sécurité de l'utilisateur.

FTA_MCS.1 Limitation élémentaire du nombre de sessions parallèles

Hiérarchique à : aucun autre composant.

FTA_MCS.1.1 **La TSF doit limiter le nombre maximum de sessions parallèles qui appartiennent au même utilisateur.**

FTA_MCS.1.2 **La TSF doit appliquer, par défaut, une limite de [affectation : *nombre par défaut*] sessions par utilisateur.**

Dépendances : **FIA_UID.1 Programmation de l'identification**

FTA_MCS.2 Limitation du nombre de sessions parallèles par les attributs de l'utilisateur

Hiéarchique à : FTA_MCS.1

FTA_MCS.2.1 La TSF doit limiter le nombre maximum de sessions parallèles qui appartiennent au même utilisateur **conformément aux règles [affectation : *règles relatives au nombre maximum de sessions parallèles*].**

FTA_MCS.2.2 La TSF doit appliquer, par défaut, une limite de [affectation : *nombre par défaut*] sessions par utilisateur.

Dépendances : **FIA_UID.1 Programmation de l'identification**

12.3 Verrouillage de session (FTA_SSL)

Comportement de la famille

493 La présente famille définit des exigences pour que la TSF offre la capacité de verrouiller et de déverrouiller des sessions interactives, à l'initiative de la TSF ou de l'utilisateur.

Classement des composants

494 Le composant "FTA_SSL.1 Verrouillage de session, initié par la TSF" inclut le verrouillage, initié par le système, d'une session interactive à la suite d'une période d'inactivité spécifiée d'un utilisateur.

495 Le composant "FTA_SSL.2 Verrouillage de session, initié par l'utilisateur" offre des capacités pour que l'utilisateur verrouille et déverrouille ses propres sessions interactives.

496 Le composant "FTA_SSL.3 Clôture de session, initiée par la TSF" fournit des exigences pour que la TSF termine la session à la suite d'une période d'inactivité d'un utilisateur.

Administration : FTA_SSL.1

497 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) la spécification de la durée d'inactivité d'un utilisateur à la suite de laquelle le verrouillage de la session d'un utilisateur individuel intervient ;

b) la spécification de la durée par défaut d'inactivité d'un utilisateur à la suite de laquelle le verrouillage intervient ;

c) l'administration des événements qui devraient survenir avant le déverrouillage de la session.

Administration : FTA_SSL.2

498 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) administration des événements qui devraient survenir avant le déverrouillage de la session.

Administration : FTA_SSL.3

499 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) la spécification de la durée d'inactivité d'un utilisateur à la suite de laquelle la clôture de la session interactive intervient pour un utilisateur individuel ;

b) la spécification de la durée par défaut d'inactivité d'un utilisateur à la suite de laquelle la clôture de la session interactive intervient.

Audit : FTA_SSL.1, FTA_SSL.2

500 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : verrouillage d'une session interactive par le mécanisme de verrouillage d'une session ;

b) Minimal : déverrouillage réussi d'une session interactive ;

c) Elémentaire : toute tentative pour déverrouiller une session interactive.

Audit : FTA_SSL.3

501 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : clôture d'une session interactive par le mécanisme de verrouillage de session.

FTA_SSL.1 Verrouillage de session, initié par la TSF

Hiérarchique à : aucun autre composant.

FTA_SSL.1.1 La TSF doit verrouiller une session interactive à la suite de [affectation : *durée d'inactivité d'un utilisateur*] :

a) en effaçant ou en écrasant le contenu des écrans d'affichage, les rendant ainsi illisibles ;

b) en désactivant tout moyen d'accès aux données de l'utilisateur ou d'affichage de celles-ci, excepté le déverrouillage de la session.

FTA_SSL.1.2 **La TSF doit exiger que les événements suivants interviennent avant le déverrouillage de la session : [affectation : *événements devant se produire*].**

Dépendances : **FIA_UAU.1 Programmation de l'authentification**

FTA_SSL.2 Verrouillage de session, initié par l'utilisateur

Hiérarchique à : aucun autre composant.

FTA_SSL.2.1 **La TSF doit autoriser l'utilisateur à verrouiller sa propre session interactive :**

a) **en effaçant ou en écrasant le contenu des écrans d'affichage, les rendant ainsi illisibles ;**

b) **en désactivant tout moyen d'accès aux données de l'utilisateur ou d'affichage de celles-ci, excepté le déverrouillage de la session.**

FTA_SSL.2.2 **La TSF doit exiger que les événements suivants interviennent avant le déverrouillage de la session : [affectation : *événements devant se produire*].**

Dépendances : **FIA_UAU.1 Programmation de l'authentification**

FTA_SSL.3 Clôture de session, initiée par la TSF

Hiérarchique à : aucun autre composant.

FTA_SSL.3.1 **La TSF doit terminer une session interactive à la suite de [affectation : *période d'inactivité d'un utilisateur*].**

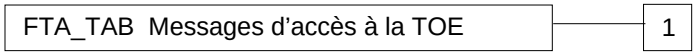
Dependencies: No dependencies

12.4 Messages d'accès à la TOE (FTA_TAB)

Comportement de la famille

502 La présente famille définit des exigences pour afficher un message d'avertissement informatif configurable concernant une utilisation appropriée de la TOE.

Classement des composants



503 Le composant "FTA_TAB.1 Messages par défaut d'accès à la TOE" exige l'affichage d'un message d'accès à la TOE. Ce message est affiché avant le dialogue d'établissement d'une session.

Administration : FTA_TAB.1

504 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) la maintenance du message par l'administrateur autorisé.

Audit : FTA_TAB.1

505 Il n'y a pas d'actions identifiées qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FTA_TAB.1 Messages par défaut d'accès à la TOE

Hiérarchique à : aucun autre composant.

FTA_TAB.1.1 Avant d'établir une session utilisateur, la TSF doit afficher un message d'avertissement informatif relatif à l'utilisation non autorisée de la TOE.

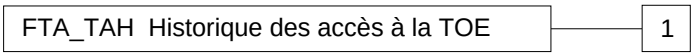
Dependencies: No dependencies

12.5 Historique des accès à la TOE (FTA_TAH)

Comportement de la famille

506 La présente famille définit des exigences pour que la TSF affiche à l'attention d'un utilisateur, après l'établissement réussi d'une session, un historique des tentatives réussies et infructueuses pour accéder au compte de l'utilisateur.

Classement des composants



507 Le composant "FTA_TAH.1 Historique des accès à la TOE" exige qu'une TOE affiche des informations associées aux tentatives précédentes d'établissement d'une session.

Administration : FTA_TAH.1

508 Il n'y a pas d'activités d'administration prévues.

Audit : FTA_TAH.1

509 Il n'y a pas d'actions identifiées qui devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST.

FTA_TAH.1 Historique des accès à la TOE

Hiérarchique à : aucun autre composant.

FTA_TAH.1.1 Dès l'établissement réussi d'une session, la TSF doit afficher à l'attention de l'utilisateur [sélection : *la date, l'heure, la méthode, le lieu*] du dernier établissement réussi d'une session.

FTA_TAH.1.2 Dès l'établissement réussi d'une session, la TSF doit afficher [sélection : *la date, l'heure, la méthode, le lieu*] de la dernière tentative d'établissement infructueuse d'une session et le nombre de tentatives infructueuses depuis le dernier établissement réussi d'une session.

FTA_TAH.1.3 La TSF ne doit pas effacer les informations concernant l'historique des accès de l'interface utilisateur sans laisser à l'utilisateur la possibilité de revoir ces informations.

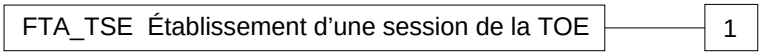
Dependencies: No dependencies

12.6 Établissement d'une session de la TOE (FTA_TSE)

Comportement de la famille

510 La présente famille définit des exigences pour refuser à un utilisateur la permission d'établir une session avec la TOE.

Classement des composants



511 Le composant "FTA_TSE.1 Établissement d'une session de la TOE" fournit des exigences pour refuser l'accès à la TOE à des utilisateurs en fonction d'attributs.

Administration : FTA_TSE.1

512 Les actions suivantes pourraient être prises en compte pour les activités d'administration de la classe FMT :

a) administration des conditions de l'établissement de la session par l'administrateur autorisé.

Audit : FTA_TSE.1

513 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : refus de l'établissement d'une session provoqué par le mécanisme d'établissement de session ;

b) Elémentaire : toutes les tentatives d'établissement d'une session utilisateur ;

c) Détaillé : capture de la valeur des paramètres d'accès sélectionnés (e.g. lieu d'accès, heure d'accès).

FTA_TSE.1 Établissement d'une session de la TOE

Hiérarchique à : aucun autre composant.

FTA_TSE.1.1 La TSF doit être capable de refuser l'établissement d'une session en fonction de [affectation : *attributs*].

Dependencies: No dependencies

13 Classe FTP : Chemins et canaux de confiance

514 Les familles de la présente classe fournissent des exigences pour l'établissement d'un chemin de communication de confiance entre des utilisateurs et la TSF, et d'un canal de communication de confiance entre la TSF et d'autres produits TI de confiance. Les chemins et les canaux de confiance ont les caractéristiques générales suivantes :

- Le chemin de communication est construit en utilisant des canaux de communication internes et externes (selon le composant) qui isolent un sous-ensemble identifié de données et de commandes de la TSF du reste de la TSF et des données de l'utilisateur.

- L'utilisation du chemin de communication peut être initiée par l'utilisateur ou par la TSF (selon le composant).

- Le chemin de communication est capable de procurer l'assurance que l'utilisateur communique avec la véritable TSF, et que la TSF communique avec le véritable utilisateur (selon le composant).

515 Dans ce paradigme, un **canal de confiance** est un canal de communication qui peut être initié indifféremment par chaque extrémité du canal, et qui offre des caractéristiques de non-répudiation de l'identité des extrémités du canal.

516 Un **chemin de confiance** offre aux utilisateurs un moyen d'exécuter des fonctions par une interaction qui est garantie directe avec la TSF. L'existence d'un chemin de confiance est généralement souhaitée pour des actions de l'utilisateur telles que l'identification ou l'authentification initiale, mais peut aussi être souhaitée à d'autres moments au cours d'une session utilisateur. Les échanges via un chemin de confiance peuvent être initiés par un utilisateur ou par la TSF. Les réponses de l'utilisateur via le chemin de confiance ont la garantie d'être protégées contre une modification par des applications non sûres, ou contre une divulgation vers celles-ci.

517 La figure 13.1 montre la décomposition de la présente classe en ses composants constitutifs.

Classe FTP

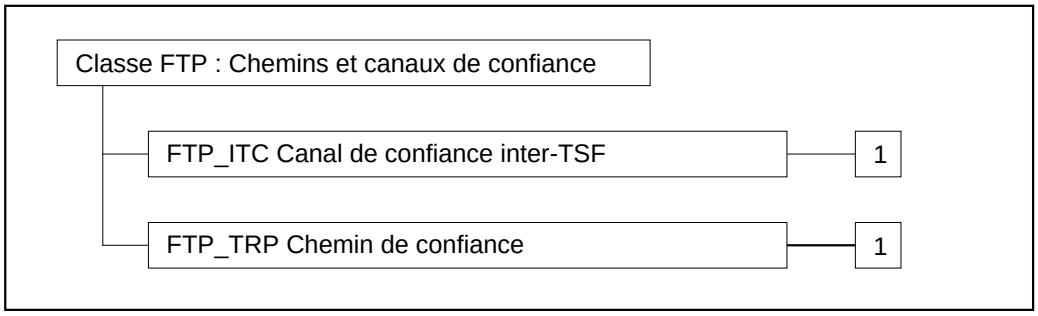


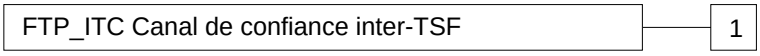
Figure 13.1 - Décomposition de la classe “Chemins et canaux de confiance”

13.1 Canal de confiance inter-TSF (FTP_ITC)

Comportement de la famille

518 La présente famille définit des exigences pour la création d'un canal de confiance entre la TSF et d'autres produits TI de confiance pour l'exécution d'opérations critiques pour la sécurité. Cette famille devrait être utilisée chaque fois qu'il y a des exigences pour la communication sûre de données de l'utilisateur ou de la TSF entre la TOE et d'autres produits TI de confiance.

Classement des composants



519 Le composant "FTP_ITC.1 Canal de confiance inter-TSF" exige que la TSF offre un canal de communication de confiance entre elle-même et un autre produit TI de confiance.

Administration : FTP_ITC.1

520 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la configuration des actions qui exigent un canal de confiance, si celui-ci est mis en œuvre.

Audit : FTP_ITC.1

521 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : défaillances des fonctions du canal de confiance ;

b) Minimal : identification de l'initiateur et de la cible des fonctions défaillantes du canal de confiance ;

c) Elémentaire : toutes les tentatives d'utilisation des fonctions du canal de confiance ;

d) Elémentaire : identification de l'initiateur et de la cible de toutes les fonctions du canal de confiance.

FTP_ITC.1 Canal de confiance inter-TSF

Hiérarchique à : aucun autre composant.

FTP_ITC.1.1 **La TSF doit fournir un canal de communication entre elle-même et un produit TI de confiance distant qui soit logiquement distinct des autres canaux de communication et qui garantisse l'identification de ses extrémités et la protection des données transitant par le canal contre la modification ou la divulgation.**

FTP_ITC.1.2 **La TSF doit permettre à [sélection : *la TSF, le produit TI de confiance distant*] d'initier la communication via le canal de confiance.**

FTP_ITC.1.3 **La TSF doit initier la communication via le canal de confiance pour [affectation : *liste des fonctions pour lesquelles un canal de confiance est exigé*].**

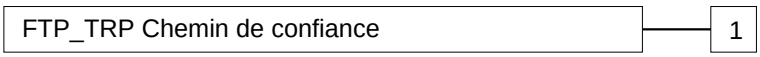
Dependencies: No dependencies

13.2 Chemin de confiance (FTP_TRP)

Comportement de la famille

522 La présente famille définit des exigences pour établir et maintenir une communication sûre en provenance d'utilisateurs ou de la TSF ou vers ces derniers. Un chemin de confiance peut être exigé pour toute interaction touchant à la sécurité. Les échanges via un chemin de confiance peuvent être initiés par un utilisateur au cours d'une interaction avec la TSF, ou bien la TSF peut établir la communication avec l'utilisateur via un chemin de confiance.

Classement des composants



523 Le composant "FTP_TRP.1 Chemin de confiance" exige qu'un chemin de confiance entre la TSF et un utilisateur soit fourni pour un ensemble d'événements défini par l'auteur d'un PP ou d'une ST. L'utilisateur ou la TSF peuvent avoir l'aptitude d'initier le chemin de confiance.

Administration : FTP_TRP.1

524 Les actions suivantes pourraient être prises en compte pour les fonctions d'administration de la classe FMT :

a) la configuration des actions qui exigent un canal de confiance, s'il est mis en œuvre.

Audit : FTP_TRP.1

525 Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : défaillance des fonctions du chemin de confiance ;

b) Minimal : identification de l'utilisateur associé à toutes les défaillances du chemin de confiance, si cette information est disponible ;

c) Elémentaire : toutes les tentatives d'utilisation des fonctions du chemin de confiance ;

d) Elémentaire : identification de l'utilisateur associé à tous les appels au chemin de confiance, si cette information est disponible.

FTP_TRP.1 Chemin de confiance

Hiérarchique à : aucun autre composant.

FTP_TRP.1.1 **La TSF doit fournir un chemin de communication entre elle-même et des utilisateurs [sélection : *distants, locaux*] qui soit logiquement distinct des autres chemins de communication et qui garantisse l'identification de ses extrémités et la protection des données transférées contre une modification ou une divulgation.**

FTP_TRP.1.2 **La TSF doit permettre à [sélection : *la TSF, des utilisateurs locaux, des utilisateurs distants*] d'initier une communication via le chemin de confiance.**

FTP_TRP.1.3 **La TSF doit exiger l'utilisation du chemin de confiance pour [sélection : *authentification initiale d'un utilisateur,* [affectation : *autres services pour lesquels un chemin de confiance est exigé*]].**

Dependencies: No dependencies

Annexe A
(Informative)

Notes d'application relatives aux exigences fonctionnelles de sécurité

526 La présente annexe contient des informations concernant les familles et les composants définis dans les éléments normatifs de la partie 2 des CC, dont les utilisateurs, développeurs ou évaluateurs peuvent avoir besoin pour utiliser les composants. Afin de faciliter la recherche des informations pertinentes, la présentation des classes, familles et composants de cette annexe est similaire à la présentation des éléments normatifs. La structure des classes, familles, et composants de cette annexe diffère de celle du corps principale de cette partie des CC, car cette annexe ne concerne que les sections à caractère informatif.

A.1 Structure des notes

527 Cette section définit le contenu et la présentation des notes relatives aux exigences fonctionnelles des CC.

A.1.1 Structure d'une classe

528 La figure A.1 ci-dessous illustre la structure d'une classe fonctionnelle dans cette annexe.

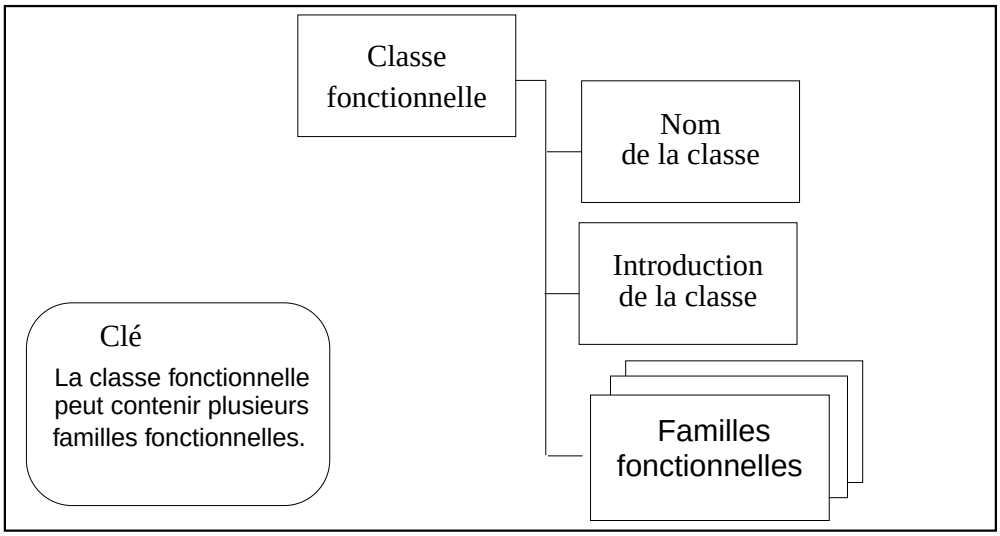


Figure A.1 - Structure d'une classe fonctionnelle

A.1.1.1 Nom de la classe

529 Il s'agit du nom unique de la classe, défini dans les éléments normatifs de cette partie des CC.

A.1.1.2 Introduction de la classe

530 La rubrique "Introduction de la classe" de cette annexe donne des informations sur l'utilisation des familles et des composants de la classe. Ces informations sont complétées par le diagramme décrivant l'organisation des familles de chaque classe et les relations hiérarchiques entre les composants de chaque famille.

A.1.2 Structure d'une famille

531 La figure A.2 illustre sous forme de diagramme la structure des notes d'application pour une famille fonctionnelle.

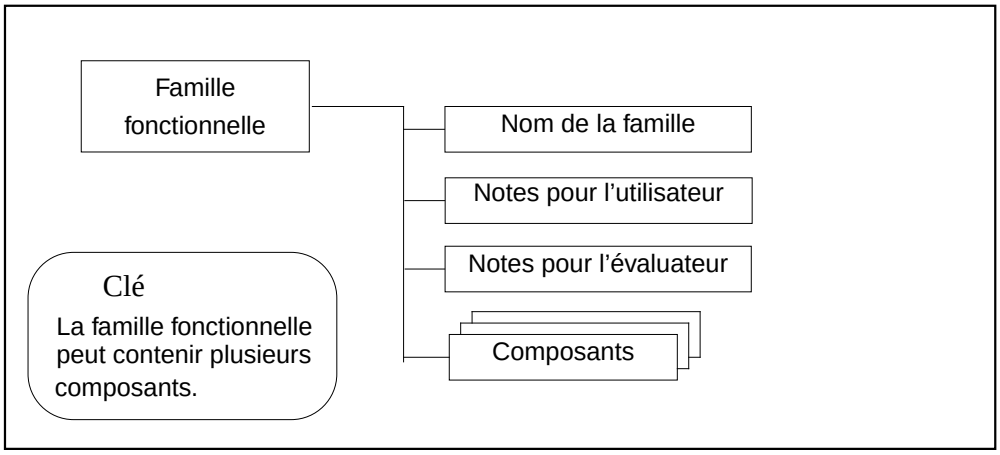


Figure A.2 - Structure des notes d'application pour une famille fonctionnelle

A.1.2.1 Nom de la famille

532 Il s'agit du nom unique de la famille, défini dans les éléments normatifs de cette partie des CC.

A.1.2.2 Notes pour l'utilisateur

533 Les *notes pour l'utilisateur* contiennent des informations supplémentaires qui présentent un intérêt pour les utilisateurs potentiels de la famille, qui sont les auteurs de PP, de ST et de paquets fonctionnels, ainsi que les développeurs de TOE incorporant des composants fonctionnels. La présentation est faite à titre informatif, et pourrait couvrir les avertissements concernant des limitations d'utilisation ainsi que les domaines qui pourraient nécessiter une attention spécifique lors de l'utilisation des composants.

A.1.2.3 Notes pour l'évaluateur

534 Les *notes pour l'évaluateur* contiennent toute information présentant un intérêt pour les développeurs et les évaluateurs de TOE qui prétendent se conformer à un composant de la famille. La présentation est faite à titre informatif, et peut couvrir des domaines variés pour lesquels une attention spécifique pourrait être nécessaire lors de l'évaluation de la TOE. Les informations pourraient inclure des clarifications concernant la signification et une spécification sur la façon d'interpréter les exigences ainsi que les mises en gardes et autres avertissements qui présentent un intérêt spécifique pour les évaluateurs.

535 Les sections "Notes pour l'utilisateur" et "Notes pour l'évaluateur" ne sont pas obligatoires et n'apparaissent que si cela est approprié.

A.1.3 Structure d'un composant

536 La figure A.3 illustre la structure des notes d'application pour un composant fonctionnel.

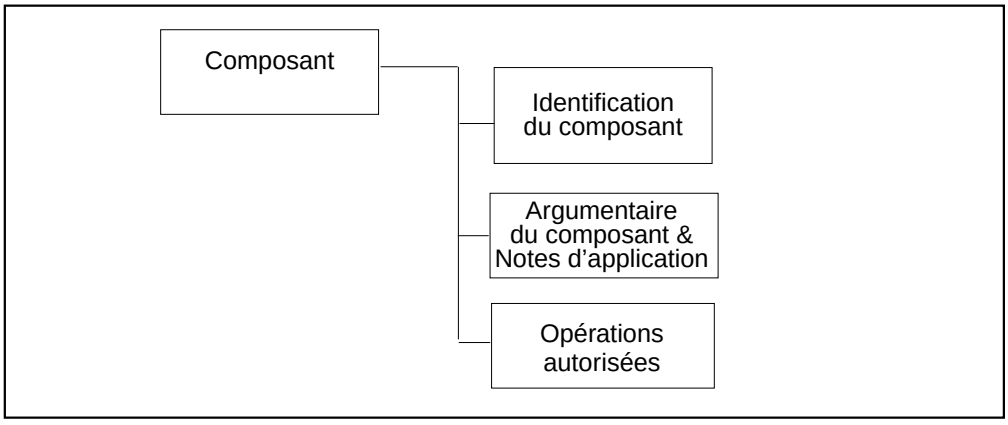


Figure A.3 - Structure d'un composant fonctionnel

A.1.3.1 Identification du composant

537 Il s'agit du nom unique du composant, défini dans les éléments normatifs de cette partie des CC.

A.1.3.2 Argumentaire d'un composant et notes d'application

538 Toute information spécifique liée au composant peut être trouvée dans cette section.

- L'*argumentaire* contient les détails provenant du raffinement des déclarations générales concernant l'argumentaire pour le niveau particulier, et ne devrait être utilisé que dans le cas où une augmentation spécifique du niveau est nécessaire.

- Les *notes d’application* contiennent un raffinement supplémentaire en terme d’explication discursive dans la mesure où il s’applique à un composant spécifique. Ce raffinement peut faire partie des notes pour l’utilisateur ou des notes pour l’évaluateur telles qu’elles sont définies dans la section A.1.2. Il peut être utilisé pour expliquer la nature des dépendances (e.g. informations partagées ou opération partagée).

539 Cette section n’est pas obligatoire et n’apparaît que si cela est approprié.

A.1.3.3 Opérations autorisées

540 Cette partie de chaque composant contient des conseils concernant les opérations autorisées pour le composant.

541 Cette section n’est pas obligatoire et n’apparaît que si cela est approprié.

A.2 Tableau des dépendances

542 Le Tableau A.1 - Tableau des dépendances pour les composants fonctionnels, indique leurs dépendances directes, indirectes et optionnelles. Chacun des composants qui présente une dépendance vis-à-vis d’un certain composant fonctionnel correspond à une colonne. Chaque composant fonctionnel correspond à une ligne. La valeur contenue dans une cellule du tableau indique si le composant mentionné dans la colonne est exigé directement (indiqué par une croix ‘X’), exigé indirectement (indiqué par un tiret ‘-’), ou exigé en option (indiqué par un ‘o’) par le composant mentionné dans la ligne. FDP_ETC.1, qui exige la présence soit de FDP_ACC.1, soit de FDP_IFC.1, constitue un exemple d’un composant présentant des dépendances optionnelles. Ainsi, si FDP_ACC.1 est présent, FDP_IFC.1 n’est pas nécessaire et vice versa. Si la cellule est vide, le composant ne dépend pas d’un autre composant.

Tableau A.1 - Tableau des dépendances pour les composants fonctionnels

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FAU_ARP.1					-	x																									-				
FAU_GEN.1																															x				
FAU_GEN.2					x																	x									-				

Tableau A.1 - Tableau des dépendances pour les composants fonctionnels

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FAU_SAA.1					x																										-				
FAU_SAA.2																						x													
FAU_SAA.3																																			
FAU_SAA.4																																			
FAU_SAR.1					x																										-				
FAU_SAR.2					-		x																								-				
FAU_SAR.3					-		x																								-				
FAU_SEL.1					x																	-					x	-			-				
FAU_STG.1					x																										-				
FAU_STG.2					x																										-				
FAU_STG.3					-			x																							-				
FAU_STG.4					x																										-				
FCO_NRO.1																						x													
FCO_NRO.2																						x													
FCO_NRR.1																						x													
FCO_NRR.2																						x													
FCS_CKM.1	-								-	o	x	o	-	-	-	-	-					-		-	x	-		-							
FCS_CKM.2	-								o	-	x	-	-	-	-	-	o					-		-	x	-		-							
FCS_CKM.3	-								o	-	x	-	-	-	-	-	o					-		-	x	-		-							
FCS_CKM.4	-								o	-	-	-	-	-	-	-	o					-		-	x	-		-							
FCS_COP.1	-								o	-	x	-	-	-	-	-	o					-		-	x	-		-							
FCS_COP.2	-								o	-	x	-	-	-	-	-	o					-		-	x	-		-							
FDP_ACC.1													-	x	-	-						-		-		-		-							

Tableau A.1 - Tableau des dépendances pour les composants fonctionnels

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FDP_ACC.2													-	x	-	-					-		-		-		-								
FDP_ACF.1													x	-	-	-					-		-		x		-								
FDP_DAU.1																																			
FDP_DAU.2																					x														
FDP_ETC.1													o	-	o	-					-		-		-		-								
FDP_ETC.2													o	-	o	-					-		-		-		-								
FDP_IFC.1													-	-	-	x					-		-		-		-								
FDP_IFC.2													-	-	-	x					-		-		-		-								
FDP_IFF.1													-	-	x	-					-		-		x		-								
FDP_IFF.2													-	-	x	-					-		-		x		-								
FDP_IFF.3			x										-	-	x	-					-		-		-		-								
FDP_IFF.4			x										-	-	x	-					-		-		-		-								
FDP_IFF.5				x									-	-	x	-					-		-		-		-								
FDP_IFF.6			x										-	-	x	-					-		-		-		-								
FDP_ITC.1													o	-	o	-					-		-		x		-								
FDP_ITC.2													o	-	o	-					-		-		-		-					x		o	
FDP_ITT.1													o	-	o	-					-		-		-		-								
FDP_ITT.2													o	-	o	-					-		-		-		-								
FDP_ITT.3													o	-	o	-		x			-		-		-		-								
FDP_ITT.4													o	-	o	-			x		-		-		-		-								
FDP_RIP.1																																			
FDP_RIP.2																																			
FDP_ROL.1													o	-	o	-					-		-		-		-								

Tableau A.1 - Tableau des dépendances pour les composants fonctionnels

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FDP_ROL.2													o	-	o	-						-		-		-		-								
FDP_SDI.1																																				
FDP_SDI.2																																				
FDP_UCT.1													o	-	o	-						-		-		-		-							o	o
FDP_UIT.1													o	-	o	-						-		-		-		-							o	o
FDP_UIT.2													o	-	o	-						-		-		-		-							x	
FDP_UIT.3													o	-	o	-						-		-		-		-							x	
FIA_AFL.1																					x	-														
FIA_ATD.1																																				
FIA_SOS.1																																				
FIA_SOS.2																																				
FIA_UAU.1																						x														
FIA_UAU.2																						x														
FIA_UAU.3																																				
FIA_UAU.4																																				
FIA_UAU.5																																				
FIA_UAU.6																																				
FIA_UAU.7																					x	-														
FIA_UID.1																																				
FIA_UID.2																																				
FIA_USB.1																				x																
FMT_MOF.1																						-						x								
FMT_MSA.1													o	-	o	-						-		-		-		x								

Tableau A.1 - Tableau des dépendances pour les composants fonctionnels

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_MTD.2	FMT_SMR.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FPT_ITC.1	FTP_TRP.1
FMT_MSA.2	x												o	-	o	-						-		x		-		x								
FMT_MSA.3													-	-	-	-						-		x		-		x								
FMT_MTD.1																						-						x								
FMT_MTD.2																						-					x	x								
FMT_MTD.3	x																					-					x	-								
FMT_REV.1																						-						x								
FMT_SAE.1																						-						x				x				
FMT_SMR.1																						x														
FMT_SMR.2																																				
FMT_SMR.3																						-						x								
FPR_ANO.1																																				
FPR_ANO.2																																				
FPR_PSE.1																																				
FPR_PSE.2																						x														
FPR_PSE.3																																				
FPR_UNL.1																																				
FPR_UNO.1																																				
FPR_UNO.2																																				
FPT_AMT.1																																				
FPT_FLS.1	x																																			
FPT_ITA.1																																				
FPT_ITC.1																																				
FPT_ITI.1																																				

Tableau A.1 - Tableau des dépendances pour les composants fonctionnels

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FPT_ITI.2																														x					
FPT_ITT.1																																			
FPT_ITT.2																																			
FPT_ITT.3																														x					
FPT_PHP.1																						-	x					-							
FPT_PHP.2																						-	x					-							
FPT_PHP.3																																			
FPT_RCV.1	x	x																											-					x	
FPT_RCV.2	x	x																											-					x	
FPT_RCV.3	x	x																											-					x	
FPT_RCV.4	x																																		
FPT_RPL.1																																			
FPT_RVM.1																																			
FPT_SEP.1																																			
FPT_SEP.2																																			
FPT_SEP.3																																			
FPT_SSP.1																														x					
FPT_SSP.2																														x					
FPT_STM.1																																			
FPT_TDC.1																																			
FPT_TRC.1																														x					
FPT_TST.1																													x						
FRU_FLT.1	-																													x					

Tableau A.1 - Tableau des dépendances pour les composants fonctionnels

	ADV_SPM.1	AGD_ADM.1	AVA_CCA.1	AVA_CCA.3	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FAU_STG.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FDP_ITT.1	FDP_ITT.2	FDP_ITT.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_AMT.1	FPT_FLS.1	FPT_ITT.1	FPT_STM.1	FPT_TDC.1	FPT_TST.1	FTP_ITC.1	FTP_TRP.1
FRU_FLT.2	-																													x						
FRU_PRS.1																																				
FRU_PRS.2																																				
FRU_RSA.1																																				
FRU_RSA.2																																				
FTA_LSA.1																																				
FTA_MCS.1																							x													
FTA_MCS.2																							x													
FTA_SSL.1																						x	-													
FTA_SSL.2																						x	-													
FTA_SSL.3																																				
FTA_TAB.1																																				
FTA_TAH.1																																				
FTA_TSE.1																																				
FTP_ITC.1																																				
FTP_TRP.1																																				

Annexe B
(Informative)

Classes, familles et composants fonctionnels

543 Les annexes C à M qui suivent contiennent les notes d'application relatives aux classes fonctionnelles définies dans le corps de la partie 2.

Annexe C
(Informative)

Audit de sécurité (FAU)

544 Les familles CC relatives à l'audit donnent aux auteurs de PP ou de ST la possibilité de définir les exigences destinées à surveiller les activités de l'utilisateur et, dans certains cas, de détecter des violations réelles, potentielles ou imminentes de la TSP. Les fonctions d'audit de sécurité de la TOE sont définies pour contribuer à la surveillance d'évènements touchant à la sécurité, et pour exercer un effet dissuasif vis-à-vis de violations de la sécurité. Les exigences des familles relatives à l'audit concernent des fonctions incluant la protection des données d'audit, le format d'enregistrement, et la sélection d'évènements, ainsi que des outils d'analyse, des alarmes en cas de violation de la sécurité, et une analyse en temps réel. La trace d'audit devrait être présentée dans un format lisible, soit directement (e.g. en stockant la trace d'audit dans un format lisible), soit indirectement (e.g. en utilisant des outils de réduction des enregistrements d'audit), soit en utilisant les deux méthodes.

545 En développant les exigences de l'audit de sécurité, l'auteur du PP ou de la ST devrait noter les relations entre les familles et les composants relatifs à l'audit. Il est possible de spécifier un ensemble d'exigences pour l'audit qui satisfassent les listes de dépendances portant sur des familles ou des composants, tout en aboutissant dans le même temps à une fonction d'audit déficiente (e.g. une fonction d'audit qui exige que tous les évènements touchant à la sécurité soient audités mais sans les contrôler sélectivement sur une base raisonnable, par exemple en les choisissant par utilisateur individuel ou par objet).

Exigences d'audit dans un environnement distribué :

546 L'implémentation d'exigences d'audit pour les réseaux et pour d'autres gros systèmes peut être sensiblement différente de celle nécessitée pour des systèmes autonomes. Les systèmes plus gros, plus complexes et plus actifs demandent plus de réflexion quand à la collecte des données d'audit et à la façon dont elles devraient être gérées, car il est plus difficile d'interpréter (ou même de stocker) les données collectées. La notion traditionnelle d'une liste triée par ordre chronologique ou "trace" d'évènements audités peut ne pas être applicable pour un réseau global asynchrone où de nombreux évènements arbitraires se produisent au même moment.

547 Ainsi, différents hôtes et serveurs d'une TOE distribuée peuvent avoir des politiques et des valeurs de nommage distinctes. La présentation de noms symboliques pour la revue d'audit peut exiger de disposer d'une convention valable sur l'ensemble du réseau afin d'éviter les redondances et les "conflits de noms".

548 Un répertoire d'audit multi-objets, dont des parties sont accessibles par un ensemble potentiellement important d'utilisateurs autorisés, peut être nécessaire si

les répertoires d'audit doivent être utilisés par une fonction utile dans des systèmes distribués.

549 Enfin, tout abus de pouvoir de la part de l'utilisateur autorisé doit être traité en évitant systématiquement le stockage en local des données d'audit relatives à des actions de l'administrateur.

550 La figure C.1 montre la décomposition de cette classe en ses composants constitutifs.

Classe FAU

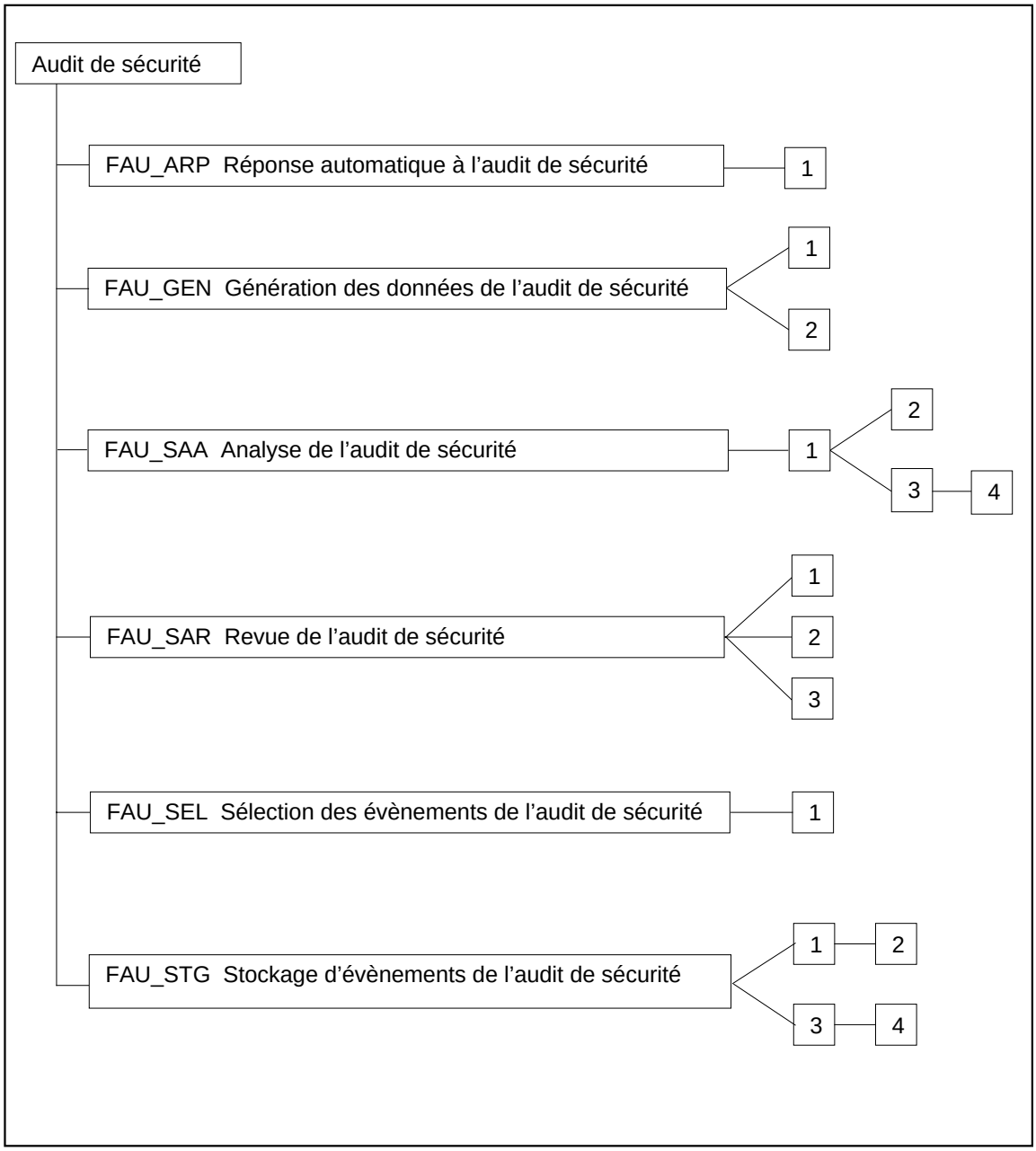


Figure C.1 - Décomposition de la classe "Audit de sécurité"

C.1 Réponse automatique de l'audit de sécurité (FAU_ARP)

551 La famille "Réponse automatique de l'audit de sécurité" décrit les exigences pour la gestion d'évènements d'audit. Celles-ci pourraient inclure des exigences concernant les alarmes ou les actions de la TSF (réponse automatique). Par exemple, la TSF pourrait inclure la génération d'alarmes en temps réel, l'arrêt du processus incriminé, l'interruption d'un service, ou la déconnexion ou l'invalidation d'un compte utilisateur.

Notes d'application

552 Un évènement d'audit est défini comme étant une "violation potentielle de la sécurité" s'il est indiqué comme tel dans les composants de la famille "FAU_SAA".

FAU_ARP.1 Alarmes de sécurité

Notes d'application pour l'utilisateur

553 Une action devrait être entreprise suite à l'apparition d'une alarme. Cette action peut consister à informer l'utilisateur autorisé, lui présenter un ensemble d'actions de barrage possibles, ou à entreprendre des actions correctives. Le minutage des actions devrait être soigneusement considéré par l'auteur du PP ou de la ST.

Opérations

Affectation :

554 **Dans FAU_ARP.1.1, l'auteur du PP ou de la ST devrait spécifier les actions à entreprendre dans le cas d'une violation potentielle de la sécurité. Un exemple d'une telle liste est : "informer l'utilisateur autorisé, invalider le sujet à l'origine de la violation potentielle de la sécurité." Il peut aussi décider que l'action à entreprendre puisse être spécifiée par un utilisateur autorisé.**

C.2 Génération des données de l'audit de sécurité (FAU_GEN)

555 La famille "Génération des données de l'audit de sécurité" contient des exigences pour spécifier les évènements d'audit qui devraient être générés par la TSF pour des évènements touchant à la sécurité.

556 Cette famille est présentée d'une manière qui évite d'imposer une dépendance sur tous les composants nécessitant un support pour l'audit. Chaque composant inclut une section d'audit dans laquelle sont énumérés les évènements à auditer pour ce domaine fonctionnel. Quand l'auteur du PP ou de la ST élabore le PP ou la ST, les éléments du domaine de l'audit sont utilisés pour compléter la variable dans ce composant. Ainsi, la spécification de ce qui pourrait être audité pour un domaine fonctionnel se trouve dans ce domaine fonctionnel.

557 La liste d'évènements auditables dépend entièrement des autres familles fonctionnelles dans le PP ou la ST. La définition de chaque famille devrait par conséquent inclure une liste des évènements auditables spécifiques à la famille. Chaque évènement auditable dans la liste d'évènements auditables spécifiée dans la famille fonctionnelle devrait correspondre à un des niveaux de génération d'évènement d'audit spécifiés dans cette famille (i.e. minimal, élémentaire, détaillé). Ceci procure à l'auteur du PP ou de la ST les informations nécessaires pour garantir que tous les évènements auditables appropriés sont spécifiés dans le PP ou la ST. L'exemple suivant montre comment des évènements auditables doivent être spécifiés dans des familles fonctionnelles appropriées :

558 "Les actions suivantes devraient être auditables dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST :

a) Minimal : utilisation réussie des fonctions d'administration des attributs de sécurité de l'utilisateur ;

b) Elémentaire : toutes les tentatives d'utilisation des fonctions d'administration des attributs de sécurité de l'utilisateur ;

c) Elémentaire : identification des attributs de sécurité de l'utilisateur qui ont été modifiés ;

d) Détaillé : à l'exception d'éléments sensibles spécifiques d'attributs (e.g. mots de passe, clés cryptographiques), les nouvelles valeurs des attributs devraient être enregistrées."

559 Pour chaque composant fonctionnel choisi, les évènements auditables qui sont indiqués dans ce composant, au niveau indiqué dans la famille FAU_GEN et au-dessous, devraient être auditables. Si dans l'exemple précédent 'audit élémentaire' était choisi dans FAU_GEN, les évènements auditables mentionnés dans a), b) et c) devraient être auditables.

560 Il faut observer que la classification d'évènements auditables est hiérarchique. Par exemple, quand la génération d'audit élémentaire est souhaitée, tous les évènements auditables identifiés comme étant classés soit audit minimal soit audit élémentaire devraient également être inclus dans le PP ou la ST en utilisant l'opération d'affectation appropriée, sauf quand l'évènement de niveau plus élevé fournit tout simplement plus de détail que l'évènement de niveau moins élevé. Quand la génération d'audit détaillé est souhaitée, tous les évènements auditables identifiés (audit minimal, audit élémentaire et audit détaillé) devraient être inclus dans le PP ou la ST.

561 Un auteur de PP ou de ST peut décider d'inclure d'autres évènements auditables en plus de ceux exigés pour un niveau d'audit donné. Par exemple, le PP ou la ST peuvent annoncer que seules des capacités d'audit minimal peuvent être annoncées, tout en incluant la plupart des capacités d'audit élémentaire parce que les quelques capacité exclues entrent en conflit avec d'autres contraintes du PP ou de la ST (e.g. parce qu'elles exigent de recueillir des données non disponibles).

Notes d'application

562 La fonctionnalité qui crée l'évènement auditable devrait être spécifiée dans le PP ou ST à titre d'exigence fonctionnelle.

563 Ci-dessous sont présentés des exemples de types d'évènements qui devraient être définis comme étant auditables dans chaque composant fonctionnel de PP ou de ST :

a) Introduction d'objets dans le TSC dans l'espace adresse d'un sujet ;

b) suppression d'objets ;

c) distribution ou révocation de droits ou de capacités d'accès ;

d) modification d'attributs de sécurité d'un sujet ou d'un objet ;

e) vérifications effectuées par la TSF à la suite de la demande d'un sujet ;

f) l'utilisation de droits d'accès pour court-circuiter une vérification ;

g) utilisation de fonctions d'identification et d'authentification ;

h) actions entreprises par un opérateur, ou par un utilisateur autorisé (e.g. suppression d'un mécanisme de protection de la TSF tels que des labels lisibles) ;

i) importation ou exportation de données de ou vers des media amovibles (e.g. listing, bandes magnétiques, disquettes).

FAU_GEN.1 Génération de données d'audit

Notes d'application pour l'utilisateur

564 Ce composant définit les exigences pour identifier les évènements auditables pour lesquels des enregistrements d'audit devraient être générés, et les informations à fournir dans les enregistrements d'audit.

565 FAU_GEN.1 pourrait même être utilisé quand la TSP n'exige pas que les identités d'utilisateurs individuels soient associées aux évènements d'audit. Cela pourrait être approprié quand le PP ou la ST contient également des exigences relatives à la protection de données privées. Si l'identité de l'utilisateur doit être incorporée, FAU_GEN.2 pourrait être utilisé en supplément.

Notes d'application de l'évaluateur

566 Il existe une dépendance sur FPT_STM. Si le fait de disposer de l'heure exacte ne constitue pas un problème pour la TOE concernée, l'élimination de cette dépendance pourrait être justifiée.

Opérations

Sélection :

567 **En utilisant FAU_GEN.1.1b, l'auteur du PP ou de la ST devrait sélectionner le niveau des évènements auditables réclamés dans la section d'audit des autres composants fonctionnels inclus dans le PP ou la ST. Ce niveau pourrait être 'audit minimal', 'audit élémentaire', 'audit détaillé' ou 'non spécifié'. Si 'non spécifié' est sélectionné, l'auteur du PP ou de la ST devrait renseigner tous les évènements auditables souhaités dans FAU_GEN.1.1c, et cette partie de l'élément (article b) peut être entièrement supprimée.**

Affectation :

568 **En utilisant FAU_GEN.1.1c, l'auteur du PP ou de la ST devrait désigner une liste d'autres évènements auditables définis spécifiquement pour être inclus dans la liste des évènements auditables. Ces évènements pourraient être des évènements auditables d'une exigence fonctionnelle qui ont un niveau d'audit supérieur à celui exigé dans FAU_GEN.1.1b, de même que les évènements générés en utilisant une interface de programmation d'application (API).**

569 **En utilisant FAU_GEN.1.2b, l'auteur du PP ou de la ST devrait affecter à chaque évènement auditable inclus dans le PP ou la ST une liste d'autres informations pertinentes pour l'audit à inclure dans les enregistrements d'évènement d'audit.**

FAU_GEN.2 Lien avec l'identité de l'utilisateur

Notes d'application pour l'utilisateur

570 Ce composant couvre l'exigence d'imputabilité d'évènements auditables au niveau de l'identité de l'utilisateur individuel. Ce composant devrait être utilisé en supplément de FAU_GEN.1 Génération de données d'audit.

571 Il existe un conflit potentiel entre les exigences d'audit et de protection de la vie privée. Pour les besoins de l'audit, il peut être souhaitable de connaître la personne qui a effectué une action. L'utilisateur peut vouloir garder ses actions pour lui et ne pas être identifié par d'autres personnes (e.g. un site proposant des offres d'emploi), ou alors la politique de sécurité organisationnelle pourrait exiger que l'identité des utilisateurs doive être protégée. Dans ces cas, les objectives pour l'audit et la protection de la vie privée pourraient être contradictoires. Par conséquent, si cette exigence est sélectionnée et que la protection de la vie privée est importante, l'inclusion du composant d'utilisation de pseudonymes par l'utilisateur pourrait être envisagée. Les exigences pour déterminer le véritable nom de l'utilisateur sur la base de son pseudonyme sont spécifiées dans la classe protection de la vie privée.

C.3 Analyse de l'audit de sécurité (FAU_SAA)

572 La présente famille définit les exigences pour des moyens automatisés qui analysent l'activité du système et les données d'audit à la recherche de violations de la sécurité possibles ou réelles. Cette analyse peut contribuer à la détection d'intrusion, ou à la réponse automatique à une violation imminente de la sécurité.

573 L'action à effectuer par la TSF lors de la détection d'une violation possible imminente ou potentielle est définie dans les composants de la famille "FAU_ARP Réponse automatique de l'audit de sécurité".

Notes d'application

574 Pour une analyse en temps réel, les données d'audit pourraient être transformées dans un format utilisable par un traitement automatisé, et dans un format différent utilisable pour une revue par des utilisateurs autorisés.

FAU_SAA.1 Analyse de violation potentielle

Notes d'application pour l'utilisateur

575 Ce composant est utilisé pour spécifier l'ensemble des évènements auditables dont les apparitions éventuellement cumulées contribuent à indiquer une violation potentielle de la TSP, ainsi que toutes les règles à utiliser pour effectuer l'analyse de la violation de sécurité.

Opérations

Affectation :

576 **En utilisant FAU_SAA.1.2.a, l'auteur du PP ou de la ST devrait identifier le sous-ensemble d'évènements auditables définis dont les apparitions éventuellement cumulées doivent être détectées comme une indication d'une violation potentielle de la TSP.**

577 **En utilisant FAU_SAA.1.2.b, l'auteur du PP ou de la ST devrait spécifier toutes les autres règles que la TSF devrait utiliser dans son analyse de la trace d'audit. Ces règles pourraient inclure des exigences spécifiques pour exprimer la nécessité que les évènements surviennent dans une certain plage de temps (e.g. dans la journée, autre période de temps).**

FAU_SAA.2 Détection d'anomalie basée sur un profil

578 Un *profil* est une structure qui caractérise le comportement d'utilisateurs ou de sujets ; il représente la façon dont les utilisateurs ou les sujets interagissent avec la TSF de différentes manières. Des modèles d'utilisation sont établis en fonction des différents types d'activité dans lesquelles s'engagent les utilisateurs ou les sujets (e.g. modèles d'exceptions soulevées, modèles d'utilisation de ressources (quand, lesquelles, comment), modèles d'actions entreprises). Les façons dans lesquelles

les différents types d'activité sont enregistrés dans le profil (e.g. mesures de ressources, compteurs d'évènements, horloges) sont désignées par le terme *métriques de profil*.

579 Chaque profil représente les modèles attendus d'utilisation de membres du *groupe cible du profil*. Ce modèle peut être basé sur l'utilisation passée (modèles historiques) ou sur l'utilisation normale d'utilisateurs de groupes cibles similaires (comportement attendu). Un groupe cible de profil désigne un ou plusieurs utilisateurs qui interagissent avec la TSF. L'activité de chaque membre du groupe de profil est utilisé par l'outil d'analyse en établissant les modèles d'utilisation représentés dans le profil. Certains exemples de groupes cibles du profil sont donnés ci-dessous :

a) **Compte utilisateur unique** : un profil par utilisateur ;

b) **Identité de groupe (group ID) ou compte de groupe** : un profil pour tous les utilisateurs qui possèdent la même identité de groupe ou travaillent en utilisant le même compte de groupe ;

c) **Rôle opérationnel** : un profil pour tous les utilisateurs partageant un rôle opérationnel donné ;

d) **Système** : un profil pour tous les utilisateurs d'un système.

580 Chaque membre d'un groupe cible du profil se voit attribuer un *indice de représentativité* individuel qui représente le degré d'adéquation de la nouvelle activité du membre avec les modèles d'utilisation établis représentés dans le profil du groupe.

581 La sophistication de l'outil de détection d'anomalie sera largement déterminée par le nombre de groupes cibles associés à un profil exigés par le PP ou la ST et la complexité des métriques de profil exigés.

582 Ce composant est utilisé pour spécifier l'ensemble d'évènements auditables dont l'apparition ou les apparitions successives indiquent une violation potentielle de la TSP, et toutes les règles à utiliser pour effectuer l'analyse de violation. Cet ensemble d'évènements ou de règles pourrait être modifié par l'utilisateur autorisé, par addition, modification ou suppression d'évènements ou de règles.

583 L'auteur du PP ou de la ST devrait énumérer spécifiquement les activités qui devraient être surveillées ou analysées par la TSF. L'auteur du PP ou de la ST devrait également identifier spécifiquement les informations propres à l'activité, nécessaires pour construire les profils d'utilisation.

584 FAU_SAA.2 exige que la TSF maintienne des profils d'utilisation du système. Le terme maintenir implique que le détecteur d'anomalie effectue activement la mise à jour du profil d'utilisation suivant l'activité nouvelle des membres du profil cible. Il est important ici que les métriques représentant l'activité de l'utilisateur soient définies par l'auteur du PP ou de la ST. Par exemple, il peut y avoir un millier d'actions différentes qu'un individu peut être capable d'effectuer, mais le détecteur

d'anomalies peut choisir de ne surveiller qu'un sous-ensemble de cette activité. Une activité anormale est intégrée dans le profil au même titre qu'une activité normale (en supposant que l'outil surveille ces actions). Des choses qui auraient pu apparaître comme anormales quatre mois auparavant pourraient avec le temps devenir la norme (et vice-versa) car les tâches de travail de l'utilisateur changent. La TSF ne pourrait pas saisir cette notion si elle ne filtrait pas les activités anormales par les algorithmes de mise à jour des profils.

585 Une notification administrative devrait être fournie de telle façon que l'utilisateur autorisé comprenne la signification de l'indice de représentativité.

586 L'auteur du PP ou de la ST devrait définir la façon d'interpréter les indices de représentativité et les conditions dans lesquelles une activité anormale est signalée au mécanisme de la famille FAU_ARP.

Opérations

Affectation :

587 **Dans FAU_SAA.2.1, l'auteur du PP ou de la ST devrait spécifier le groupe cible associé à un profil. Un seul PP ou une seule ST peut inclure plusieurs groupes cibles associés à un profil.**

588 **Dans FAU_SAA.2.3, l'auteur du PP ou de la ST devrait spécifier les conditions dans lesquelles une activité anormale est signalée par la TSF. Les conditions peuvent inclure le fait que l'indice de représentativité atteigne une certaine valeur, ou soit basé sur le type d'activité anormale observée.**

FAU_SAA.3 Heuristiques des attaques simples

Notes d'application pour l'utilisateur

589 En pratique, il est rare dans le meilleur des cas qu'un outil d'analyse puisse détecter avec certitude qu'une violation de la sécurité est imminente. Cependant, il existe véritablement certains évènements système qui sont à ce point caractéristiques qu'ils méritent une revue indépendante. De tels évènements comprennent par exemple l'effacement d'un fichier de données de sécurité de la TSF (e.g. le fichier des mots de passe) ou l'activité d'un utilisateur distant essayant d'obtenir un privilège d'administration. Ces évènements sont appelés *évènements caractéristiques* du fait que leur apparition isolée dans l'activité du système est le signe d'une intrusion.

590 La complexité d'un outil donné dépend beaucoup des spécifications définies par l'auteur du PP ou de la ST pour identifier l'ensemble de base des évènements caractéristiques.

591 L'auteur du PP ou de la ST devrait énumérer de façon détaillée les évènements qui devraient être surveillés par la TSF afin d'effectuer l'analyse. L'auteur du PP ou de la ST devrait identifier de façon détaillée les informations associées à l'évènement

qui sont nécessaires pour déterminer si ce dernier correspond à un évènement caractéristique.

592 Une notification administrative devrait être faite de telle façon que l'utilisateur autorisé comprenne la signification de l'évènement et les réponses possibles appropriées.

593 Un effort a été fait dans la spécification de ces exigences pour éviter une dépendance sur les données d'audit comme étant les seules données d'entrée pour surveiller l'activité du système. Ceci a été fait en se rappelant de l'existence d'outils de détection d'intrusion déjà développés qui n'effectuent pas leur analyse de l'activité du système en n'utilisant que les données d'audit (parmi des exemples d'autres données d'entrée, on trouve les datagrammes de réseaux, les données relatives aux ressources ou à la comptabilité ou des combinaisons de diverses données système).

594 Les éléments de FAU_SAA.3 n'exigent pas que la TSF qui implémente les heuristiques d'attaques immédiates soit la même TSF dont l'activité est surveillée. On peut ainsi développer un composant de détection d'intrusion qui opère indépendamment du système dont l'activité est analysée.

Opérations

Affectation :

595 **En utilisant FAU_SAA.3.1, l'auteur du PP ou de la ST devrait identifier un sous-ensemble de base d'évènements système dont les apparitions, en dehors de toute autre activité système, peut indiquer une violation de la TSP. Cela inclut des évènements qui indiquent par eux-mêmes une violation caractérisée de la TSP, ou dont les apparitions sont si caractéristiques qu'elles justifient que des actions soient entreprises.**

596 **Dans FAU_SAA.3.2, l'auteur du PP ou de la ST devrait spécifier les informations utilisées pour déterminer l'activité du système. Ces informations sont constituées par les données d'entrée utilisées par l'outil d'analyse pour déterminer l'activité du système dans la TOE. Ces données peuvent inclure les données d'audit, des combinaisons de données d'audit avec d'autres données système, ou peut consister de données distinctes des données d'audit. L'auteur du PP ou de la ST devrait définir précisément les évènements système et les attributs d'évènements qui sont surveillés dans les données d'entrée.**

FAU_SAA.4 Heuristiques des attaques complexes

Notes d'application pour l'utilisateur

597 En pratique, il est rare dans le meilleur des cas qu'un outil d'analyse puisse détecter avec certitude qu'une violation de la sécurité est imminente. Cependant, il existe véritablement certains évènements système qui sont à ce point caractéristiques qu'ils méritent une revue indépendante. De tels évènements comprennent par

exemple l'effacement d'un fichier de données de sécurité de la TSF (e.g. le fichier des mots de passe) ou l'activité d'un utilisateur distant essayant d'obtenir un privilège d'administration. Ces évènements sont appelés *évènements caractéristiques* du fait que leur apparition isolée dans l'activité du système est le signe d'une intrusion.

598 La complexité d'un outil donné dépend beaucoup des spécifications définies par l'auteur du PP ou de la ST pour identifier l'ensemble de base des évènements caractéristiques.

599 L'auteur du PP ou de la ST devrait définir un ensemble de base d'évènements caractéristiques et des suites d'évènements pour être représentés par la TSF. Des évènements caractéristiques supplémentaires et des suites d'évènements peuvent être définis par le développeur du système.

600 L'auteur du PP ou de la ST devrait énumérer de façon détaillée les évènements qui devraient être surveillés par la TSF afin d'effectuer l'analyse. L'auteur du PP ou de la ST devrait identifier de façon détaillée les informations associées à l'évènement qui sont nécessaires pour déterminer si ce dernier correspond à un évènement caractéristique.

601 Une notification administrative devrait être faite de telle façon que l'utilisateur autorisé comprenne la signification de l'évènement et les réponses possibles appropriées.

602 Un effort a été fait dans la spécification de ces exigences pour éviter une dépendance sur les données d'audit comme étant les seules données d'entrée pour surveiller l'activité du système. Ceci a été fait en se rappelant de l'existence d'outils de détection d'intrusion déjà développés qui n'effectuent pas leur analyse de l'activité du système en n'utilisant que les données d'audit (parmi des exemples d'autres données d'entrée, on trouve les datagrammes de réseaux, les données relatives aux ressources ou à la comptabilité ou des combinaisons de diverses données système).

603 Les éléments de FAU_SAA.4 n'exigent pas que la TSF qui implémente les heuristiques d'attaques immédiates soit la même TSF dont l'activité est surveillée. On peut ainsi développer un composant de détection d'intrusion qui opère indépendamment du système dont l'activité est analysée.

Opérations

Affectation :

604 **En utilisant FAU_SAA.4.1, l'auteur du PP ou de la ST devrait identifier un ensemble de base de listes de suites d'évènements système dont les apparitions sont représentatives de scénarios de pénétration connus. Ces suites d'évènements représentent des scénarios de pénétration connus. Chaque évènement représenté dans la suite devrait correspondre à un évènement système surveillé, de telle façon que**

lorsque les évènements système surviennent, ils soient reliés aux suites d'évènements connues caractéristiques de scénarios de pénétration.

605 En utilisant FAU_SAA.4.1, l'auteur du PP ou de la ST devrait identifier un sous-ensemble de base d'évènements système dont les apparitions, en dehors de toute autre activité système, peut indiquer une violation de la TSP. Cela inclut des évènements qui indiquent par eux-mêmes une violation caractérisée de la TSP, ou dont les apparitions sont si caractéristiques qu'elles justifient que des actions soient entreprises.

606 Dans FAU_SAA.4.2, l'auteur du PP ou de la ST devrait spécifier les informations utilisées pour déterminer l'activité du système. Ces informations sont constituées par les données d'entrée utilisées par l'outil d'analyse pour déterminer l'activité du système dans la TOE. Ces données peuvent inclure les données d'audit, des combinaisons de données d'audit avec d'autres données système, ou peut consister de données distinctes des données d'audit. L'auteur du PP ou de la ST devrait définir précisément les évènements système et les attributs d'évènements qui sont surveillés dans les données d'entrée.

C.4 Revue de l'audit de sécurité (FAU_SAR)

607 La famille "Revue de l'audit de sécurité" définit les exigences relatives à la revue d'informations d'audit.

608 Ces fonctions devraient permettre une sélection d'audit avant ou après le stockage qui inclut par exemple la possibilité de revoir sélectivement :

- les actions d'un ou de plusieurs utilisateurs (e.g. identification, authentification, entrée dans la TOE et actions de contrôle d'accès) ;
- les actions effectuées sur un objet spécifique ou une ressource de la TOE ;
- toutes les exceptions d'un ensemble spécifié d'exceptions auditées ;
- ou les actions associées à un attribut spécifique de la TSP.

Notes d'application

609 La différence entre revues d'audit est due aux fonctionnalités. La revue d'audit comprend (seulement) la possibilité de visualiser les données d'audit. La revue sélective est plus sophistiquée et exige la possibilité d'effectuer des recherches en fonction d'un seul critère ou de plusieurs critères liés par des relations logiques (i.e. des ou et des et), de trier les données d'audit, de filtrer les données d'audit avant leur revue.

FAU_SAR.1 Revue d'audit

Notes d'application pour l'utilisateur

610 Ce composant est utilisé pour spécifier que des utilisateurs ou des utilisateurs autorisés peuvent lire les enregistrements d'audit. Ces enregistrements d'audit seront fournis à l'utilisateur d'une manière appropriée. Il existe différents types d'utilisateurs (des utilisateurs humains, des machines) qui pourraient avoir des besoins différents.

611 Le contenu des enregistrements d'audit qui peuvent être visualisés peut être spécifié.

Opérations

Affectation :

612 **Dans FAU_SAR.1.1, l'auteur du PP ou de la ST devrait spécifier les utilisateurs autorisés qui peuvent utiliser cette possibilité. Si cela est approprié l'auteur du PP ou de la ST peut inclure des rôles de sécurité (voir FMT_SMR.1 Rôles de sécurité).**

613 **Dans FAU_SAR.1.1, l'auteur du PP ou de la ST devrait spécifier le type d'informations que l'utilisateur spécifié a le droit d'obtenir à partir des enregistrements d'audit. On peut citer comme exemples "tout type", "identité des sujets", "toutes les informations des enregistrements d'audit se rapportant à cet utilisateur".**

FAU_SAR.2 Revue d'audit restreinte

Notes d'application pour l'utilisateur

614 Ce composant spécifie que tout utilisateur non identifié dans FAU_SAR.1 ne pourra pas lire les enregistrements d'audit.

FAU_SAR.3 Revue d'audit sélective

Notes d'application pour l'utilisateur

615 Ce composant est utilisé pour spécifier qu'il devrait être possible d'effectuer une sélection des données d'audit pour être revues. Si elle est basée sur plusieurs critères, ces critères devraient être liés par des relations logiques (i.e. 'et' ou 'ou') et les outils devraient offrir la possibilité de manipuler les données d'audit (e.g. trier, filtrer).

Opérations

Sélection :

616 **En utilisant FAU_SAR.3.1, l'auteur du PP ou de la ST devrait décider si des recherches, des tris ou des ordonnancements peuvent être effectués par la TSF.**

Affectation :

617 **En utilisant FAU_SAR.3.1, l'auteur du PP ou de la ST devrait désigner les critères, éventuellement liés par des relations logiques, à utiliser pour sélectionner les données d'audit à des fins de revue. Les relations logiques sont destinées à spécifier si l'opération peut être effectuée sur un attribut individuel ou sur une collection d'attributs. Un exemple d'affectation pourrait être : "application, compte utilisateur ou lieu". Dans ce cas l'opération pourrait être spécifiée en utilisant toute combinaison des trois attributs : application, compte utilisateur et lieu.**

C.5 Sélection des évènements de l'audit de sécurité (FAU_SEL)

618 La famille "Sélection des évènements de l'audit de sécurité" fournit des exigences relatives aux possibilités d'identifier lesquels des évènements auditables possibles doivent être audités. Les évènements auditables sont définis dans la famille "FAU_GEN Génération des données de l'audit de sécurité", mais ces évènements devraient être définis comme pouvant être sélectionnés dans ce composant pour être audités.

Notes d'application

619 Cette famille garantit qu'il est possible d'empêcher la trace d'audit de devenir si volumineuse qu'elle en devient inutile en définissant la granularité appropriée pour les évènements de l'audit de sécurité sélectionnés.

FAU_SEL.1 Audit sélectif

Notes d'application pour l'utilisateur

620 Ce composant définit les critères utilisés pour la sélection d'évènements pour être audités. Ces critères pourraient permettre d'inclure ou d'exclure des évènements de l'ensemble des évènements auditables, en fonction des attributs de l'utilisateur, des attributs du sujet, des attributs de l'objet ou de types d'évènements.

621 L'existence d'une identité attachée à un utilisateur individuel n'est pas supposée dans ce composant. Ceci permet de considérer des TOE telles que des routeurs qui peuvent ne pas supporter la notion d'utilisateurs.

622 Pour un environnement distribué, l'identité de l'hôte pourrait être utilisée comme critère de sélection pour auditer des évènements.

623 La fonction d'administration "FMT_MTD.1 Administration des données de la TSF" prendra en charge les droits des utilisateurs autorisés à effectuer des requêtes ou à modifier les sélections.

Opérations

Sélection :

624 **En utilisant FAU_SEL.1.1a, l'auteur du PP ou de la ST devrait décider si les attributs de sécurité sur lesquels la sélectivité de l'audit est basée sont liés à l'identité de l'objet, à l'identité de l'utilisateur, à l'identité du sujet, à l'identité de l'hôte, ou à un type d'évènement.**

Affectation :

625 **En utilisant FAU_SEL.1.1b, l'auteur du PP ou de la ST devrait spécifier tous les attributs supplémentaires sur lesquels la sélectivité de l'audit est basée.**

C.6 Stockage d'évènements de l'audit de sécurité (FAU_STG)

626 La famille "Stockage d'évènements de l'audit de sécurité" décrit des exigences pour stocker les données d'audit pour une utilisation ultérieure, incluant des exigences pour contrôler la perte d'informations de l'audit due à une défaillance du système, à une attaque ou à l'épuisement d'espace de stockage.

FAU_STG.1 Stockage protégé de la trace d'audit

Notes d'application pour l'utilisateur

627 Dans un environnement distribué, comme la trace d'audit est située dans le TSC mais n'est pas nécessairement située au même endroit que la fonction qui génère les données d'audit, l'auteur du PP ou de la ST pourrait exiger l'authentification de l'auteur de l'enregistrement d'audit, ou la non-répudiation de la source de l'enregistrement avant de stocker cet enregistrement dans la trace d'audit.

628 La TSF protégera la trace d'audit d'une suppression et d'une modification non autorisée. Il est à noter que dans certains systèmes l'auditeur (rôle) pourrait ne pas être autorisé à supprimer les enregistrements d'audit pendant un certain temps.

Opérations

Sélection :

629 **Dans FAU_STG.1.2, l'auteur du PP ou de la ST devrait spécifier si la TSF doit empêcher ou seulement être capable de détecter des modifications de la trace d'audit.**

FAU_STG.2 Garanties de disponibilité des données d'audit

Notes d'application pour l'utilisateur

630 Ce composant permet à l'auteur du PP ou de la ST de spécifier les métriques auxquelles la trace d'audit devrait se conformer.

631 Dans un environnement distribué, comme la trace d'audit est située dans le TSC mais n'est pas nécessairement située au même endroit que la fonction qui génère les données d'audit, l'auteur du PP ou de la ST pourrait exiger l'authentification de l'émetteur de l'enregistrement d'audit, ou la non-répudiation de l'origine de la source de l'enregistrement avant de stocker cet enregistrement dans la trace d'audit.

Opérations

Sélection :

632 Dans FAU_STG.2.2, l'auteur du PP ou de la ST devrait spécifier si la TSF doit empêcher ou seulement être capable de détecter des modifications de la trace d'audit.

633 **Dans FAU_STG.2.3, l'auteur du PP ou de la ST devrait spécifier la condition sous laquelle la TSF doit encore être capable de maintenir une quantité définie de données d'audit. Cette condition peut être une des suivantes : épuisement de l'espace de stockage de l'audit, défaillance, attaque.**

Affectation :

634 **Dans FAU_STG.2.3, l'auteur du PP ou de la ST devrait spécifier la métrique que la TSF doit garantir par rapport à la trace d'audit. Cette métrique limite les pertes de données en comptant le nombre d'enregistrements qui doivent être conservés, ou la durée pendant laquelle les enregistrements ont la garantie d'être conservés. Un exemple de métrique pourrait être "100 000" indiquant que 100 000 enregistrements d'audit peuvent être stockés.**

FAU_STG.3 Action en cas de perte possible de données d'audit

Notes d'application pour l'utilisateur

635 Ce composant exige que des actions soient entreprises quand la trace d'audit dépasse certaines limites pré-définies.

Opérations

Affectation :

636 **Dans FAU_STG.3.1, l'auteur du PP ou de la ST devrait indiquer la limite pré-définie. Si les fonctions d'administration indiquent que ce nombre pourrait être changé par l'utilisateur autorisé, cette valeur est alors la valeur par défaut. L'auteur du PP ou de la ST pourrait choisir de laisser l'utilisateur autorisé définir cette limite. Dans ce cas l'affectation peut être par exemple "un utilisateur autorisé fixe la limite".**

637 **Dans FAU_STG.3.1, l'auteur du PP ou de la ST devrait spécifier les actions qui devraient être entreprises dans le cas d'une défaillance imminente dans le stockage des données d'audit, indiquée par dépassement du seuil. Les actions pourraient inclure l'information d'un utilisateur autorisé.**

FAU_STG.4 Prévention des pertes de données d'audit

Notes d'application pour l'utilisateur

638 Ce composant spécifie le comportement de la TOE dans le cas où la trace d'audit est pleine : soit des enregistrements d'audit sont ignorés, soit la TOE est gelée de telle façon qu'aucun évènement auditable ne puisse plus se produire. L'exigence stipule aussi que, quelle que soit la façon dont l'exigence est instanciée, l'utilisateur autorisé muni des droits spécifiques à cet effet puisse continuer à générer des évènements auditables (actions). La raison en est que, dans le cas contraire, l'utilisateur autorisé ne pourrait même pas redémarrer le système. Le choix de l'action à entreprendre par la TSF devrait être pris en compte dans le cas de l'épuisement de l'espace de stockage de l'audit, par exemple d'ignorer des évènements, ce qui offre une meilleure disponibilité de la TOE et qui permet l'exécution d'actions sans qu'elles soient enregistrées et sans que l'utilisateur n'en soit tenu pour responsable.

Opérations

Sélection :

639 **Dans FAU_STG.4.1, l'auteur du PP ou de la ST devrait décider si la TSF doit ignorer des actions auditables ou si elle devrait empêcher les actions auditables de se produire, ou encore si les enregistrements d'audit les plus anciens devraient être écrasés quand la TSF ne peut plus stocker les enregistrements d'audit.**

Affectation :

640 **Dans FAU_STG.4.1, l'auteur du PP ou de la ST devrait spécifier les autres actions qui devraient être entreprises dans le cas d'une défaillance dans le stockage des données d'audit, comme par exemple d'informer l'utilisateur autorisé.**

Annexe D
(Informative)

Communication (FCO)

641 Cette classe décrit les exigences qui intéressent spécifiquement les TOE utilisées pour le transport des informations. Les familles de cette classe traitent de la non-répudiation.

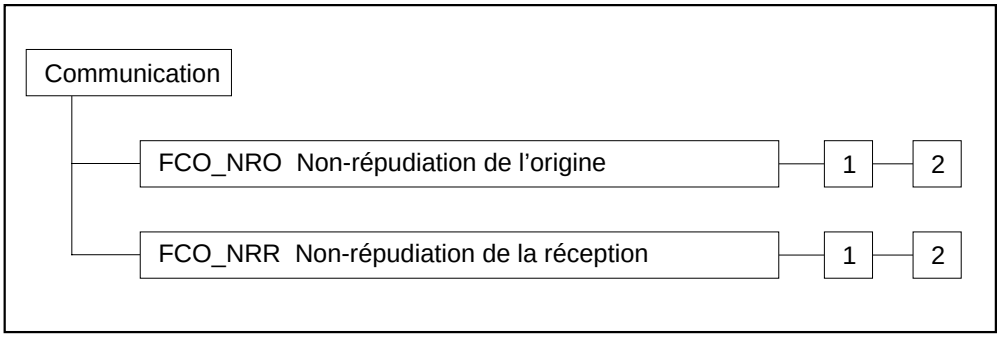


Figure D.1 - Décomposition de la classe "Communication"

642 La figure D.1 montre la décomposition de la présente classe en ses composants constitutifs.

643 Dans cette classe le concept d'"informations" est utilisé. Ces informations devraient être interprétées comme étant l'objet envoyé, et pourraient être constituées d'un message électronique, d'un fichier, ou d'un ensemble de types d'attributs prédéfinis.

644 Dans la littérature, les termes 'preuve de la réception' et 'preuve de l'origine' sont des termes couramment utilisés. Cependant il est reconnu que le terme 'preuve' pourrait être interprété dans un sens juridique qui impliquerait une forme de justification mathématique. Les composants de cette classe considèrent que l'utilisation de facto du mot 'preuve' se place dans le contexte de la 'preuve' que la TSF démontre que le transfert de types d'informations ne peut pas être répudié.

D.1 Non-répudiation de l'origine (FCO_NRO)

645 La non-répudiation de l'origine définit les exigences pour fournir des éléments de preuve aux utilisateurs ou aux sujets concernant l'identité de l'émetteur d'informations. L'émetteur ne peut pas nier avec succès avoir envoyé les informations car les éléments de preuve de l'origine (e.g. une signature numérique) constituent une preuve du lien entre l'émetteur et les informations envoyées. Le destinataire ou une tierce partie peut vérifier les éléments de preuve de l'origine. Ces éléments de preuve ne devraient pas être falsifiables.

Notes pour l'utilisateur

646 Si les informations ou les attributs qui y sont associés sont altérés de quelque façon que ce soit, la validation des éléments de preuve de l'origine pourrait échouer. Par conséquent, un auteur de PP ou de ST devrait penser à inclure dans le PP ou la ST des exigences relatives à l'intégrité telles que celles contenues dans le composant "FDP_UIT.1 Intégrité lors d'un échange de données".

647 Dans la non-répudiation, plusieurs rôles distincts sont impliqués, chacun d'entre eux pouvant être combiné à un ou plusieurs sujets. Le premier rôle est celui d'un sujet qui demande des éléments de preuve de l'origine (seulement dans le composant "FCO_NRO.1 Preuve sélective de l'origine"). Le deuxième rôle est celui du destinataire ou d'autres sujets auxquels des éléments de preuve sont fournis (e.g. un notaire). Le troisième rôle est celui d'un sujet qui demande la vérification des éléments de preuve de l'origine, par exemple un destinataire ou une tierce partie telle qu'un arbitre.

648 L'auteur du PP ou de la ST doit spécifier les conditions qui doivent être satisfaites pour être capable de vérifier la validité des éléments de preuve. Un exemple de condition qui pourrait être spécifiée est d'exiger que la vérification des éléments de preuve aie lieu dans les 24 heures. Ces conditions permettent par conséquent d'adapter la non-répudiation à des exigences légales, telles que le fait d'être capable de fournir des éléments de preuve couvrant plusieurs années.

649 Dans la plupart des cas, l'identité du destinataire est l'identité de l'utilisateur qui reçoit la transmission. Dans certaines occasions, l'auteur du PP ou de la ST ne veut pas que l'identité de l'utilisateur soit exportée. Dans ce cas l'auteur du PP ou de la ST doit considérer si le fait d'inclure cette classe est approprié, ou si l'identité du fournisseur du service de transport ou l'identité de l'hôte devrait être utilisée.

650 Outre (ou au lieu de) l'identité de l'utilisateur, un auteur de PP ou de ST pourrait se préoccuper de la date à laquelle les informations ont été transmises. Par exemple, des demandes de propositions doivent être transmises avant une certaine date afin d'être prises en compte. Dans de telles occasions, ces exigences peuvent être adaptées pour fournir un horodatage (date de l'origine).

FCO_NRO.1 Preuve sélective de l'origine

Opérations

Affectation :

651 **Dans FCO_NRO.1.1, l'auteur du PP ou de la ST devrait renseigner les types d'informations, tels que par exemple des messages électroniques, qui sont soumis à la fonction chargée de produire des éléments de preuve de l'origine.**

Sélection :

652 **Dans FCO_NRO.1.1, l'auteur du PP ou de la ST devrait spécifier l'utilisateur ou le sujet qui peut demander des éléments de preuve de l'origine.**

Affectation :

653 **Dans FCO_NRO.1.1, l'auteur du PP ou de la ST, en fonction de la sélection, devrait spécifier les tierces parties qui peuvent demander des éléments de preuve de la réception. Une tierce partie pourrait être un arbitre, un juge ou une organisation juridique.**

654 **Dans FCO_NRO.1.2, l'auteur du PP ou de la ST devrait renseigner la liste des attributs qui doivent être associés aux informations, comme par exemple l'identité de l'émetteur, la date de l'envoi, et le lieu de l'envoi.**

655 **Dans FCO_NRO.1.2, l'auteur du PP ou de la ST devrait renseigner la liste des champs d'information dans les informations avec lesquelles les attributs fournissent des éléments de preuve de l'origine, telles que le corps d'un message.**

Sélection :

656 **Dans FCO_NRO.1.3, l'auteur du PP ou de la ST devrait spécifier l'utilisateur ou le sujet qui peut vérifier les éléments de preuve de l'origine.**

Affectation :

657 **Dans FCO_NRO.1.3, l'auteur du PP ou de la ST, en fonction de la sélection, devrait spécifier les tierces parties qui peuvent vérifier les éléments de preuve de l'origine.**

658 **Dans FCO_NRO.1.3, l'auteur du PP ou de la ST devrait renseigner la liste des limitations à prendre en compte pour pouvoir vérifier les éléments de preuve : par exemple, les éléments de preuve peuvent seulement être vérifiés à des intervalles de 24 heures. Une affectation telle que 'immédiatement' ou 'dans un délai indéfini' est acceptable.**

FCO_NRO.2 Preuve systématique de l'origine

Opérations

Affectation :

659 Dans FCO_NRO.2.1, l'auteur du PP ou de la ST devrait renseigner les types d'informations, par exemple des messages électroniques, qui sont soumis à la fonction chargée de produire des éléments de preuve de l'origine.

660 Dans FCO_NRO.2.2, l'auteur du PP ou de la ST devrait renseigner la liste des attributs qui devraient être associés aux informations, comme par exemple l'identité de l'émetteur, la date de l'envoi, et le lieu de l'envoi.

661 Dans FCO_NRO.2.2, l'auteur du PP ou de la ST devrait renseigner la liste des champs d'information dans les informations avec lesquelles les attributs fournissent des éléments de preuve de l'origine, telles que le corps d'un message.

Sélection :

662 Dans FCO_NRO.2.3, l'auteur du PP ou de la ST devrait spécifier l'utilisateur ou le sujet qui peut vérifier les éléments de preuve de l'origine.

Affectation :

663 Dans FCO_NRO.2.3, l'auteur du PP ou de la ST, en fonction de la sélection, devrait spécifier les tierces parties qui peuvent vérifier les éléments de preuve de la réception. Une tierce partie pourrait être un arbitre, un juge ou une organisation juridique.

664 Dans FCO_NRO.2.3, l'auteur du PP ou de la ST devrait renseigner la liste des limitations à prendre en compte pour pouvoir vérifier les éléments de preuve : par exemple, les éléments de preuve peuvent seulement être vérifiés à des intervalles de 24 heures. Une affectation telle que 'immédiatement' ou 'dans un délai indéfini' est acceptable.

D.2 Non-répudiation de la réception (FCO_NRR)

665 La non-répudiation de la réception définit les exigences pour fournir des éléments de preuve aux utilisateurs ou aux sujets montrant que le destinataire a reçu les informations. Le destinataire ne peut pas nier avec succès avoir reçu les informations car les éléments de preuve de la réception (e.g. une signature numérique) constituent une preuve du lien entre le destinataire et les informations. L'émetteur ou une tierce partie peut vérifier les éléments de preuve de la réception. Ces éléments de preuve ne devraient pas être falsifiables.

Notes pour l'utilisateur

666 Il devrait être noté que la fourniture des éléments de preuve de la réception des informations n'implique pas nécessairement que les informations ont été lues ou comprises, mais seulement délivrées.

667 Si les informations ou les attributs qui y sont associés sont altérés de quelque façon que ce soit, la validation des éléments de preuve de la réception par rapport aux informations d'origine pourrait échouer. Par conséquent, un auteur de PP ou de ST devrait penser à inclure dans le PP ou la ST des exigences relatives à l'intégrité telles que celles contenues dans le composant "FDP_UIT.1 Intégrité lors d'un échange de données".

668 Dans la non-répudiation, plusieurs rôles distincts sont impliqués, chacun d'entre eux pouvant être combiné à un ou plusieurs sujets. Le premier rôle est celui d'un sujet qui demande des éléments de preuve de la réception (seulement dans le composant "FCO_NRR.1 Preuve sélective de la réception"). Le deuxième rôle est celui du destinataire ou d'autres sujets auxquels des éléments de preuve sont fournis (e.g. un notaire). Le troisième rôle est celui d'un sujet qui demande la vérification des éléments de preuve de la réception, par exemple un émetteur d'informations ou une tierce partie telle qu'un arbitre.

669 L'auteur du PP ou de la ST doit spécifier les conditions qui doivent être satisfaites pour être capable de vérifier la validité des éléments de preuve. Un exemple de condition qui pourrait être spécifiée est d'exiger que la vérification des éléments de preuve aie lieu dans les 24 heures. Ces conditions permettent par conséquent d'adapter la non-répudiation à des exigences légales, telles que le fait d'être capable de fournir des éléments de preuve couvrant plusieurs années.

670 Dans la plupart des cas, l'identité du destinataire est l'identité de l'utilisateur qui reçoit la transmission. Dans certaines occasions, l'auteur du PP ou de la ST ne veut pas que l'identité de l'utilisateur soit exportée. Dans ce cas l'auteur du PP ou de la ST doit considérer si le fait d'inclure cette classe est approprié, ou si l'identité du fournisseur du service de transport ou l'identité de l'hôte devrait être utilisée.

671 Outre (ou au lieu de) l'identité de l'utilisateur, un auteur de PP ou de ST pourrait se préoccuper plus de la date à laquelle les informations ont été reçues. Par exemple, quand une offre n'est plus valable après une certaine date, les commandes doivent être reçues avant cette date afin d'être prises en compte. Dans de telles occasions,

ces exigences peuvent être adaptées pour fournir un horodatage (date de la réception).

FCO_NRR.1 Preuve sélective de la réception

Opérations

Affectation :

672 **Dans FCO_NRR.1.1, l'auteur du PP ou de la ST devrait renseigner les types d'informations, tels que par exemple des messages électroniques, qui sont soumis à la fonction chargée de produire des éléments de preuve de la réception.**

Sélection :

673 **Dans FCO_NRR.1.1, l'auteur du PP ou de la ST devrait spécifier l'utilisateur ou le sujet qui peut demander des éléments de preuve de la réception.**

Affectation :

674 **Dans FCO_NRR.1.1, l'auteur du PP ou de la ST, en fonction de la sélection, devrait spécifier les tierces parties qui peuvent demander des éléments de preuve de la réception. Une tierce partie pourrait être un arbitre, un juge ou une organisation juridique.**

675 **Dans FCO_NRR.1.2, l'auteur du PP ou de la ST devrait renseigner la liste des attributs qui doivent être associés aux informations, comme par exemple l'identité du destinataire, la date de la réception, et le lieu de la réception.**

676 **Dans FCO_NRR.1.2, l'auteur du PP ou de la ST devrait renseigner la liste des champs d'information dans les informations avec lesquelles les attributs fournissent des éléments de preuve de la réception, telles que le corps d'un message.**

Sélection :

677 **Dans FCO_NRR.1.3, l'auteur du PP ou de la ST devrait spécifier l'utilisateur ou le sujet qui peut vérifier les éléments de preuve de la réception.**

Affectation :

678 **Dans FCO_NRR.1.3, l'auteur du PP ou de la ST, en fonction de la sélection, devrait spécifier les tierces parties qui peuvent vérifier les éléments de preuve de la réception.**

679 **Dans FCO_NRR.1.3, l'auteur du PP ou de la ST devrait renseigner la liste des limitations à prendre en compte pour pouvoir vérifier les éléments de preuve : par exemple, les éléments de preuve peuvent**

seulement être vérifiés à des intervalles de 24 heures. Une affectation telle que ‘immédiatement’ ou ‘dans un délai indéfini’ est acceptable.

FCO_NRR.2 Preuve systématique de la réception

Opérations

Affectation :

680 Dans FCO_NRR.2.1, l’auteur du PP ou de la ST devrait renseigner les types d’informations, tels par exemple que des messages électroniques, qui sont soumis à la fonction chargée de produire des éléments de preuve de la réception.

681 Dans FCO_NRR.2.2, l’auteur du PP ou de la ST devrait renseigner la liste des attributs qui doivent être associés aux informations, comme par exemple l’identité du destinataire, la date de la réception, et le lieu de la réception.

682 Dans FCO_NRR.2.2, l’auteur du PP ou de la ST devrait renseigner la liste des champs d’information dans les informations avec lesquelles les attributs fournissent des éléments de preuve de la réception, telles que le corps d’un message.

Sélection :

683 Dans FCO_NRR.2.3, l’auteur du PP ou de la ST devrait spécifier l’utilisateur ou le sujet qui peut vérifier les éléments de preuve de la réception.

Affectation :

684 Dans FCO_NRR.2.3, l’auteur du PP ou de la ST, en fonction de la sélection, devrait spécifier les tierces parties qui peuvent vérifier les éléments de preuve de la réception. Une tierce partie pourrait être un arbitre, un juge ou une organisation juridique.

685 Dans FCO_NRR.2.3, l’auteur du PP ou de la ST devrait renseigner la liste des limitations à prendre en compte pour pouvoir vérifier les éléments de preuve : par exemple, les éléments de preuve peuvent seulement être vérifiés à des intervalles de 24 heures. Une affectation telle que ‘immédiatement’ ou ‘dans un délai indéfini’ est acceptable.

Annexe E
(Informative)

Support cryptographique (FCS)

686 La TSF peut utiliser des fonctionnalités cryptographiques pour contribuer à satisfaire à plusieurs objectifs de sécurité de haut niveau. Ces derniers comprennent entre autres : l'identification et l'authentification, la non-répudiation, le chemin de confiance, le canal de confiance et la séparation des données. La présente classe est utilisée dans le cas où la TOE implémente des fonctions cryptographiques dans du matériel, des micro-programmes ou du logiciel.

687 La classe FCS est composée de deux familles : "FCS_CKM Gestion de clés cryptographiques" et "FCS_COP Opération cryptographique". La famille FCS_CKM traite des aspects de la gestion de clés cryptographiques, tandis que la famille FCS_COP concerne l'utilisation opérationnelle des clés cryptographiques.

688 Fig. E.1 montre la décomposition de cette classe dans ses composants constitutifs.

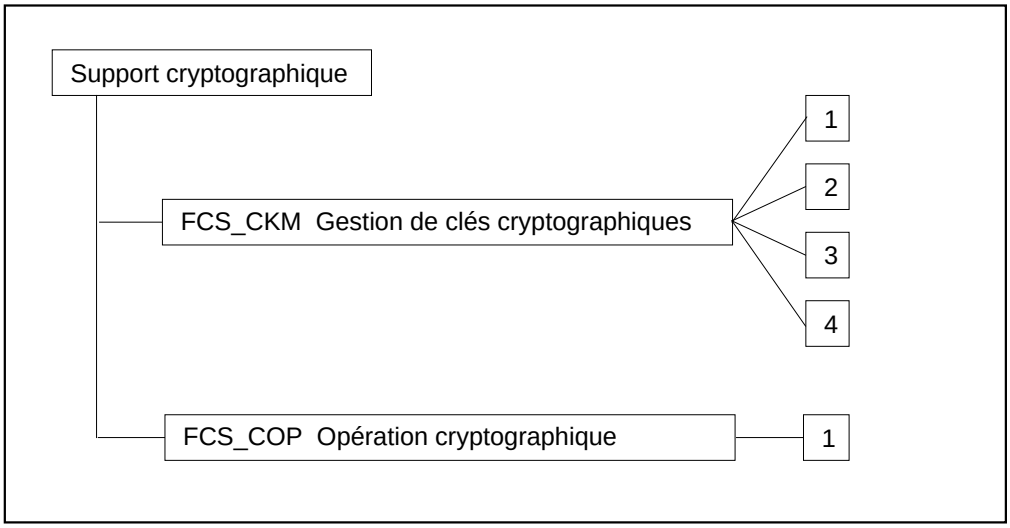


Figure E.1 - Décomposition de la classe "Support cryptographique"

689 Pour chaque méthode de génération de clés cryptographiques implémentée par la TOE, le cas échéant, l'auteur du PP ou de la ST devrait sélectionner le composant FCS_CKM.1.

690 Pour chaque méthode de distribution de clés cryptographiques implémentée par la TOE, le cas échéant, l'auteur du PP ou de la ST devrait sélectionner le composant FCS_CKM.2.

691 Pour chaque méthode de contrôle d'accès aux clés cryptographiques implémentée par la TOE, le cas échéant, l'auteur du PP ou de la ST devrait sélectionner le composant FCS_CKM.3.

692 Pour chaque méthode de destruction de clés cryptographiques implémentée par la TOE, le cas échéant, l'auteur du PP ou de la ST devrait sélectionner le composant FCS_CKM.4.

693 Pour chaque opération cryptographique (telle que la signature numérique, le chiffrement de données, la négociation de clés, le hachage sécurisé, etc.) réalisée par la TOE, le cas échéant l'auteur du PP ou de la ST devrait sélectionner le composant FCS_COP.1.

694 Une fonctionnalité cryptographique peut être utilisée pour satisfaire aux objectifs spécifiés dans la classe FCO et dans les familles FDP_DAU, FDP_SDI, FDP_UCT, FDP_UIT, FIA_SOS, FIA_UAU pour satisfaire à différents objectifs. Dans les cas où une fonctionnalité cryptographique est utilisée pour satisfaire à des objectifs d'autres classes, les composants fonctionnels individuels spécifient les objectifs que la fonctionnalité cryptographique doit satisfaire. Les objectifs de la classe FCS devraient être utilisés quand une fonctionnalité cryptographique de la TOE est recherchée par des utilisateurs.

E.1 Gestion de clés cryptographiques (FCS_CKM)

Notes pour l'utilisateur

695 Les clés cryptographiques doivent être gérées tout au long de leur durée de vie. Les événements typiques du cycle de vie d'une clé cryptographique comprennent entre autres : la génération, la distribution, la mise à la clé, le stockage, l'accès (e.g. sauvegarde, notarisation, archivage, recouvrement) et la destruction.

696 Au minimum, les clés cryptographiques devraient passer par les étapes suivantes : génération, stockage et destruction. Le passage par d'autres étapes dépend de la stratégie de gestion des clés qui est implémentée, la TOE ne devant pas forcément être impliquée pour l'ensemble du cycle de vie des clés (e.g. la TOE peut seulement générer et distribuer des clés cryptographiques).

697 Cette famille est prévue pour supporter le cycle de vie d'une clé cryptographique et définit en conséquence des exigences pour les activités suivantes : génération de clés cryptographiques, distribution de clés cryptographiques, accès aux clés cryptographiques et destruction de clés cryptographiques. Cette famille devrait être incluse chaque fois qu'il existe des exigences fonctionnelles pour la gestion des clés cryptographiques.

698 Dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST, en ce qui concerne les événements audités :

a) Les attributs de l'objet peuvent inclure l'utilisateur spécifié de la clé cryptographique, le rôle de l'utilisateur, l'opération cryptographique pour laquelle la clé cryptographique doit être utilisée, l'identifiant de la clé cryptographique et la période de validité de la clé cryptographique.

b) La valeur de l'objet peut inclure les valeurs de la clé ou des clés cryptographique(s) et les paramètres **à l'exclusion** de toute information sensible (telles que des clés cryptographiques secrètes ou privées).

699 Des nombres aléatoires sont utilisés typiquement pour générer des clés cryptographiques. Si c'est le cas, alors le composant "FCS_CKM.1 Génération de clés cryptographiques" devrait être utilisé à la place du composant "FIA_SOS.2 Génération de secrets par la TSF". Dans les cas où une génération de nombres aléatoires est nécessaire pour d'autres buts que pour la génération des clés cryptographiques, le composant "FIA_SOS.2 Génération de secrets par la TSF" devrait être utilisé.

FCS_CKM.1 Génération de clés cryptographiques

Notes d'application pour l'utilisateur

700 Ce composant exige que les tailles des clés cryptographiques et la méthode utilisée pour générer des clés cryptographiques soient spécifiées, ce qui peut être fait par référence à une norme désignée. Il devrait être utilisé pour spécifier les tailles des

clés cryptographiques et la méthode (e.g. l'algorithme) utilisées pour générer les clés cryptographiques. Le composant n'a besoin d'être appliqué qu'une seule fois dans le cas où la même méthode est utilisée pour plusieurs tailles de clé. La taille de clé pourrait être la même ou être différente pour les différentes entités, et pourrait constituer la valeur d'entrée ou bien la valeur en sortie de la méthode.

Opérations

Affectation :

701 **Dans FCS_CKM.1.1, l'auteur du PP ou de la ST devrait spécifier l'algorithme de génération de clés cryptographiques à utiliser.**

702 **Dans FCS_CKM.1.1, l'auteur du PP ou de la ST devrait spécifier les tailles des clés cryptographiques à utiliser. Les tailles des clés spécifiées devraient être appropriées pour l'algorithme dans le cadre de l'utilisation prévue.**

703 **Dans FCS_CKM.1.1, l'auteur du PP ou de la ST devrait spécifier la norme désignée dans laquelle est documentée la méthode utilisée pour générer des clés cryptographiques. La norme spécifiée peut éventuellement comprendre une ou plusieurs publications de normes, issues par exemple des normes internationales, nationales, industrielles ou organisationnelles.**

FCS_CKM.2 Distribution de clés cryptographiques

Notes d'application pour l'utilisateur

704 Ce composant exige que la méthode utilisée pour distribuer des clés cryptographiques soit spécifiée, ce qui peut être fait conformément à une norme désignée.

Opérations

Affectation :

705 **Dans FCS_CKM.2.1, l'auteur du PP ou de la ST devrait spécifier la méthode de distribution des clés cryptographiques à utiliser.**

706 **Dans FCS_CKM.2.1, l'auteur du PP ou de la ST devrait spécifier la norme désignée dans laquelle est documentée la méthode utilisée pour distribuer des clés cryptographiques. La norme spécifiée peut éventuellement comprendre zéro, une ou plusieurs publications de normes, issues par exemple des normes internationales, nationales, industrielles ou organisationnelles.**

FCS_CKM.3 Accès aux clés cryptographiques

Notes d'application pour l'utilisateur

707 Ce composant exige que la méthode utilisée pour accéder aux clés cryptographiques soit spécifiée, ce qui peut être fait conformément à une norme désignée.

Opérations

Affectation :

708 **Dans FCS_CKM.3.1, l'auteur du PP ou de la ST devrait spécifier le type d'accès aux clés cryptographiques qui est utilisé. Parmi des exemples de types d'accès aux clés cryptographiques on peut citer entre autres la sauvegarde de clés cryptographiques, l'archivage de clés cryptographiques, la notarisation de clés cryptographiques et le recouvrement de clés cryptographiques.**

709 **Dans FCS_CKM.3.1, l'auteur du PP ou de la ST devrait spécifier la méthode d'accès aux clés cryptographiques à utiliser.**

710 **Dans FCS_CKM.3.1, l'auteur du PP ou de la ST devrait spécifier la norme désignée dans laquelle est documentée la méthode utilisée pour accéder aux clés cryptographiques. La norme spécifiée peut éventuellement comprendre zéro, une ou plusieurs publications de normes, issues par exemple des normes internationales, nationales, industrielles ou organisationnelles.**

FCS_CKM.4 Destruction de clés cryptographiques

Notes d'application pour l'utilisateur

711 Ce composant exige que la méthode utilisée pour détruire des clés cryptographiques soit spécifiée, ce qui peut être fait conformément à une norme désignée.

Opérations

Affectation :

712 **Dans FCS_CKM.4.1, l'auteur du PP ou de la ST devrait spécifier la méthode de destruction de clés à utiliser pour détruire des clés cryptographiques.**

713 **Dans FCS_CKM.4.1, l'auteur du PP ou de la ST devrait spécifier la norme désignée dans laquelle est documentée la méthode utilisée pour détruire des clés cryptographiques. La norme spécifiée peut éventuellement comprendre une ou plusieurs publications de normes, issues par exemple des normes internationales, nationales, industrielles ou organisationnelles.**

E.2 Opération cryptographique (FCS_COP)

Notes pour l'utilisateur

714 Une opération cryptographique peut avoir un ou plusieurs modes d'opération associés. Dans ce cas, le ou les modes cryptographiques doivent être spécifiés. Parmi des exemples de mode d'opération cryptographique on peut citer le mode chaînage sur les blocs chiffrés, le mode de rebouclage sur la sortie, le mode dictionnaire et le mode autoclave sur le chiffré.

715 Les opérations cryptographiques peuvent être utilisées pour supporter un ou plusieurs services de sécurité de la TOE. Il peut être nécessaire d'itérer le composant FCS_COP plus d'une fois en fonction de :

a) l'application utilisateur pour laquelle le service de sécurité est utilisé.

b) l'utilisation de différents algorithmes cryptographiques ou de différentes tailles de clés cryptographiques.

c) le type ou la sensibilité des données qui sont exploitées.

716 Dans le cas où la famille "FAU_GEN Génération des données de l'audit de sécurité" est incluse dans le PP ou la ST, en ce qui concerne les événements audités :

a) Les types d'opérations cryptographiques peuvent inclure la génération ou la vérification de signatures numériques, la génération d'une somme de contrôle pour des besoins d'intégrité ou pour la vérification d'un code de contrôle, le hachage sécurisé (condensat de message), le chiffrement ou le déchiffrement de données, le chiffrement ou le déchiffrement de clés cryptographiques, la négociation de clés cryptographiques et la génération de nombres aléatoires.

b) Les attributs du sujet peuvent inclure le ou les rôles du sujet et le ou les utilisateurs associés au sujet.

c) Les attributs de l'objet peuvent inclure l'utilisateur désigné de la clé cryptographique, le rôle de l'utilisateur, l'opération cryptographique pour laquelle la clé cryptographique doit être utilisée, l'identifiant de la clé cryptographique et la période de validité de la clé cryptographique.

FCS_COP.1 Opération cryptographique

Notes d'application pour l'utilisateur

717 Ce composant exige la description de l'algorithme cryptographique et de la taille de clé utilisée pour exécuter l'opération ou les opérations cryptographiques spécifiées qui peuvent être basées sur une norme désignée.

Opérations

Affectation :

718 **Dans FCS_COP.1.1, l'auteur du PP ou de la ST devrait spécifier les opérations cryptographiques exécutées. Les opérations cryptographiques typiques comprennent la génération ou la vérification de signatures numériques, la génération d'un code d'intégrité de message cryptographique pour des besoins d'intégrité ou pour la vérification d'un code d'intégrité, le hachage sécurisé (condensat de message), le chiffrement ou le déchiffrement de données, le chiffrement ou le déchiffrement de clés cryptographiques, la négociation de clés cryptographiques et la génération de nombres aléatoires. L'opération cryptographique peut s'appliquer à des données de l'utilisateur ou à des données de la TSF.**

719 **Dans FCS_COP.1.1, l'auteur du PP ou de la ST devrait spécifier l'algorithme cryptographique à utiliser. Parmi les algorithmes cryptographiques typiques on peut citer entre autres le DES, le RSA et IDEA.**

720 **Dans FCS_COP.1.1, l'auteur du PP ou de la ST devrait spécifier les tailles des clés cryptographiques à utiliser. Les tailles des clés spécifiées devraient convenir à l'algorithme dans le cadre de l'utilisation prévue.**

721 **Dans FCS_COP.1.1, l'auteur du PP ou de la ST devrait spécifier la norme désignée qui explique comment l'opération ou les opérations cryptographiques identifiées sont exécutées. La norme spécifiée peut éventuellement comprendre zéro, une ou plusieurs publications de normes, issues par exemple des normes internationales, nationales, de l'industrie ou des normes organisationnelles.**

Annexe F
(Informative)

Protection des données de l'utilisateur (FDP)

722 La présente classe contient les familles qui spécifient des exigences pour les fonctions de sécurité de la TOE et pour les politiques des fonctions de sécurité de la TOE relatives à la protection des données de l'utilisateur. Cette classe diffère des classes FIA et FPT par le fait qu'elle spécifie des composants pour protéger les données de l'utilisateur, alors que la classe FIA spécifie des composants pour protéger les attributs associés à l'utilisateur et que la classe FPT spécifie des composants pour protéger les informations de la TSF.

723 La classe FDP ne contient pas d'exigences explicites pour le traditionnel contrôle d'accès obligatoire (Mandatory Access Control, MAC) ni pour le traditionnel contrôle d'accès discrétionnaire (Discretionary Access Control, DAC) ; cependant, de telles exigences peuvent être élaborées en utilisant des composants de cette classe.

724 La classe FDP ne traite pas explicitement de la confidentialité, de l'intégrité ni de la disponibilité dans la mesure où ces trois aspects sont le plus souvent imbriqués dans la politique et les mécanismes. Cependant, la politique de sécurité de la TOE doit couvrir de façon adéquate ces trois objectifs dans le PP ou la ST.

725 Le dernier aspect de cette classe est la spécification du contrôle d'accès en termes d'"opérations". Une opération est définie comme un type d'accès spécifique à un objet spécifique. Selon le niveau d'abstraction de l'auteur du PP ou de la ST, ces opérations seront décrites au moyen d'opérations de "lecture" ou d'"écriture" ou au moyen d'opérations plus complexes, comme par exemple "mise à jour de la base de données".

726 Les politiques de contrôle d'accès sont des politiques qui contrôlent l'accès au contenant des informations. Les attributs représentent les attributs des objets. Une fois que les informations en sont extraites, le sujet est libre de les modifier, y compris de les écrire dans un contenant différent, avec des attributs différents. Par opposition, une politique de flux d'information contrôle l'accès aux informations indépendamment de leur contenant. Les attributs des informations, qui peuvent être associés aux attributs du contenant (ou peuvent ne pas l'être, comme dans le cas d'une base de données multi-niveaux) restent associés aux informations lors de leur transfert. Le sujet n'a pas la possibilité, en l'absence d'une autorisation explicite, de changer les attributs des informations.

727 Cette classe n'est pas destinée à fournir une taxinomie complète des politiques d'accès des TI, dans la mesure où des politiques différentes peuvent être imaginées. Les politiques incluses dans cette classe sont simplement celles pour lesquelles l'expérience sur les systèmes réels constitue la base pour spécifier des exigences. Il

peut exister des intentions différentes qui ne sont pas prises en compte dans les définitions proposées ici.

728 Par exemple, on peut imaginer l'objectif de disposer de contrôles de flux d'information imposés (et définis) par l'utilisateur (e.g. une implémentation automatique de gestion de l'avertissement PAS D'ETRANGER). De tels concepts pourraient être traités au moyen de raffinements ou d'extensions des composants de la classe FDP.

729 Enfin, il est important de se souvenir, en examinant les composants de FDP, qu'ils représentent des exigences pour des fonctions qui peuvent être implémentées par un mécanisme qui sert également ou pourrait servir un autre objectif. Par exemple, il est possible de bâtir une politique de contrôle d'accès (FDP_ACC) qui utilise des labels (FDP_IFF.1) comme base du mécanisme de contrôle d'accès.

730 Une politique de sécurité de la TOE peut comprendre de nombreuses politiques d'une fonction de sécurité (SFP), chacune devant être identifiée par les deux composants orientés vers la politique, FDP_ACC et FDP_IFC. Ces politiques prendront généralement en compte les aspects de confidentialité, d'intégrité et de disponibilité comme cela est exigé pour satisfaire aux exigences de la TOE. On devrait prendre soin de garantir que tous les objets sont couverts par une SFP au moins et qu'il n'y a pas de conflits provenant de l'implémentation de plusieurs SFP.

731 Les figures F.1 et F.2 montrent la décomposition de cette classe en ses composants constitutifs.

Classe FDP

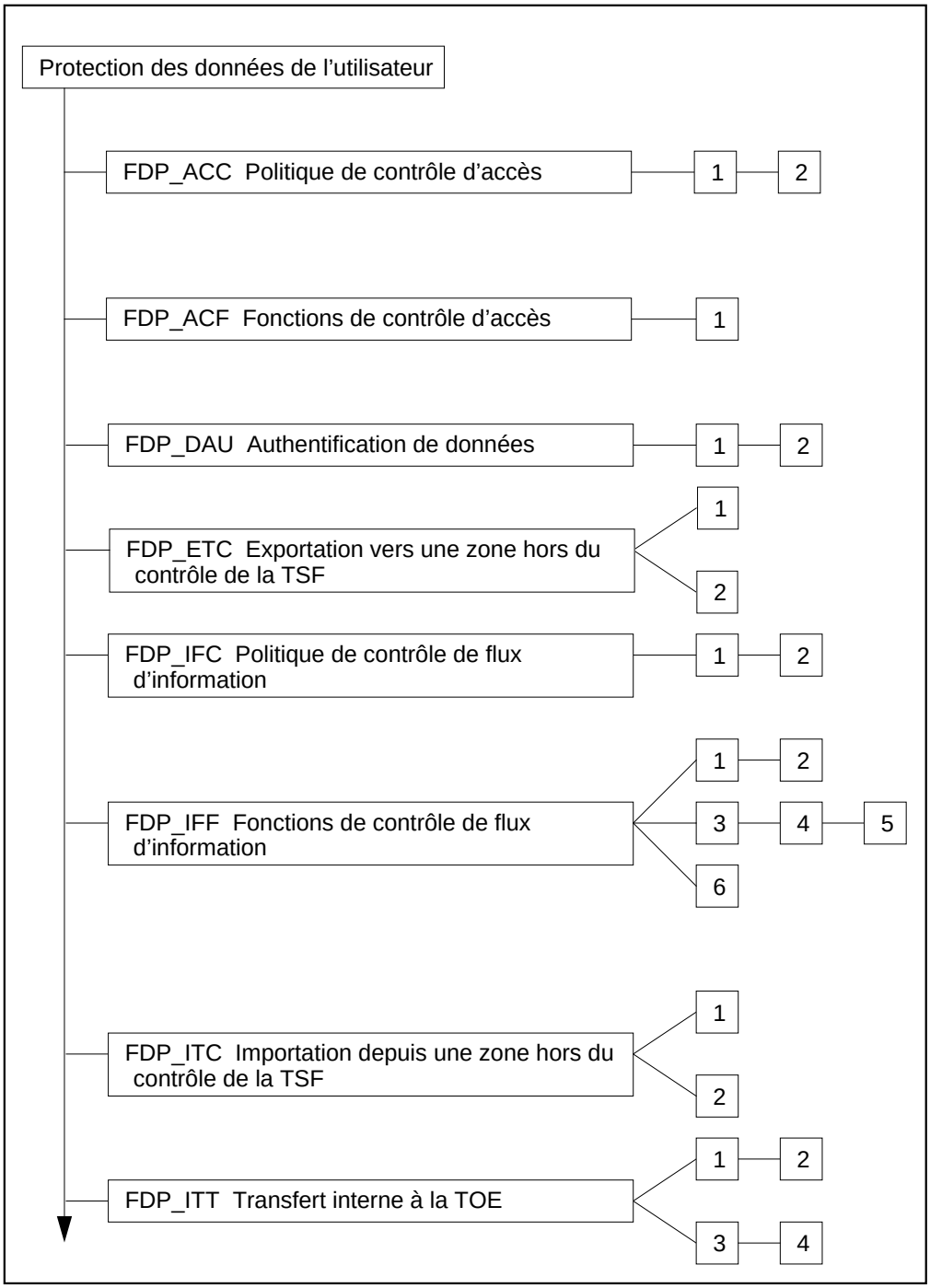


Figure F.1 - Décomposition de la classe "Protection des données de l'utilisateur"

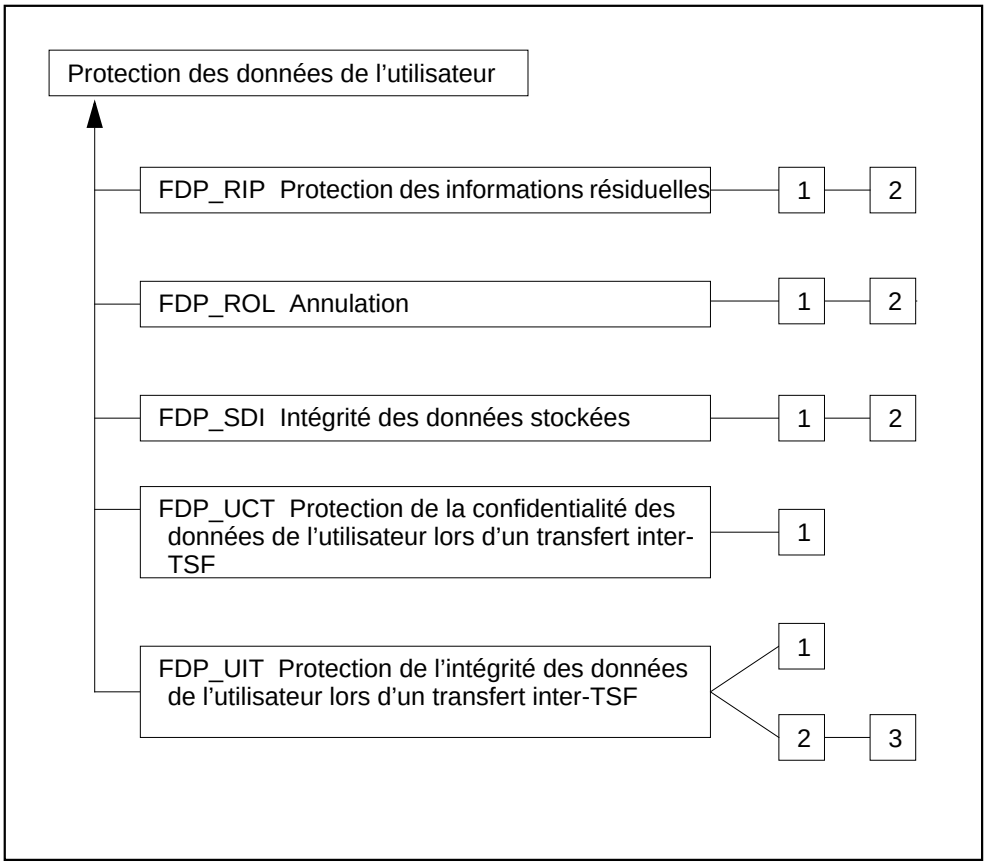


Figure F.2 - Décomposition de la classe "Protection des données de l'utilisateur" (suite)

732 En élaborant un PP ou une ST qui utilise des composants tirés de la classe FDP, les informations suivantes donnent des conseils pour savoir où chercher dans la classe et quels composants choisir.

733 Les exigences de la classe FDP sont définies en terme de fonction de sécurité (abréviation SF) implémente une SFP. Comme une TOE peut implémenter plusieurs SFP en même temps, l'auteur du PP ou de la ST doit spécifier un nom pour chaque SFP, de façon à ce qu'elle puisse être référencée dans d'autres familles. Ce nom devra alors être utilisé dans chaque composant sélectionné pour indiquer qu'il est utilisé en tant que définition des exigences de cette fonction. Cela permet à l'auteur d'indiquer aisément le domaine d'application pour des opérations telles que les objets couverts, les opérations couvertes, les utilisateurs autorisés, etc.

734 Chaque instantiation d'un composant ne peut s'appliquer qu'à une SFP. Par conséquent si une SFP est spécifiée dans un composant, alors cette SFP s'appliquera à tous les éléments de ce composant. Les composants peuvent être instantiés plusieurs fois dans un PP ou une ST pour prendre en compte les différentes politiques si cela est souhaité.

735 La clé pour sélectionner les composants de cette famille est d'avoir une politique de sécurité de la TOE bien définie pour permettre une sélection correcte des composants à partir des deux composants de politique de sécurité FDP_ACC et FDP_IFC. Dans FDP_ACC et FDP_IFC respectivement, toutes les politiques de contrôle d'accès et toutes les politiques de contrôle de flux d'information sont désignées. De plus, le domaine d'application de ces composants se décline en termes de sujets, d'objets et d'opérations couverts par cette fonction de sécurité. Les noms de ces politiques sont censés être utilisés dans tous les composants fonctionnels qui ont une opération demandant l'affectation ou la sélection d'une "SFP de contrôle d'accès" ou d'une "SFP de contrôle de flux d'information". Les règles qui définissent les fonctionnalités des SFP désignées de contrôle d'accès et de contrôle de flux d'information sont définies dans les familles FDP_ACF et FDP_IFF (respectivement).

736 Les étapes suivantes aident à comprendre comment cette classe est appliquée dans la construction d'un PP ou d'une ST :

a) Identifier les politiques à appliquer dans les familles FDP_ACC, et FDP_IFC. Ces familles définissent un domaine d'application pour la politique, une granularité de contrôle et peuvent identifier certaines règles pour accompagner la politique.

b) Identifier les composants et exécuter toutes les opérations applicables dans les composants de politique. Les opérations d'affectation peuvent être généralement exécutées (par exemple avec une affectation "tous fichiers") ou de façon plus spécifique (les fichiers "A", "B", etc.) en fonction du niveau de détail connu.

c) Identifier tous les composants de fonction applicables dans les familles FDP_ACF et FDP_IFF pour couvrir les familles de politiques désignées dans FDP_ACC et FDP_IFC. Exécuter les opérations pour que les composants définissent les règles à appliquer par les politiques désignées. Cela devrait rendre les composants conformes aux exigences de la fonction envisagée ou à élaborer.

d) Identifier la personne qui aura la possibilité de contrôler et de changer des attributs de sécurité de la fonction, tels que "seulement un administrateur de la sécurité", "seulement le propriétaire de l'objet", etc. Sélectionner les composants appropriés dans la Classe FMT Administration de la sécurité et exécuter les opérations. Des raffinements peuvent être utilisés ici pour identifier des caractéristiques manquantes, telles que par exemple "certains ou tous les changements doivent être effectués via un chemin de confiance".

e) Identifier tous les composants appropriés dans la Classe FMT Administration de la sécurité pour les valeurs initiales des nouveaux objets et sujets.

f) Identifier tous les composants d'annulation applicables dans la famille FDP_ROL.

g) Identifier toutes les exigences de protection des informations résiduelles applicables dans la famille FDP_RIP.

h) Identifier tous les composants d'importation et d'exportation applicables, et la façon dont les attributs de sécurité devraient être manipulés pendant l'importation et l'exportation, dans les familles FDP_ITC et FDP_ETC.

i) Identifier tous les composants de communication interne à la TOE applicables dans la famille FDP_ITT.

j) Identifier toutes les exigences d'intégrité pour la protection des informations stockées dans la famille FDP_SDI.

k) Identifier tous les composants de communication inter-TSF applicables dans la famille FDP_UCT ou FDP_UIT.

F.1 Politique de contrôle d'accès (FDP_ACC)

737 La présente famille est basée sur le concept de contrôles arbitraires de l'interaction entre sujets et objets. La portée et le but des contrôles dépendent des attributs de celui qui accède (le sujet), des attributs du contenant auquel on accède (l'objet), des actions (opérations) et de toutes les règles de contrôle d'accès associées.

Notes pour l'utilisateur

738 Les composants de cette famille sont capables d'identifier les SFP de contrôle d'accès (par leur nom) à appliquer par les traditionnels mécanismes de contrôle d'accès discrétionnaire (DAC). La famille définit de plus les sujets, objets et opérations qui sont couverts par des SFP de contrôle d'accès identifiées. Les règles qui définissent la fonctionnalité d'une SFP de contrôle d'accès seront définies par d'autres familles, telles que FDP_ACF et FDP_RIP. Les noms des SFP de contrôle d'accès définies dans FDP_ACC sont censés être utilisés dans les composants fonctionnels qui ont une opération demandant l'affectation ou la sélection d'une "SFP de contrôle d'accès."

739 Les SFP de contrôle d'accès couvrent un ensemble de triplets : sujet, objet, et opérations. Par conséquent un sujet peut être couvert par plusieurs SFP de contrôle d'accès mais seulement par rapport à une opération différente ou à un objet différent. La même chose s'applique bien sûr aux objets et aux opérations.

740 Un aspect critique d'une fonction de contrôle d'accès appliquant une SFP de contrôle d'accès est la possibilité pour des utilisateurs de modifier les attributs impliqués dans les décisions de contrôle d'accès. La famille FDP_ACC ne traite pas de ces aspects. Certaines de ces exigences n'ont pas été définies, mais elles peuvent être ajoutées en tant que raffinements, tandis que d'autres sont couvertes dans d'autres familles et classes telles que la Classe FMT Administration de la sécurité.

741 Il n'y a pas d'exigences d'audit dans FDP_ACC car cette famille spécifie des exigences pour une SFP de contrôle d'accès. Des exigences d'audit peuvent être trouvées dans des familles spécifiant des fonctions pour satisfaire les SFP de contrôle d'accès identifiées dans ces familles.

742 Cette famille donne à un auteur de PP ou de ST la possibilité de spécifier plusieurs politiques, par exemple une SFP de contrôle d'accès fixe à appliquer pour un domaine d'application, et une SFP de contrôle d'accès flexible à définir pour un domaine d'application différent. Pour spécifier plusieurs politiques de contrôle d'accès, les composants de cette famille peuvent être itérés plusieurs fois dans un PP ou une ST avec différents sous-ensembles d'opérations et d'objets. Cela permet de traiter des TOE qui contiennent plusieurs politiques, chacune couvrant un ensemble particulier d'opérations et d'objets. En d'autres termes, l'auteur du PP ou de la ST devrait spécifier les informations requises dans les composants ACC pour chacune des SFP de contrôle d'accès que la TSF appliquera. Par exemple, une TOE incorporant trois SFP de contrôle d'accès, chacune couvrant seulement un sous-ensemble d'objets, de sujets, et d'opérations dans la TOE, contiendra un

composant “FDP_ACC.1 Contrôle d’accès partiel” pour chacune des trois SFP de contrôle d’accès, nécessitant un total de trois composants FDP_ACC.1.

FDP_ACC.1 Contrôle d’accès partiel

Notes d’application pour l’utilisateur

743 Les termes “objet” et “sujet” font référence à des éléments génériques de la TOE. Pour qu’une politique soit implémentable, les entités doivent être clairement identifiées. Pour un PP, les objets et les opérations pourraient être exprimés avec des expressions telles que : “objets désignés”, “répertoires de données”, “observer les accès”, etc. Pour un système spécifique, ces termes génériques (sujet, objet) doivent être raffinés, e.g. fichiers, registres, ports, démons, appels ouverts, etc.

744 Ce composant spécifie que la politique couvre un certain ensemble bien défini d’opérations sur certain sous-ensemble d’objets. Il ne fixe aucune contrainte sur toute opération ne figurant pas dans l’ensemble, y compris les opérations sur des objets pour lesquels d’autres opérations sont contrôlées.

Opérations

Affectation :

745 **Dans FDP_ACC.1.1, l’auteur du PP ou de la ST devrait spécifier une SFP de contrôle d’accès nommée de façon unique à appliquer par la TSF.**

746 **Dans FDP_ACC.1.1, l’auteur du PP ou de la ST devrait spécifier la liste de sujets, d’objets, et d’opérations entre sujets et objets couverts par la SFP.**

FDP_ACC.2 Contrôle d’accès complet

Notes d’application pour l’utilisateur

747 Ce composant exige que toutes les opérations possibles sur des objets, qui sont comprises dans la SFP, soient couvertes par une SFP de contrôle d’accès.

748 L’auteur du PP ou de la ST doit démontrer que chaque combinaison d’objets et de sujets est couverte par une SFP de contrôle d’accès.

Opérations

Affectation :

749 Dans FDP_ACC.2.1, l’auteur du PP ou de la ST devrait spécifier une SFP de contrôle d’accès désignée de façon unique, à appliquer par la TSF.

750 **Dans FDP_ACC.2.1, l’auteur du PP ou de la ST devrait spécifier la liste de sujets et d’objets couverts par la SFP. Toutes les opérations entre ces sujets et objets seront couvertes par la SFP.**

F.2 Fonctions de contrôle d'accès (FDP_ACF)

751 La présente famille décrit les règles relatives aux fonctions spécifiques qui peuvent implémenter une politique de contrôle d'accès citée dans FDP_ACC, qui spécifie également le domaine d'application de la politique.

Notes pour l'utilisateur

752 Cette famille donne à un auteur de PP ou de ST la possibilité de décrire les règles pour le contrôle d'accès. Ceci aboutit à un système où l'accès aux objets ne changera pas. Un tel objet est par exemple "message du jour", qui est lisible par tous et modifiable seulement par l'administrateur autorisé. Cette famille offre également à l'auteur du PP ou de la ST la possibilité de décrire les règles qui permettent de faire des exceptions aux règles générales de contrôle d'accès. De telles exceptions peuvent explicitement soit permettre soit refuser l'autorisation d'accéder à un objet.

753 Il n'existe pas de composants explicites pour spécifier d'autres fonctions possibles telles que le contrôle à deux personnes, des règles de séquencement pour opérations, ou des contrôles exclusifs. Cependant, ces mécanismes, ainsi que les mécanismes traditionnels DAC, peuvent être représentés avec les composants existants, en élaborant soigneusement les règles de contrôle d'accès.

754 Il est possible de spécifier un ensemble de SF de contrôle d'accès acceptables dans cette famille, comme par exemple :

- listes de contrôle d'accès (access control lists : ACL)
- spécifications de contrôle d'accès basées sur la date
- spécifications de contrôle d'accès basées sur l'origine
- attributs de contrôle d'accès contrôlés par le propriétaire

FDP_ACF.1 Contrôle d'accès basé sur les attributs de sécurité

Notes d'application pour l'utilisateur

755 Ce composant fournit des exigences pour un mécanisme qui régit le contrôle d'accès en fonction des attributs de sécurité associés à des sujets et des objets. Chaque objet et chaque sujet possède un ensemble d'attributs associés, tels que le lieu et la date de création, les droits d'accès (e.g., listes de contrôle d'accès (ACL)). Ce composant permet à l'auteur du PP ou de la ST de spécifier les attributs qui seront utilisés pour l'arbitrage de contrôle d'accès. Ce composant permet que des règles de contrôle d'accès utilisant ces attributs soient spécifiées.

756 Des exemples d'attributs qu'un auteur de PP ou de ST pourrait spécifier sont présentées dans les paragraphes suivants.

757 Un *attribut d'identité* peut être associé à des utilisateurs, sujets, ou objets pour être utilisé lors de l'arbitrage. Comme exemples de tels attributs on peut citer le nom du programme utilisé dans la création du sujet, ou un attribut de sécurité affecté au programme.

758 Un *attribut temporel* peut être utilisé pour spécifier que l'accès sera autorisé pendant certaines heures de la journée, certains jours de la semaine, ou pendant une certaine année calendaire.

759 Un *attribut de lieu* pourrait spécifier si le lieu est l'endroit où se fait la requête pour l'opération, l'endroit où l'opération est exécutée, ou l'endroit où se produisent les deux actions. Ce lieu pourrait être défini en fonction des tables internes destinées à représenter les interfaces logiques de la TSF par des lieux tels que les sites des terminaux, des CPU, etc.

760 Un *attribut de groupe* permet à un groupe unique d'utilisateurs d'être associé à une opération pour des buts de contrôle d'accès. Si nécessaire, l'opération de raffinement devrait être utilisée pour spécifier le nombre maximum de groupes pouvant être définis, la participation maximum dans un groupe, et le nombre maximum de groupes auxquels un utilisateur peut être associé au même moment.

761 Ce composant fournit également des exigences pour que les fonctions de sécurité du contrôle d'accès puissent de façon explicite autoriser ou refuser l'accès à un objet en fonction d'attributs de sécurité. Ceci pourrait être utilisé pour accorder des privilèges, des droits d'accès ou des autorisations d'accès dans la TOE. De tels privilèges, droits ou autorisations pourraient s'appliquer à des utilisateurs, à des sujets (représentant des utilisateurs ou des applications) et à des objets.

Opérations

Affectation :

762 **Dans FDP_ACF.1.1, l'auteur du PP ou de la ST devrait spécifier le nom d'une SFP de contrôle d'accès que la TSF devra appliquer. Le nom de la SFP de contrôle d'accès et le domaine d'application de cette politique sont définis dans des composants de FDP_ACC.**

763 **Dans FDP_ACF.1.1, l'auteur du PP ou de la ST devrait spécifier les attributs de sécurité ou des groupes désignés d'attributs de sécurité que la fonction utilisera dans la spécification des règles. De tels attributs sont par exemple : l'identité de l'utilisateur, l'identité du sujet, le rôle, l'heure du jour, le lieu, les ACL ou tout autre attribut spécifié par l'auteur du PP ou de la ST. Des groupes d'attributs de sécurité désignés peuvent être spécifiés pour offrir un moyen pratique de faire référence à plusieurs attributs de sécurité. Des groupes désignés pourraient procurer un moyen utile pour associer des "rôles" définis dans "FMT_SMR Rôles pour l'administration de la sécurité", ainsi que tous leurs attributs pertinents, à des sujets. En d'autres termes, chaque rôle pourrait être associé à un groupe d'attributs désigné.**

764 **Dans FDP_ACF.1.2, l'auteur du PP ou de la ST devrait spécifier les règles des SFP régissant l'accès aux sujets contrôlés et aux objets contrôlés utilisant des opérations contrôlées sur des objets contrôlés. Ces règles spécifient quand l'accès est accordé ou refusé. L'auteur peut spécifier des fonctions générales de contrôle d'accès (e.g. des bits de**

permission typiques) ou des fonctions de contrôle d'accès plus fines (e.g. par ACL).

765 **Dans FDP_ACF.1.3, l'auteur du PP ou de la ST devrait spécifier les règles, en fonction d'attributs de sécurité, qui autorisent explicitement l'accès de sujets à des objets qui seront utilisés pour autoriser explicitement un accès. Ces règles viennent en complément de celles spécifiées dans FDP_ACF.1.1. Elles sont comprises dans FDP_ACF.1.3 car elles sont destinées à contenir des exceptions aux règles définies dans FDP_ACF.1.1. Des règles pour autoriser explicitement un accès sont par exemple fonction d'un ensemble de privilèges associé à un sujet qui autorise systématiquement l'accès à des objets couverts par la SFP de contrôle d'accès qui a été spécifiée. Si une telle possibilité n'est pas souhaitée, alors l'auteur du PP ou de la ST devrait spécifier "aucune".**

766 **Dans FDP_ACF.1.4, l'auteur du PP ou de la ST devrait spécifier les règles, en fonction d'attributs de sécurité, qui refusent explicitement l'accès de sujets à des objets. Ces règles viennent en complément de celles spécifiées dans FDP_ACF.1.1. Elles sont comprises dans FDP_ACF.1.4 car elles sont destinées à contenir des exceptions aux règles définies dans FDP_ACF.1.1. Des règles pour autoriser explicitement un accès sont par exemple fonction d'un ensemble de privilèges associés à un sujet qui autorise systématiquement l'accès à des objets couverts par la SFP de contrôle d'accès qui a été spécifiée. Si une telle possibilité n'est pas souhaitée, alors l'auteur du PP ou de la ST devrait spécifier "aucune".**

F.3 Authentification de données (FDP_DAU)

767 La présente famille décrit des fonctions spécifiques qui peuvent être utilisées pour authentifier des données ‘statiques’.

Notes pour l’utilisateur

768 Les composants de cette famille doivent être utilisés quand il existe une exigence pour une authentification de données ‘statiques’, i.e. lorsque des données doivent être signées mais non transmises. (Il est à noter que la famille FCO_NRO traite de la non-répudiation de l’origine des informations reçues lors d’un échange de données.)

FDP_DAU.1 Authentification de données élémentaire

Notes d’application pour l’utilisateur

769 Ce composant peut être satisfait par des fonctions de hachage à sens unique (somme de contrôle cryptographique, empreintes digitales, condensat de message), pour générer une valeur de hachage pour un document définitif qui peut être utilisée pour vérifier la validité ou l’authenticité de son contenu.

Opérations

Affectation :

770 **Dans FDP_DAU.1.1, l’auteur du PP ou de la ST devrait spécifier la liste d’objets ou de types d’informations pour lesquels la TSF doit être capable de générer une preuve d’authentification de données.**

771 **Dans FDP_DAU.1.2, l’auteur du PP ou de la ST devrait spécifier la liste de sujets qui auront la possibilité de vérifier une preuve d’authentification de données pour les objets identifiés dans l’élément précédent. La liste de sujets pourrait être très spécifique si les sujets sont connus, ou elle pourrait être plus générique et faire référence à un “type” de sujet tel qu’un rôle identifié.**

FDP_DAU.2 Authentification de données avec identité du garant

Notes d’application pour l’utilisateur

772 Ce composant exige en plus la possibilité de vérifier l’identité de l’utilisateur qui offre la garantie d’authenticité (e.g. une tierce partie de confiance).

Opérations

Affectation :

773 Dans FDP_DAU.2.1, l'auteur du PP ou de la ST devrait spécifier la liste d'objets ou de types d'informations pour lesquels la TSF doit être capable de générer une preuve d'authentification de données.

774 **Dans FDP_DAU.2.2, l'auteur du PP ou de la ST devrait spécifier la liste de sujets qui auront la possibilité de vérifier une preuve d'authentification de données pour les objets identifiés dans l'élément précédent ainsi que l'identité de l'utilisateur qui a créé la preuve de l'authentification de données.**

F.4 Exportation vers une zone hors du contrôle de la TSF (FDP_ETC)

775 La présente famille définit les fonctions pour exporter des données de l'utilisateur à partir de la TOE de telle sorte que leurs attributs de sécurité peuvent être soit explicitement préservés soit être ignorés une fois que les données ont été exportées. La cohérence de ces attributs de sécurité est traitée par FPT_TDC Cohérence des données de la TSF inter-TSF.

776 FDP_ETC concerne les limitations de l'exportation et l'association d'attributs de sécurité avec les données de l'utilisateur exportées.

Notes pour l'utilisateur

777 Cette famille, ainsi que la famille correspondante pour l'importation FDP_ITC, traite de la façon dont la TOE gère des données de l'utilisateur transférées sous son contrôle ou en dehors de son contrôle. Cette famille concerne dans son principe l'exportation de données de l'utilisateur et de leurs attributs de sécurité associés.

778 Plusieurs activités pourraient être impliquées ici :

a) exporter des données de l'utilisateur sans attribut de sécurité ;

b) exporter des données de l'utilisateur ainsi que des attributs de sécurité, les deux étant associés, et les attributs de sécurité représentant sans ambiguïté les données de l'utilisateur exportées.

779 S'il existe plusieurs SFP (de contrôle d'accès ou de contrôle de flux d'information) alors il peut être indiqué d'itérer ces composants une fois pour chaque SFP désignée.

FDP_ETC.1 Exportation de données de l'utilisateur sans attributs de sécurité

Notes d'application pour l'utilisateur

780 Ce composant est utilisé pour spécifier l'exportation des données de l'utilisateur sans exporter leurs attributs de sécurité.

Opérations

Affectation :

781 **Dans FDP_ETC.1.1, l'auteur du PP ou de la ST devrait spécifier la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information qui seront appliquées en exportant des données de l'utilisateur. Les données de l'utilisateur que cette fonction exporte sont délimitées par l'affectation de ces SFP.**

FDP_ETC.2 Exportation de données de l'utilisateur avec attributs de sécurité

Notes d'application pour l'utilisateur

782 Les données de l'utilisateur sont exportées avec leurs attributs de sécurité. Les attributs de sécurité sont associés sans ambiguïté avec les données de l'utilisateur. Il y a plusieurs façons de réaliser cette association. Une façon de les associer consiste à mettre les données de l'utilisateur et les attributs de sécurité physiquement sur le même support (e.g. la même disquette), ou en utilisant des techniques cryptographiques telles que des signatures sûres pour associer les attributs et les données de l'utilisateur. "FTP_ITC Canal de confiance inter-TSF" pourrait être utilisé pour garantir que les attributs sont correctement reçus par l'autre produit TI de confiance tandis que "FPT_TDC Cohérence des données de la TSF inter-TSF" peut être utilisé pour s'assurer que ces attributs sont correctement interprétés. De plus, "FTP_TRP Chemin de confiance" pourrait être utilisé pour s'assurer que l' exportation est initiée par le bon utilisateur.

Opérations

Affectation :

783 **Dans FDP_ETC.2.1, l'auteur du PP ou de la ST devrait spécifier la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information qui seront appliquées en exportant des données de l'utilisateur. Les données de l'utilisateur que cette fonction exporte sont délimitées par l'affectation de ces SFP.**

784 **Dans FDP_ETC.2.4, l'auteur du PP ou de la ST devrait spécifier toute règle de contrôle d'exportation supplémentaire ou "aucune" s'il n'y en a pas. Ces règles seront appliquées par la TSF en complément des SFP de contrôle d'accès ou des SFP de contrôle de flux d'information sélectionnées dans FDP_ETC.2.1.**

F.5 Politique de contrôle de flux d'information (FDP_IFC)

785 La présente famille couvre l'identification de SFP de contrôle de flux d'information et, pour chaque SFP, spécifie le domaine d'application de la SFP.

786 Parmi des exemples de politiques de sécurité qui pourraient satisfaire cet objectif, on trouve :

- le modèle de sécurité de Bell et La Padula [B&L] ;
- le modèle d'intégrité de Biba [Biba] ;
- le modèle de non-interférence [Gogu1,Gogu2].

Notes pour l'utilisateur

787 Les composants de cette famille sont capables d'identifier les SFP de contrôle de flux d'information devant être appliquées par les mécanismes de contrôle d'accès obligatoire qui pourraient être trouvés dans une TOE. Cependant, ils vont au-delà des mécanismes traditionnels MAC et peuvent être utilisés pour identifier et décrire des politiques de non-interférence et de transitions d'états. Ils définissent aussi les sujets sous le contrôle de la politique, les informations sous le contrôle de la politique, et les opérations qui provoquent le transfert d'informations contrôlées en direction et en provenance de sujets contrôlés pour chaque SFP de contrôle de flux d'information dans la TOE. La fonctionnalité qui définit les règles d'une SFP de contrôle de flux d'information est définie par d'autres familles telles que FDP_IFF et FDP_RIP. Les SFP de contrôle d'accès désignées ici dans FDP_IFC sont destinées à être utilisées dans les composants fonctionnels qui ont une opération nécessitant l'affectation ou la sélection d'une "SFP de contrôle de flux d'information."

788 Ces composants sont tout à fait flexibles. Ils permettent au domaine de contrôle de flux d'être spécifié et il n'y a aucune exigence pour que le mécanisme soit basé sur des labels. Les différents éléments des composants de contrôle de flux d'information permettent également différents degrés d'exception à la politique.

789 Chaque SFP couvre un ensemble de triplets : sujet, information, et opérations qui provoquent le transfert d'informations contrôlées en direction et en provenance de sujets. Certaines politiques de contrôle de flux d'information peuvent se placer à un niveau de détail très fin et décrire explicitement des sujets en termes de processus dans un système d'exploitation. D'autres politiques de contrôle de flux d'information peuvent se placer à un niveau élevé et décrire des sujets en termes génériques d'utilisateurs ou de canaux d'entrées/sorties. Si la politique de contrôle de flux d'information se place à un niveau de détail trop élevé, elle ne peut pas définir clairement les fonctions de sécurité des TI souhaitées. Dans de tels cas, il est plus approprié d'inclure de telles descriptions de politiques de contrôle de flux d'information dans les objectifs. Alors les fonctions de sécurité des TI souhaitées peuvent être spécifiées pour contribuer à ces objectifs.

790 Dans le second composant (FDP_IFC.2 Contrôle de flux d'information complet), chaque SFP de contrôle de flux d'information couvre toutes les opérations possibles qui provoquent le transfert des informations couvertes par cette SFP en direction et

en provenance de sujets couverts par cette SFP. De plus, tous les flux d'information devront être couverts par une SFP. Par conséquent, pour chaque action qui provoque le transfert d'informations, il existera un ensemble de règles définissant si l'action est autorisée. S'il y a plusieurs SFP qui sont applicables pour un flux d'information donné, toutes les SFP concernées doivent autoriser ce flux avant qu'il ne puisse être transféré.

791 Une SFP de contrôle de flux d'information couvre un ensemble d'opérations bien défini. Les couvertures par les SFP peuvent être "complètes" par rapport à certains flux d'information, ou elles peuvent concerner seulement certaines des opérations qui affectent les flux d'information.

792 Une SFP de contrôle d'accès contrôle l'accès aux objets qui contiennent des informations. Une SFP de contrôle de flux d'information contrôle l'accès aux informations, indépendamment de leur contenant. Les attributs des informations, qui peuvent être associés aux attributs du contenant (ou peuvent ne pas l'être, comme dans le cas d'une base de données multi-niveaux) demeurent avec les informations pendant leur transfert. La personne qui accède n'a pas la possibilité, en l'absence d'une autorisation explicite, de changer les attributs des informations.

793 Les flux d'information et les opérations peuvent être exprimées à plusieurs niveaux. Dans le cas d'une ST, les flux d'information et opérations pourraient être spécifiés au niveau d'un système spécifique : paquets TCP/IP transférés à travers un firewall en fonction d'adresses IP connues. Pour un PP, les flux d'information et les opérations pourraient être exprimées par types : message électronique, répertoires de données, observer les accès, etc.

794 Les composants de cette famille peuvent être appliqués plusieurs fois dans un PP ou une ST à différents sous-ensembles d'opérations et d'objets. Cela permet de traiter des TOE qui contiennent plusieurs politiques, chacune traitant d'un ensemble particulier d'objets, de sujets, et d'opérations.

FDP_IFC.1 Contrôle de flux d'information partiel

Notes d'application pour l'utilisateur

795 Ce composant exige qu'une politique de contrôle de flux d'information s'applique à un sous-ensemble des opérations possibles dans la TOE.

Opérations

Affectation :

796 **Dans FDP_IFC.1.1, l'auteur du PP ou de la ST devrait spécifier une SFP de contrôle de flux d'information désignée de façon unique, devant être appliquée par la TSF.**

797 **Dans FDP_IFC.1.1, l'auteur du PP ou de la ST devrait spécifier la liste de sujets, d'informations et d'opérations qui provoquent le transfert d'informations contrôlées à destination et en provenance de sujets**

contrôlés couverts par la SFP. Comme indiqué ci-dessus, la liste de sujets pourrait se placer à différents niveaux de détail en fonction des besoins de l'auteur du PP ou de la ST. Elle pourrait spécifier des utilisateurs, des machines ou des processus par exemple. Les informations pourraient faire référence à des données telles que des messages électroniques ou des protocoles réseaux, ou à des objets plus spécifiques semblables à ceux spécifiés dans le cadre d'une politique de contrôle d'accès. Si les informations qui sont spécifiées sont contenues dans un objet qui fait l'objet d'une politique de contrôle d'accès, alors à la fois la politique de contrôle d'accès et la politique de contrôle de flux d'information doivent être appliquées avant que les informations spécifiées puissent transiter à destination ou en provenance de l'objet.

FDP_IFC.2 Contrôle de flux d'information complet

Notes d'application pour l'utilisateur

798 Ce composant exige que toutes les opérations possibles qui provoquent le transfert d'informations à destination et en provenance de sujets compris dans la SFP soient couvertes par une SFP de contrôle de flux d'information.

799 L'auteur du PP ou de la ST doit démontrer que chaque combinaison de flux d'information et de sujets est couverte par une SFP de contrôle de flux d'information.

Opérations

Affectation :

800 Dans FDP_IFC.2.1, l'auteur du PP ou de la ST devrait spécifier une SFP de contrôle de flux d'information désignée de façon unique devant être appliquée par la TSF.

801 **Dans FDP_IFC.2.1, l'auteur du PP ou de la ST devrait spécifier la liste de sujets et d'informations qui devraient être couverts par la SFP. Toutes les opérations qui provoquent le transfert d'informations contrôlées à destination et en provenance de sujets contrôlés seront couverts par la SFP.** Comme indiqué ci-dessus, la liste de sujets pourrait se placer à différents niveaux de détail en fonction des besoins de l'auteur du PP ou de la ST. Elle pourrait spécifier des utilisateurs, des machines ou des processus par exemple. Les informations pourraient faire référence à des données telles que des messages électroniques ou des protocoles de réseaux, ou à des objets plus spécifiques semblables à ceux spécifiés dans le cadre d'une politique de contrôle d'accès. Si les informations qui sont spécifiées sont contenues dans un objet qui fait l'objet d'une politique de contrôle d'accès, alors à la fois la politique de contrôle d'accès et la politique de contrôle de flux d'information doivent être appliquées avant que les informations spécifiées puissent transiter à destination ou en provenance de l'objet**.**

F.6 Fonctions de contrôle de flux d'information (FDP_IFF)

802 La présente famille décrit les règles concernant les fonctions spécifiques qui peuvent implémenter les SFP de contrôle de flux d'information citées dans FDP_IFC, qui spécifie également le domaine d'application de la politique. Elle est formée de deux "arborescences", l'une concernant les problèmes habituels de fonctions de contrôle de flux d'information, et l'autre concernant les flux d'information illicites (i.e. canaux cachés) par rapport à une ou plusieurs SFP de contrôle de flux d'information. Cette division est faite car les problèmes concernant les flux d'information illicites sont, en un certain sens, orthogonaux aux autres problèmes traités par une SFP. Les flux d'information illicites sont des flux transitant en violation de la politique et donc ils ne constituent pas un problème de politique.

Notes pour l'utilisateur

803 Afin d'implémenter une protection forte contre la divulgation ou la modification due à un logiciel non sûr, des contrôles sur les flux d'information sont nécessaires. Les contrôles d'accès seuls ne sont pas suffisants car ils ne contrôlent que l'accès aux contenants, permettant aux informations qu'ils contiennent de transiter sans contrôles à travers un système.

804 Dans cette famille, l'expression "types de flux d'information illicites" est utilisée. Cette expression peut être utilisée pour faire référence à la classification des flux, par exemple en "canaux de stockages" ou "canaux temporels", ou elle peut faire référence à des classifications améliorées reflétant les besoins d'un auteur de PP ou de ST.

805 La flexibilité de ces composants permet la définition d'une politique de privilèges dans FDP_IFF.1 et FDP_IFF.2 autorisant à court-circuiter de façon contrôlée tout ou partie d'une SFP donnée. Si le besoin d'une approche prédéfinie pour court-circuiter une SFP existe, l'auteur du PP ou de la ST devrait envisager l'incorporation d'une politique de privilèges.

FDP_IFF.1 Attributs de sécurité simples

Notes d'application pour l'utilisateur

806 Ce composant exige des attributs de sécurité pour les informations et les sujets qui provoquent le transfert de ces informations et des sujets qui agissent comme des destinataires de ces informations. Les attributs des contenants d'informations devraient aussi être pris en compte s'il est souhaité qu'ils jouent un rôle dans les décisions de contrôle de flux d'information ou s'ils sont couverts par une politique de contrôle d'accès. Ce composant spécifie les règles clés qui sont appliquées, et décrit comment les attributs de sécurité en sont déduits. Par exemple, ce composant devrait être utilisé lorsque au moins une des SFP de contrôle de flux d'information dans la TSP est basée sur des labels tels que ceux définis dans le modèle de politique de sécurité de Bell et LaPadula [B&L], mais ces attributs de sécurité ne forment pas une hiérarchie.

807 Ce composant ne spécifie pas les détails indiquant comment un attribut de sécurité est attribué (i.e. par utilisateur ou par processus). La flexibilité dans la politique est obtenue en élaborant des affectations qui permettent de spécifier une politique et des exigences pour les fonctions supplémentaires, si nécessaire.

808 Ce composant fournit également des exigences pour que les fonctions de contrôle de flux d'information puissent autoriser et refuser explicitement un flux d'information basé sur des attributs de sécurité. Cela pourrait être utilisé pour implémenter une politique de privilèges qui couvre des exceptions à la politique de base définie dans ce composant.

Opérations

Affectation :

809 **Dans FDP_IFF.1.1, l'auteur du PP ou de la ST devrait spécifier les SFP de contrôle de flux d'information appliquées par la TSF. Le nom d'une SFP de contrôle de flux d'information et son domaine d'application sont définis dans les composants de la famille FDP_IFC.**

810 **Dans FDP_IFF.1.1, l'auteur du PP ou de la ST devrait spécifier le nombre minimum et le type d'attributs de sécurité que la fonction utilisera dans la spécification des règles. De tels attributs peuvent être par exemple l'identifiant d'un sujet, le niveau de sensibilité d'un sujet, le niveau d'habilitation d'un sujet, le niveau de sensibilité d'informations, etc. Le nombre minimum de types d'attributs de sécurité devrait être suffisant pour prendre en compte les besoins environnementaux.**

811 **Dans FDP_IFF.1.2, l'auteur du PP ou de la ST devrait spécifier pour chaque opération les relations basées sur les attributs de sécurité qui doivent exister entre un sujet et les attributs de sécurité des informations que la TSF appliquera.**

812 **Dans FDP_IFF.1.3, l'auteur du PP ou de la ST devrait spécifier toutes les règles supplémentaires de SFP de contrôle de flux d'information que la TSF doit appliquer. S'il n'y a pas de règles supplémentaires, alors l'auteur du PP ou de la ST devrait spécifier "aucune".**

813 **Dans FDP_IFF.1.4, l'auteur du PP ou de la ST devrait spécifier toutes les capacités supplémentaires en termes de SFP que la TSF doit fournir. S'il n'y en a pas, alors l'auteur du PP ou de la ST devrait spécifier "aucune".**

814 **Dans FDP_IFF.1.5, l'auteur du PP ou de la ST devrait spécifier les règles, en fonction des attributs de sécurité, qui autorisent explicitement des flux d'information. Ces règles viennent en complément de celles spécifiées dans les éléments précédents. Elles figurent dans FDP_IFF.1.5 car elles sont destinées à contenir des exceptions aux règles définies dans les éléments précédents. Les règles pour autoriser explicitement des flux d'information sont par exemple**

fonction d'un ensemble de privilèges associé à un sujet, qui accorde systématiquement au sujet la possibilité de provoquer un transfert pour des informations qui sont couvertes par la SFP qui a été spécifiée. Si une telle possibilité n'est pas souhaitée, alors l'auteur du PP ou de la ST devrait spécifier "aucune".

815 **Dans FDP_IFF.1.6, l'auteur du PP ou de la ST devrait spécifier les règles, en fonction des attributs de sécurité, qui refusent explicitement des flux d'information. Ces règles viennent en complément de celles spécifiées dans les éléments précédents. Elles figurent dans FDP_IFF.1.6 car elles sont destinées à contenir des exceptions aux règles définies dans les éléments précédents. Les règles pour autoriser explicitement des flux d'information sont par exemple fonction d'un ensemble de privilèges associé à un sujet, qui refuse systématiquement au sujet la possibilité de provoquer un transfert pour des informations qui sont couvertes par la SFP qui a été spécifiée. Si une telle possibilité n'est pas souhaitée, alors l'auteur du PP ou de la ST devrait spécifier "aucune".**

FDP_IFF.2 Attributs de sécurité hiérarchiques

Notes d'application pour l'utilisateur

816 Ce composant exige que toutes les SFP de contrôle de flux d'information dans la TSP utilisent des attributs de sécurité hiérarchiques qui forment un treillis.

817 Il devrait être utilisé par exemple quand au moins une des SFP de contrôle de flux d'information dans la TSP est basée sur des labels tels que ceux définis dans le modèle de politique de sécurité de Bell et LaPadula [B&L] et forment une hiérarchie.

818 Il est important de noter que les exigences de relations hiérarchiques identifiées dans FDP_IFF.2.5 doivent seulement s'appliquer aux attributs de sécurité de contrôle de flux d'information pour les SFP de contrôle de flux d'information qui ont été identifiées dans FDP_IFF.2.1. Ce composant n'est pas censé s'appliquer à d'autres SFP telles que des SFP de contrôle d'accès.

819 De même que le composant précédent, ce composant pourrait aussi être utilisé pour implémenter une politique de privilèges couvrant les règles qui pourvoient à l'autorisation ou au refus explicite de flux d'information.

820 S'il arrive que plusieurs SFP de contrôle de flux d'information doivent être spécifiées, et que chacune de ces SFP aient leurs propres attributs de sécurité qui ne soient pas reliés les uns aux autres, alors l'auteur du PP ou de la ST devrait itérer ce composant une fois pour chacune de ces SFP. Sinon un conflit pourrait survenir avec les sous-éléments de FDP_IFF.2.5 car les relations requises n'existeront pas.

Opérations

Affectation :

821 Dans FDP_IFF.2.1, l'auteur du PP ou de la ST devrait spécifier les SFP de contrôle de flux d'information appliquées par la TSF. Le nom d'une SFP de contrôle de flux d'information et son domaine d'application sont définis dans les composants de la famille FDP_IFC.

822 Dans FDP_IFF.2.1, l'auteur du PP ou de la ST devrait spécifier le nombre minimum et le type d'attributs de sécurité que la fonction utilisera dans la spécification des règles. De tels attributs peuvent être par exemple l'identifiant d'un sujet, le niveau de sensibilité d'un sujet, le niveau d'habilitation d'un sujet, le niveau de sensibilité d'information, etc. Le nombre minimum de types d'attributs de sécurité devrait être suffisant pour prendre en compte les besoins environnementaux.

823 Dans FDP_IFF.2.2, l'auteur du PP ou de la ST devrait spécifier pour chaque opération les relations basées sur les attributs de sécurité qui doivent exister entre un sujet et les attributs de sécurité des informations que la TSF appliquera. **Ces relations devraient être basées sur les relations ordonnées entre les attributs de sécurité.**

824 Dans FDP_IFF.2.3, l'auteur du PP ou de la ST devrait spécifier toutes les règles supplémentaires de SFP de contrôle de flux d'information que la TSF doit appliquer. S'il n'y a pas de règles supplémentaires, alors l'auteur du PP ou de la ST devrait spécifier "aucune".

825 Dans FDP_IFF.2.4, l'auteur du PP ou de la ST devrait spécifier toutes les capacités supplémentaires en termes de SFP que la TSF doit fournir. S'il n'y a pas de possibilités supplémentaires, alors l'auteur du PP ou de la ST devrait spécifier "aucune".

826 Dans FDP_IFF.2.5, l'auteur du PP ou de la ST devrait spécifier les règles, en fonction des attributs de sécurité, qui autorisent explicitement des flux d'information. Ces règles viennent en complément de celles spécifiées dans les éléments précédents. Elles figurent dans FDP_IFF.2.5 car elles sont destinées à contenir des exceptions aux règles définies dans les éléments précédents. Les règles pour autoriser explicitement des flux d'information sont par exemple fonction d'un ensemble de privilèges associé à un sujet, qui accorde systématiquement au sujet la possibilité de provoquer un transfert pour des informations qui sont couvertes par la SFP qui a été spécifiée. Si une telle possibilité n'est pas souhaitée, alors l'auteur du PP ou de la ST devrait spécifier "aucune".

827 Dans FDP_IFF.2.6, l'auteur du PP ou de la ST devrait spécifier les règles, en fonction des attributs de sécurité, qui refusent explicitement des flux d'information. Ces règles viennent en complément de celles spécifiées dans les éléments précédents. Elles figurent dans FDP_IFF.2.6 car elles sont destinées à contenir des exceptions aux règles définies dans les éléments précédents. Les règles pour autoriser explicitement des flux d'information

sont par exemple fonction d'un ensemble de privilèges associé à un sujet, qui refuse systématiquement au sujet la possibilité de provoquer un transfert pour des informations qui sont couvertes par la SFP qui a été spécifiée. Si une telle possibilité n'est pas souhaitée, alors l'auteur du PP ou de la ST devrait spécifier "aucune".

FDP_IFF.3 Flux d'information illicites limités

Notes d'application pour l'utilisateur

828 Ce composant devrait être utilisé quand au moins une des SFP exigeant le contrôle de flux d'information illicites n'exige pas l'élimination des flux.

829 Pour les flux d'information illicites spécifiés, certaines capacités maximales devraient être indiquées. De plus, un auteur de PP ou de ST a la possibilité de spécifier si les flux d'information illicites doivent être audités.

Opérations

Affectation :

830 **Dans FDP_IFF.3.1, l'auteur du PP ou de la ST devrait spécifier les SFP de contrôle de flux d'information appliquées par la TSF. Le nom de la SFP de contrôle de flux d'information et son domaine d'application sont définis dans les composants de la famille FDP_IFC.**

831 **Dans FDP_IFF.3.1, l'auteur du PP ou de la ST devrait spécifier les types de flux d'information illicites qui font l'objet d'une limitation de capacité maximale.**

832 **Dans FDP_IFF.3.1, l'auteur du PP ou de la ST devrait spécifier la capacité maximale permise pour tout flux d'information illicite identifié.**

FDP_IFF.4 Élimination partielle des flux d'information illicites

Notes d'application pour l'utilisateur

833 Ce composant devrait être utilisé quand toutes les SFP qui exigent le contrôle de flux d'information illicites exigent l'élimination de certains flux d'information illicites (mais pas nécessairement de tous).

Opérations

Affectation :

834 Dans FDP_IFF.4.1, l'auteur du PP ou de la ST devrait spécifier les SFP de contrôle de flux d'information appliquées par la TSF. Le nom de la SFP de

contrôle de flux d'information et son domaine d'application sont définis dans les composants de la famille FDP_IFC.

835 Dans FDP_IFF.4.1, l'auteur du PP ou de la ST devrait spécifier les types de flux d'information illicites qui font l'objet d'une limitation de capacité maximale.

836 Dans FDP_IFF.4.1, l'auteur du PP ou de la ST devrait spécifier la capacité maximale permise pour tout flux d'information illicite identifié.

837 **Dans FDP_IFF.4.2, l'auteur du PP ou de la ST devrait spécifier les types de flux d'information illicites qui doivent être éliminés. Cette liste ne peut pas être vide car ce composant exige que certains flux d'information illicites doivent être éliminés.**

FDP_IFF.5 Aucun flux d'information illicite

Notes d'application pour l'utilisateur

838 Ce composant devrait être utilisé quand les SFP qui exigent le contrôle de flux d'information illicites exigent l'élimination de tous les flux d'information illicites. Cependant, l'auteur du PP ou de la ST devrait soigneusement envisager l'impact potentiel que pourrait avoir l'élimination de tous les flux d'information illicites sur le fonctionnement normal de la TOE. De nombreuses applications pratiques ont démontré qu'il existe une relation indirecte entre les flux d'information illicites et les fonctionnalités normales dans une TOE, et l'élimination de tous les flux d'information illicites peut avoir pour résultat l'apparition d'une fonctionnalité pas du tout souhaitée.

Opérations

Affectation :

839 **Dans FDP_IFF.5.1, l'auteur du PP ou de la ST devrait spécifier la SFP de contrôle de flux d'information pour laquelle les flux d'information illicites doivent être éliminés. Le nom de la SFP de contrôle de flux d'information et le domaine d'application pour cette politique sont définis dans composants de FDP_IFC.**

FDP_IFF.6 Contrôle des flux d'information illicites

Notes d'application pour l'utilisateur

840 Ce composant devrait être utilisé quand on souhaite que la TSF offre la possibilité de contrôler l'utilisation de flux d'information illicites qui dépassent une capacité spécifiée. Si l'on souhaite que de tels flux soient audités, alors ce composant pourrait servir de source d'événements d'audit à exploiter par des composants de la famille FAU_GEN Génération des données de l'audit de sécurité.

Opérations

Affectation :

841 **Dans FDP_IFF.6.1, l'auteur du PP ou de la ST devrait spécifier les SFP de contrôle de flux d'information appliquées par la TSF. Le nom de la SFP de contrôle de flux d'information et le domaine d'application pour cette politique sont définis dans composants de FDP_IFC.**

842 **Dans FDP_IFF.6.1, l'auteur du PP ou de la ST devrait spécifier la liste de types de flux d'information illicites qui seront contrôlés pour qu'ils ne dépassent pas une capacité maximale.**

843 **Dans FDP_IFF.6.1, l'auteur du PP ou de la ST devrait spécifier la capacité maximale au delà de laquelle les flux d'information illicites seront contrôlés par la TSF.**

F.7 Importation depuis une zone hors du contrôle de la TSF (FDP_ITC)

844 La présente famille définit des mécanismes pour importer des données de l'utilisateur à partir d'une zone située hors du TSC dans la TOE de telle façon que les attributs de sécurité des données de l'utilisateur puissent être préservés. La cohérence des attributs de sécurité est traitée par la famille "FPT_TDC Cohérence des données de la TSF inter-TSF".

845 La famille FDP_ITC couvre les limitations d'importation, la spécification par l'utilisateur d'attributs de sécurité, et l'association d'attributs de sécurité aux données de l'utilisateur.

Notes pour l'utilisateur

846 Cette famille, ainsi que la famille correspondante pour l'exportation FDP_ETC, aborde la façon dont la TOE traite les données de l'utilisateur qui échappent à son contrôle. Cette famille concerne l'attribution et l'extraction des attributs de sécurité des données de l'utilisateur.

847 Plusieurs activités pourraient être impliquées ici :

a) l'importation de données de l'utilisateur en provenance d'un support non formaté (e.g. une disquette, une bande magnétique, un scanner, un signal vidéo ou audio), sans inclure aucun attribut de sécurité, et le marquage physique du support pour indiquer son contenu ;

b) l'importation de données de l'utilisateur, avec ses attributs de sécurité, depuis un support et la vérification que les attributs de sécurité de l'objet sont appropriés ;

c) l'importation de données de l'utilisateur, avec ses attributs de sécurité, depuis un support utilisant une technique de scellement cryptographique pour protéger l'association des données de l'utilisateur et de ses attributs de sécurité.

848 Cette famille n'est pas concernée par le fait de déterminer si les données de l'utilisateur peuvent être importées. Elle est concernée par les valeurs des attributs de sécurité à associer aux données de l'utilisateur importées.

849 Il existe deux possibilités pour l'importation de données de l'utilisateur : soit les données de l'utilisateur sont associées de façon non ambiguë à des attributs de sécurité fiables d'un objet (les valeurs et la signification des attributs de sécurité ne sont pas modifiées), soit aucun attribut de sécurité fiable (ou aucun attribut de sécurité) n'est disponible depuis l'origine de l'importation. Cette famille traite des deux cas.

850 S'il n'existe pas d'attributs de sécurité fiables disponibles, ils peuvent avoir été associés aux données de l'utilisateur par un moyen physique (les attributs de

sécurité sont sur le même support), ou par un moyen logique (les attributs de sécurité sont distribués de façon différente, mais ils incluent une identification unique de l'objet, e.g. une somme de contrôle cryptographique).

851 Cette famille concerne l'importation de données de l'utilisateur et la maintenance de l'association d'attributs de sécurité comme cela est exigé par la SFP. D'autres familles couvrent d'autres aspects de l'importation tels que la cohérence, les canaux de confiance et l'intégrité qui sont en dehors du champ d'application de cette famille. De plus, la famille FDP_ITC n'est concernée que par l'interface avec le medium d'importation. La famille FDP_ETC est responsable de l'autre extrémité du medium (l'origine).

852 Certaines des exigences bien connues pour l'importation concernent :

a) l'importation de données de l'utilisateur sans aucun attribut de sécurité ;

b) l'importation de données de l'utilisateur avec des attributs de sécurité, les deux étant associés et les attributs de sécurité représentant de façon non ambiguë les informations importées.

853 Ces exigences d'importation peuvent être gérées par la TSF avec ou sans intervention humaine, en fonction des limitations TI et de la politique de sécurité organisationnelle. Par exemple, si des données de l'utilisateur sont reçues sur un canal "confidentiel", les attributs de sécurité des objets se verront attribuer le niveau "confidentiel".

854 S'il existe plusieurs SFP (de contrôle d'accès ou de contrôle de flux d'information) alors il peut se révéler approprié d'itérer ces composants une fois pour chaque SFP désignée.

FDP_ITC.1 Importation de données de l'utilisateur sans attributs de sécurité

Notes d'application pour l'utilisateur

855 Ce composant est utilisé pour spécifier l'importation de données de l'utilisateur qui ne possèdent pas d'attributs de sécurité fiables (ou pas d'attributs du tout) associés. Cette fonction exige que les attributs de sécurité pour les données de l'utilisateur importées soient initialisés dans la TSF. Il peut aussi advenir que l'auteur du PP ou de la ST spécifie les règles pour l'importation. Dans certains environnements, il peut se révéler approprié d'exiger que ces attributs soient distribués via un chemin de confiance ou un mécanisme de canal de confiance.

Opérations

Affectation :

856 **Dans FDP_ITC.1.1, l'auteur du PP ou de la ST devrait spécifier la SFP de contrôle d'accès ou la SFP de contrôle de flux d'information qui sera appliquée lors de l'importation des données de l'utilisateur en**

provenance d'une zone située hors du TSC. Les données de l'utilisateur que cette fonction importe sont délimitées par l'affectation de ces SFP.

857 **Dans FDP_ITC.1.3, l'auteur du PP ou de la ST devrait spécifier toutes les règles de contrôle d'importation supplémentaires ou "aucune" s'il n'y un pas de règles de contrôle d'importation supplémentaires. Ces règles seront appliquées par la TSF en complément des SFP de contrôle d'accès ou des SFP de contrôle de flux d'information sélectionnées dans FDP_ITC.1.1.**

FDP_ITC.2 Importation de données de l'utilisateur avec attributs de sécurité

Notes d'application pour l'utilisateur

858 Ce composant est utilisé pour spécifier l'importation de données de l'utilisateur qui possèdent des attributs de sécurité fiables associés. Cette fonction s'appuie sur les attributs de sécurité qui sont associés précisément et sans ambiguïté aux objets sur le medium d'importation. Après avoir été importés, ces objets posséderont ces même attributs. Cela exige que la famille FPT_TDC garantisse la cohérence des données. Il pourrait aussi advenir que l'auteur du PP ou de la ST spécifie les règles d'importation.

Opérations

Affectation :

859 **Dans FDP_ITC.2.1, l'auteur du PP ou de la ST devrait spécifier la SFP de contrôle d'accès ou la SFP de contrôle de flux d'information qui sera appliquée lors de l'importation des données de l'utilisateur en provenance d'une zone située hors du TSC. Les données de l'utilisateur que cette fonction importe sont délimitées par l'affectation de ces SFP.**

860 **Dans FDP_ITC.2.5, l'auteur du PP ou de la ST devrait spécifier toutes les règles de contrôle d'importation supplémentaires ou "aucune" s'il n'y un pas de règles de contrôle d'importation supplémentaires. Ces règles seront appliquées par la TSF en complément des SFP de contrôle d'accès ou des SFP de contrôle de flux d'information sélectionnées dans FDP_ITC.2.1.**

F.8 Transfert interne à la TOE (FDP_ITT)

861 La présente famille fournit des exigences qui concernent la protection de données de l'utilisateur lorsqu'elles sont transférées entre des parties d'une TOE via un canal interne. Elle peut différer des familles FDP_UCT et FDP_UIT, qui procurent une protection pour des données de l'utilisateur lors d'un transfert entre des TSF distinctes via un canal externe, ainsi que des familles FDP_ETC et FDP_ITC, qui traitent du transfert de données en direction ou en provenance d'une zone située hors du contrôle de la TSF.

Notes pour l'utilisateur

862 Les exigences de cette famille permettent à un auteur de PP ou de ST de spécifier la sécurité souhaitée pour des données de l'utilisateur en transit dans la TOE. Cette sécurité pourrait consister en une protection contre la divulgation, la modification, ou la perte de disponibilité.

863 La détermination du degré de séparation physique sur laquelle cette famille devrait s'appuyer dépend de l'environnement d'utilisation prévu. Dans un environnement hostile, il peut y avoir des risques liés à des transferts entre des parties de la TOE séparées seulement par un bus système. Dans des environnements moins hostiles, les transferts peuvent se faire via des moyens plus traditionnels.

864 S'il y a plusieurs SFP (de contrôle d'accès ou de contrôle de flux d'information), alors il peut se révéler approprié d'itérer ces composants une fois pour chaque SFP désignée.

FDP_ITT.1 Protection élémentaire d'un transfert interne

Opérations

Affectation :

865 **Dans FDP_ITT.1.1, l'auteur du PP ou de la ST devrait spécifier le ou les SFP de contrôle d'accès ou SFP de contrôle de flux d'information s'appliquant aux informations qui sont transférées.**

Sélection :

866 **Dans FDP_ITT.1.1, l'auteur du PP ou de la ST devrait spécifier les types d'erreurs de transmission que la TSF devrait empêcher pendant le transport de données de l'utilisateur. Les options sont les suivantes : divulgation, modification, perte d'utilisation.**

FDP_ITT.2 Séparation de données au cours d'une transmission en fonction d'attributs

Notes d'application pour l'utilisateur

867 Ce composant pourrait par exemple être utilisé pour procurer différentes formes de protection à des informations ayant des niveaux de classification différents.

868 Une des façons d'accomplir la séparation de données quand elles sont transmises est d'utiliser des canaux logiques ou physiques séparés.

Opérations

Affectation :

869 Dans FDP_ITT.2.1, l'auteur du PP ou de la ST devrait spécifier le ou les SFP de contrôle d'accès ou SFP de contrôle de flux d'information s'appliquant aux informations qui sont transférées.

Sélection :

870 Dans FDP_ITT.2.1, l'auteur du PP ou de la ST devrait spécifier les types d'erreurs de transmission que la TSF devrait empêcher pendant le transport de données de l'utilisateur. Les options sont les suivantes : divulgation, modification, perte d'utilisation.

Affectation :

871 **Dans FDP_ITT.2.2, l'auteur du PP ou de la ST devrait spécifier les attributs de sécurité dont la TSF utilisera les valeurs pour déterminer s'il y a lieu de séparer des données qui sont transmises entre des parties de la TOE physiquement séparées. Par exemple, les données de l'utilisateur associées à l'identité d'un propriétaire sont transmises séparément des données de l'utilisateur associées à l'identité d'un propriétaire différent. Dans ce cas, la valeur "identité du propriétaire des données" est celle qui est utilisée pour déterminer s'il y a lieu de séparer les données pour la transmission.**

FDP_ITT.3 Contrôle de l'intégrité

Notes d'application pour l'utilisateur

872 Ce composant est utilisé en combinaison soit avec le composant FDP_ITT.1 soit avec FDP_ITT.2. Il garantit que la TSF vérifie l'intégrité des données de l'utilisateur reçues (avec leurs attributs). FDP_ITT.1 ou FDP_ITT.2 permet de fournir les données d'une manière telle qu'elles sont protégées contre une modification (pour que FDP_ITT.3 puisse détecter toute modification).

873 L'auteur du PP ou de la ST doit spécifier les types d'erreurs qui doivent être détectées. L'auteur du PP ou de la ST devrait prendre en compte : une modification de données, une substitution de données, un changement irrécupérable dans

l'ordonnancement de données, un rejeu de données, des données incomplètes, en complément à d'autres erreurs d'intégrité.

874 L'auteur du PP ou de la ST doit spécifier les actions que la TSF devrait entreprendre après détection d'une défaillance, par exemple : ignorer les données de l'utilisateur, demander les données à nouveau, informer l'administrateur autorisé, rediriger le trafic par d'autres lignes.

Opérations

Affectation :

875 **Dans FDP_ITT.3.1, l'auteur du PP ou de la ST devrait spécifier la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information s'appliquant aux informations qui sont transférées et contrôlées vis-à-vis d'erreurs d'intégrité.**

876 **Dans FDP_ITT.3.1, l'auteur du PP ou de la ST devrait spécifier le type d'erreurs d'intégrité possibles à contrôler pendant la transmission des données de l'utilisateur.**

877 **Dans FDP_ITT.3.2, l'auteur du PP ou de la ST devrait spécifier l'action à entreprendre par la TSF quand une erreur d'intégrité est découverte. Par exemple la TSF devrait demander que les données de l'utilisateur soient soumises à nouveau. La ou les SFP spécifiées dans FDP_ITT.3.1 seront appliquées quand les actions seront entreprises par la TSF.**

FDP_ITT.4 Contrôle de l'intégrité basé sur des attributs

878 Ce composant est utilisé en combinaison avec FDP_ITT.2. Il garantit que la TSF vérifie l'intégrité des données de l'utilisateur reçues, qui ont été transmises par des canaux séparés (en fonction des valeurs prises par des attributs de sécurité spécifiés). Il permet à l'auteur du PP ou de la ST de spécifier les actions à entreprendre après détection d'une erreur d'intégrité.

879 Par exemple, ce composant pourrait être utilisé pour permettre la détection de différentes erreurs d'intégrité et pour entreprendre l'action correspondante sur l'information à différents niveaux d'intégrité.

880 L'auteur du PP ou de la ST doit spécifier les types d'erreurs qui doivent être détectées. L'auteur du PP ou de la ST devrait prendre en compte : une modification de données, une substitution de données, un changement irrécupérable dans l'ordonnancement de données, un rejeu de données, des données incomplètes, en complément à d'autres erreurs d'intégrité.

881 L'auteur du PP ou de la ST devrait spécifier les attributs (et les canaux de transmission associés) qui nécessitent un contrôle des erreurs d'intégrité.

882 L'auteur du PP ou de la ST doit spécifier les actions que la TSF devrait entreprendre après détection d'une défaillance, par exemple : ignorer les données de l'utilisateur,

demander les données à nouveau, informer l'administrateur autorisé, rediriger le trafic par d'autres lignes.

Opérations

Affectation :

883 Dans FDP_ITT.4.1, l'auteur du PP ou de la ST devrait spécifier la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information s'appliquant aux informations qui sont transférées et contrôlées vis-à-vis d'erreurs d'intégrité.

884 Dans FDP_ITT.4.1, l'auteur du PP ou de la ST devrait spécifier le type d'erreurs d'intégrité possibles à contrôler pendant la transmission des données de l'utilisateur.

885 **Dans FDP_ITT.4.1, l'auteur du PP ou de la ST devrait spécifier une liste d'attributs de sécurité qui exigent des canaux de transmission séparés. Cette liste est utilisée pour déterminer quelles sont les données de l'utilisateur à contrôler vis-à-vis des erreurs d'intégrité, en fonction de leurs attributs de sécurité et du canal de transmission qu'elles ont emprunté. Cet élément est directement relié au composant FDP_ITT.2 Séparation de données au cours d'une transmission en fonction d'attributs.**

886 Dans FDP_ITT.4.2, l'auteur du PP ou de la ST devrait spécifier l'action à entreprendre par la TSF quand une erreur d'intégrité est découverte. Par exemple la TSF devrait demander que les données de l'utilisateur soient soumises à nouveau. La ou les SFP spécifiées dans FDP_ITT.3.1 seront appliquées quand les actions seront entreprises par la TSF.

F.9 Protection des informations résiduelles (FDP_RIP)

887 La présente famille répond au besoin de garantir que les informations détruites ne seront plus accessibles, et que des objets nouvellement créés ne contiennent pas d'informations venant d'objets utilisés précédemment dans la TOE. Cette famille ne traite pas des objets stockés hors ligne.

Notes pour l'utilisateur

888 Cette famille exige la protection des informations qui ont été logiquement supprimées ou libérées (non disponibles pour l'utilisateur mais encore présentes dans le système et pouvant être récupérées). En particulier, cela inclut les informations qui sont contenues dans un objet, faisant partie des ressources réutilisables de la TSF, où la destruction de l'objet ne signifie pas nécessairement la destruction de la ressource ou d'une partie quelconque de la ressource.

889 Elle s'applique également à des ressources qui sont réutilisées en série par différents sujets dans le système. Par exemple, la plupart des systèmes d'exploitation utilisent typiquement des registres "hardware" (des ressources) pour le support de processus dans le système. Quand les processus sont basculés d'un état "actif" vers un état "dormant" (et vice versa), ces registres sont réutilisées en série par différents sujets. Comme cette action de bascule (swapping) ne peut pas être considérée comme une allocation ou une désallocation d'une ressource, la famille FDP_RIP pourrait s'appliquer à de tels événements et ressources.

890 La famille FDP_RIP contrôle typiquement l'accès à des informations qui ne font pas partie d'un objet actuellement défini ou accessible ; cependant, dans certain cas cela peut ne pas être vrai. Par exemple, l'objet "A" est un fichier et l'objet "B" est le disque sur lequel réside ce fichier. Si l'objet "A" est supprimé, les informations de l'objet "A" sont contrôlées par FDP_RIP même s'il fait encore partie de l'objet "B".

891 Il est important de noter que la famille FDP_RIP ne s'applique qu'à des objets en ligne et non à des objets hors ligne tels que ceux sauvegardés sur des bandes magnétiques. Par exemple, si un fichier est supprimé dans la TOE, FDP_RIP peut être instanciée pour exiger qu'aucune information résiduelle n'existe après la désallocation ; cependant, la TSF ne peut pas étendre cette exigence à ce même fichier qui se trouve sur une sauvegarde hors ligne. Par conséquent ce même fichier est encore disponible. Si cela constitue une préoccupation, alors l'auteur du PP ou de la ST devrait s'assurer que des objectifs environnementaux corrects sont définis pour soutenir un guide administratif destiné à couvrir les objets hors ligne.

892 Les familles FDP_RIP et FDP_ROL peuvent entrer en conflit quand FDP_RIP est instanciée pour exiger que des informations résiduelles soient effacées au moment où l'application redonne le contrôle de l'objet à la TSF (i.e. après désallocation). Par conséquent, la sélection par FDP_RIP de l'option "désallocation" ne devrait pas être utilisée avec FDP_ROL puisqu'il n'y aurait pas d'informations sur lesquelles effectuer une annulation. L'autre sélection, "non disponibilité après allocation", peut être utilisée avec FDP_ROL, mais il existe un risque que la ressource qui

possède les informations ait été allouée à un nouvel objet avant que l'annulation n'ait eu lieu. Si cela devait arriver, alors ce dernier ne serait pas possible.

893 Il n'y a pas d'exigences d'audit dans FDP_RIP car ce n'est pas une fonction appelable par l'utilisateur. L'audit de l'allocation ou de la désallocation de ressources serait auditable dans le cadre de la SFP de contrôle d'accès ou de la SFP de contrôle de flux d'information.

894 Cette famille devrait s'appliquer aux objets spécifiés dans la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information telles que spécifiées par l'auteur du PP ou de la ST.

FDP_RIP.1 Protection partielle des informations résiduelles

Notes d'application pour l'utilisateur

895 Ce composant exige que, pour un sous-ensemble d'objets de la TOE, la TSF garantisse qu'il n'y ait plus d'informations résiduelles disponibles contenues dans une ressource allouée à ces objets ou désallouée de ces objets.

Opérations

Sélection :

896 **Dans FDP_RIP.1.1, l'auteur du PP ou de la ST devrait spécifier l'événement, allocation de la ressource ou désallocation de la ressource, qui fait appel à la fonction de protection des informations résiduelles.**

Affectation :

897 **Dans FDP_RIP.1.1, l'auteur du PP ou de la ST devrait spécifier la liste des objets soumis à la protection des informations résiduelles.**

FDP_RIP.2 Protection totale des informations résiduelles

Notes d'application pour l'utilisateur

898 Ce composant exige que, pour **tous les objets** de la TOE, la TSF garantisse qu'il n'y ait plus d'informations résiduelles disponibles contenues dans une ressource allouée à ces objets ou désallouée de ces objets.

Opérations

Sélection :

899 Dans FDP_RIP.2.1, l'auteur du PP ou de la ST devrait spécifier l'événement, allocation de la ressource ou désallocation de la ressource, qui fait appel à la fonction de protection des informations résiduelles.

F.10 Annulation (FDP_ROL)

900 La présente famille répond au besoin de retourner dans un état valide bien défini, tel que le besoin d'un utilisateur d'annuler des modifications à un fichier ou d'annuler des transactions dans le cas de suites incomplètes de transactions comme avec des bases de données.

901 Cette famille est destinée à assister un utilisateur pour le retour dans un état valide bien défini après qu'il ait annulé le dernier ensemble d'actions ou, dans des bases de données distribuées, pour le retour de tous les exemplaires des bases de données distribuées dans l'état existant avant qu'une opération ait échoué.

902 FDP_RIP et FDP_ROL entrent en conflit quand FDP_RIP exige que le contenu soit rendu indisponible au moment où une ressource est désallouée d'un objet. Par conséquent, cette utilisation de FDP_RIP ne peut pas être combinée avec FDP_ROL puisqu'il n'y aurait pas d'informations sur lesquelles effectuer une annulation. La famille FDP_RIP peut être utilisée seulement avec FDP_ROL lorsqu'elle exige que le contenu doit être indisponible au moment où une ressource est allouée à un objet, parce que le mécanisme de FDP_ROL a la possibilité d'accéder aux informations précédentes qui peuvent encore être présentes dans la TOE afin d'annuler l'opération avec succès.

903 L'exigence d'annulation est encadrée par certaines limites. Par exemple, un éditeur de texte ne permet typiquement l'annulation que d'un certain nombre de commandes. On pourrait choisir comme autre exemple les sauvegardes : si des bandes de sauvegardes sont recyclées, une fois qu'une bande a été réutilisée, les informations ne peuvent plus être récupérées. Cela délimite également l'exigence d'annulation.

FDP_ROL.1 Annulation élémentaire

Notes d'application pour l'utilisateur

904 Ce composant permet à un utilisateur ou à un sujet d'annuler un ensemble d'opérations sur un ensemble d'objets prédéfini. L'annulation est seulement possible dans certaines limites, par exemple pour un certain nombre de caractères ou pour une certaine période de temps.

Opérations

Affectation :

905 **Dans FDP_ROL.1.1, l'auteur du PP ou de la ST devrait spécifier la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information qui seront appliquées en exécutant des opérations**

d'annulation. Cela est nécessaire pour assurer que l'annulation n'est pas utilisée pour contourner les SFP spécifiées.

906 **Dans FDP_ROL.1.1, l'auteur du PP ou de la ST devrait spécifier la liste d'opérations qui peuvent être annulées.**

907 **Dans FDP_ROL.1.1, l'auteur du PP ou de la ST devrait spécifier la liste d'objets qui sont soumis à la politique d'annulation.**

908 **Dans FDP_ROL.1.2, l'auteur du PP ou de la ST devrait spécifier la limite dans laquelle des opérations d'annulation peuvent être exécutées. La limite peut être spécifiée en terme de période de temps prédéfinie ; par exemple, des opérations qui ont été exécutées dans les deux dernières minutes peuvent être annulées. D'autres limites possibles peuvent être définies en termes de nombre maximum d'opérations autorisées ou de taille de mémoire tampon.**

FDP_ROL.2 Annulation avancée

Notes d'application pour l'utilisateur

909 Ce composant exige que la TSF offre la possibilité d'annuler toutes les opérations ; cependant, l'utilisateur peut choisir d'annuler seulement une part d'entre elles.

Opérations

Affectation :

910 Dans FDP_ROL.2.1, l'auteur du PP ou de la ST devrait spécifier la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information qui seront appliquées en exécutant des opérations d'annulation. Cela est nécessaire pour assurer que l'annulation n'est pas utilisée pour contourner les SFP spécifiées.

911 Dans FDP_ROL.2.1, l'auteur du PP ou de la ST devrait spécifier la liste d'objets qui sont soumis à la politique d'annulation.

912 Dans FDP_ROL.2.2, l'auteur du PP ou de la ST devrait spécifier la limite dans laquelle des opérations d'annulation peuvent être exécutées. La limite peut être spécifiée en terme de période de temps prédéfinie ; par exemple, des opérations qui ont été exécutées dans les deux dernières minutes peuvent être annulées. D'autres limites possibles peuvent être définies en termes de nombre maximum d'opérations autorisées ou de taille de mémoire tampon.

F.11 Intégrité des données stockées (FDP_SDI)

913 La présente famille fournit des exigences qui concernent la protection de données de l'utilisateur lorsqu'elles sont stockées au sein du TSC.

Notes pour l'utilisateur

914 Des défaillances du matériel ou des erreurs peuvent affecter des données stockées en mémoire. Cette famille fournit des exigences pour détecter ces erreurs non intentionnelles. L'intégrité des données de l'utilisateur stockées dans des dispositifs de stockage dans le TSC est également couverte par cette famille.

915 Pour empêcher un sujet de modifier les données, les familles FDP_IFF ou FDP_ACF sont nécessaires (plutôt que la présente famille).

916 Cette famille diffère de FDP_ITT Transfert interne à la TOE, qui protège les données de l'utilisateur des erreurs d'intégrité pendant leur transfert dans la TOE.

FDP_SDI.1 Contrôle de l'intégrité des données stockées

Notes d'application pour l'utilisateur

917 Ce composant contrôle l'intégrité des données stockées dans des supports. L'auteur du PP ou de la ST peut spécifier différents types d'attributs de données de l'utilisateur qui seront utilisés comme base pour le contrôle.

Opérations

Affectation :

918 **Dans FDP_SDI.1.1, l'auteur du PP ou de la ST devrait spécifier les erreurs d'intégrité que la TSF devra détecter.**

919 **Dans FDP_SDI.1.1, l'auteur du PP ou de la ST devrait spécifier les attributs des données de l'utilisateur qui seront utilisés comme base pour le contrôle.**

FDP_SDI.2 Contrôle de l'intégrité des données stockées et action à entreprendre

Notes d'application pour l'utilisateur

920 Ce composant contrôle l'intégrité des données stockées dans des supports. L'auteur du PP ou de la ST peut spécifier l'action qui devrait être entreprise dans le cas où une erreur d'intégrité est détectée.

Opérations

Affectation :

921 Dans FDP_SDI.2.1, l'auteur du PP ou de la ST devrait spécifier les erreurs d'intégrité que la TSF devra détecter.

922 Dans FDP_SDI.2.1, l'auteur du PP ou de la ST devrait spécifier les attributs des données de l'utilisateur qui seront utilisés comme base pour le contrôle.

923 **Dans FDP_SDI.2.2, l'auteur du PP ou de la ST devrait spécifier les actions à entreprendre dans le cas où une erreur d'intégrité est détectée.**

F.12 Protection de la confidentialité des données de l'utilisateur lors d'un transfert inter-TSF (FDP_UCT)

924 La présente famille définit les exigences pour garantir la confidentialité des données de l'utilisateur lors d'un transfert via un canal externe entre la TOE et un autre produit TI de confiance. La confidentialité est assurée en empêchant la divulgation non autorisée des données de l'utilisateur en transit entre les deux extrémités, qui peuvent être constituées par une TSF ou par un utilisateur.

Notes pour l'utilisateur

925 Cette famille fournit une exigence pour la protection des données de l'utilisateur pendant le transit. En revanche, FTP_ITC gère les données de la TSF.

FDP_UCT.1 Confidentialité élémentaire lors d'un échange de données

Notes d'application pour l'utilisateur

926 La TSF a la possibilité de protéger certaines données de l'utilisateur d'une divulgation, lors d'un échange.

Opérations

Affectation :

927 **Dans FDP_UCT.1.1, l'auteur du PP ou de la ST devrait spécifier la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information qui seront appliquées lors d'un échange de données de l'utilisateur. Les politiques spécifiées seront appliquées pour prendre des décisions relatives aux entités qui peuvent échanger des données et aux données qui peuvent être échangées.**

Sélection :

928 **Dans FDP_UCT.1.1, l'auteur du PP ou de la ST devrait spécifier si cet élément s'applique à un mécanisme qui transmet ou qui reçoit des données de l'utilisateur.**

F.13 Protection de l'intégrité des données de l'utilisateur lors d'un transfert inter-TSF (FDP_UIT)

929 La présente famille définit les exigences pour assurer l'intégrité des données de l'utilisateur en transit entre la TSF et un autre produit TI de confiance, et pour reconstituer les données à partir des erreurs détectables. Au minimum, cette famille contrôle l'intégrité des données de l'utilisateur contre des modifications. De plus, cette famille couvre différents moyens de corriger les erreurs d'intégrité détectées.

Notes pour l'utilisateur

930 Cette famille définit les exigences pour procurer l'intégrité des données de l'utilisateur en transit, alors que FPT_ITI gère les données de la TSF.

931 FDP_UIT et FDP_UCT sont des familles duales, puisque FDP_UCT couvre la confidentialité des données de l'utilisateur. Par conséquent, le même mécanisme qui implémente FDP_UIT pourrait être utilisé pour implémenter d'autres familles telles que FDP_UCT et FDP_ITC.

FDP_UIT.1 Intégrité lors d'un échange de données

Notes d'application pour l'utilisateur

932 La TSF possède la possibilité élémentaire d'envoyer ou de recevoir des données de l'utilisateur d'une manière telle qu'une modification des données de l'utilisateur puisse être détectée. Il n'y a pas d'exigence pour qu'un mécanisme de la TSF essaye de recouvrer les données après modification.

Opérations

Affectation :

933 **Dans FDP_UIT.1.1, l'auteur du PP ou de la ST devrait spécifier la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information qui seront appliquées aux données transmises ou aux données reçues. Les politiques spécifiées seront appliquées pour prendre des décisions relatives aux entités qui peuvent échanger des données et aux données qui peuvent être échangées.**

Sélection :

934 **Dans FDP_UIT.1.1, l'auteur du PP ou de la ST devrait spécifier si cet élément s'applique à une TSF qui transmet ou qui reçoit des objets.**

935 **Dans FDP_UIT.1.1, l'auteur du PP ou de la ST devrait spécifier si les données devraient être protégées contre une modification, une suppression, une insertion ou un rejeu.**

936 **Dans FDP_UIT.1.2, l'auteur du PP ou de la ST devrait spécifier si les erreurs du type modification, suppression, insertion ou rejeu sont détectées.**

FDP_UIT.2 Reconstitution grâce à l'émetteur lors d'un échange de données

Notes d'application pour l'utilisateur

937 Ce composant offre la possibilité de récupérer des données soumises à un ensemble d'erreurs de transmission identifiées, si nécessaire avec l'aide de l'autre produit TI de confiance. Comme l'autre produit TI de confiance est en dehors du TSC, la TSF ne peut pas contrôler son comportement. Cependant, elle peut fournir des fonctions qui ont la possibilité de coopérer avec l'autre produit TI de confiance pour les objectifs de recouvrement. Par exemple, la TSF pourrait inclure des fonctions qui dépendent du produit TI de confiance émetteur pour réexpédier les données dans le cas où une erreur est détectée. Ce composant traite de la possibilité pour la TSF de gérer un tel recouvrement d'erreur.

Opérations

Affectation :

938 **Dans FDP_UIT.2.1, l'auteur du PP ou de la ST devrait spécifier la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information qui seront appliquées pour récupérer des données de l'utilisateur. Les politiques spécifiées seront appliquées pour décider quelles données peuvent être récupérées et comment le faire.**

939 **Dans FDP_UIT.2.1, l'auteur du PP ou de la ST devrait spécifier la liste des erreurs d'intégrité pour laquelle la TSF, avec l'aide du produit TI de confiance émetteur, est capable de récupérer les données de l'utilisateur d'origine.**

FDP_UIT.3 Reconstitution par le destinataire lors d'un échange de données

Notes d'application pour l'utilisateur

940 Ce composant offre la possibilité de récupérer des données soumises à un ensemble d'erreurs de transmission identifiées. Il accomplit cette tâche sans l'aide du produit TI de confiance émetteur. Par exemple, si certaines erreurs sont détectées, le protocole de transmission doit être suffisamment robuste pour permettre à la TSF

de récupérer les données en dépit de l'erreur à l'aide de sommes de contrôle et d'autres informations disponibles dans ce protocole.

Opérations

Affectation :

941 Dans FDP_UIT.3.1, l'auteur du PP ou de la ST devrait spécifier la ou les SFP de contrôle d'accès ou la ou les SFP de contrôle de flux d'information qui seront appliquées pour récupérer des données de l'utilisateur. Les politiques spécifiées seront appliquées pour décider quelles données peuvent être récupérées et comment le faire.

942 Dans FDP_UIT.3.1, l'auteur du PP ou de la ST devrait spécifier la liste des erreurs d'intégrité pour laquelle la TSF **destinataire, seule**, est capable de récupérer les données de l'utilisateur d'origine.

Annexe G
(Informative)

Identification et authentification (FIA)

943 Une exigence de sécurité courante consiste à pouvoir identifier sans ambiguïté la personne ou l'entité qui exécute des fonctions dans une TOE. Ceci implique non seulement d'établir l'identité annoncée de chaque utilisateur, mais aussi de vérifier que chaque utilisateur est vraiment celui qu'il prétend être. Ceci s'obtient en exigeant que les utilisateurs donnent à la TSF certaines informations qui sont connues de la TSF comme étant associées avec l'utilisateur en question.

944 Les familles de la présente classe traitent des exigences pour que des fonctions établissent et contrôlent l'identité annoncée d'un utilisateur. L'identification et l'authentification sont exigées pour garantir que les attributs de sécurité corrects (e.g. identité, groupes, rôles, niveaux de sécurité ou d'intégrité) sont associés aux utilisateurs.

945 L'identification non ambiguë d'utilisateurs autorisés et l'association correcte d'attributs de sécurité à des utilisateurs et à des sujets sont critiques pour l'application des politiques de sécurité.

946 La famille FIA_UID couvre la détermination de l'identité d'un utilisateur.

947 La famille FIA_UAU couvre la vérification de l'identité d'un utilisateur.

948 La famille FIA_AFL couvre la définition de limites au nombre de tentatives d'authentification infructueuses répétées.

949 La famille FIA_ATD couvre la définition des attributs de l'utilisateur qui sont utilisés dans l'application de la TSP.

950 La famille FIA_USB couvre l'association correcte d'attributs de sécurité pour chaque utilisateur autorisé.

951 La famille FIA_SOS couvre la génération et la vérification des secrets qui satisfont une métrique définie.

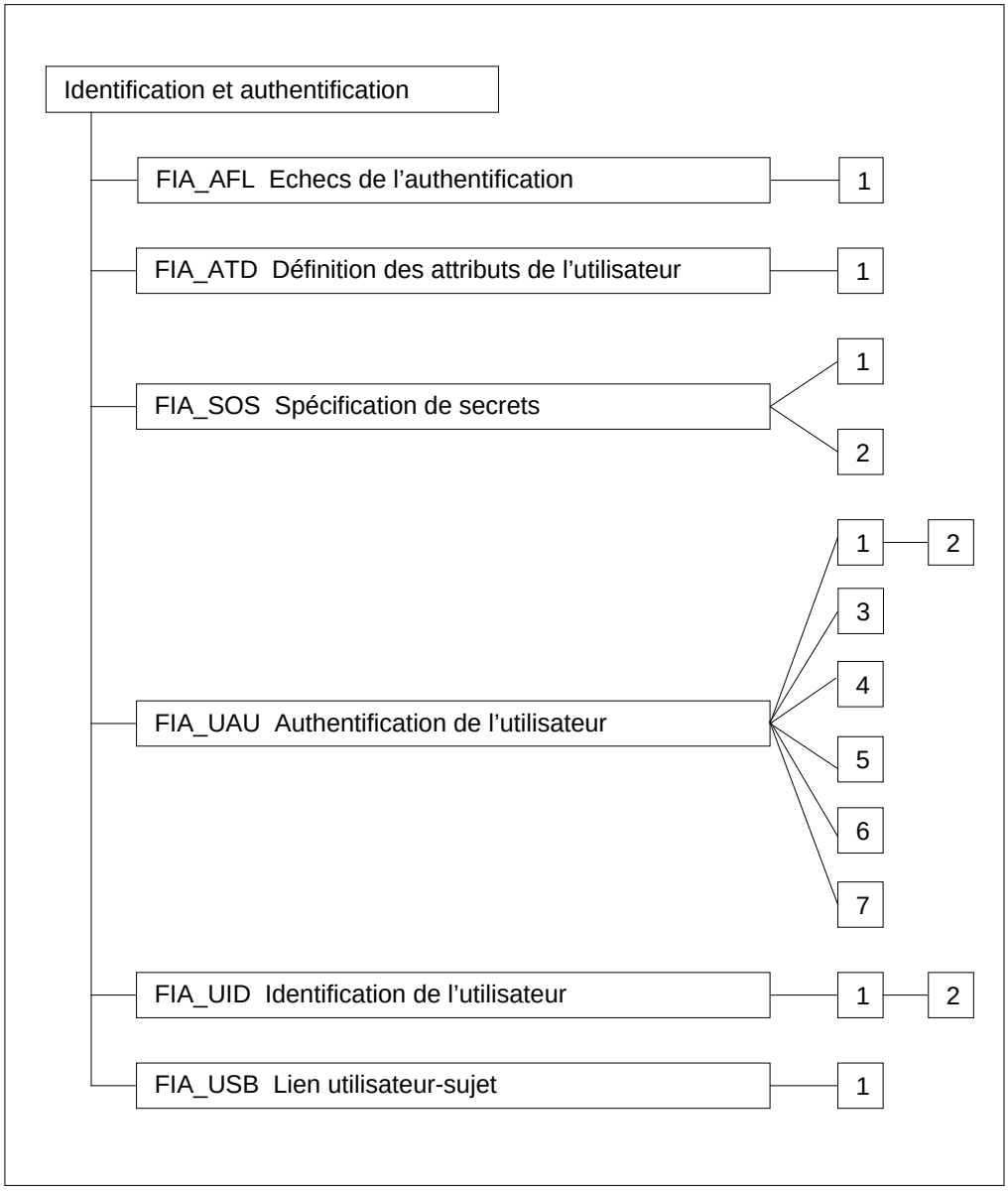


Figure 7.1 - Décomposition de la classe "Identification et authentification"

G.1 Echecs de l'authentification (FIA_AFL)

952 La présente famille contient des exigences pour définir le nombre de tentatives d'authentification et les actions de la TSF dans le cas de tentatives d'authentification infructueuses. Les paramètres comprennent entre autres le nombre de tentatives d'authentification qui ont échoué et des seuils de durée.

953 Le processus d'établissement d'une session est l'interaction avec l'utilisateur dans le but d'effectuer l'établissement d'une session indépendamment de l'implémentation actuelle. Si le nombre de tentatives d'authentification infructueuses dépasse le seuil indiqué, le compte de l'utilisateur ou le terminal (ou bien les deux) seront verrouillés. Si le compte de l'utilisateur est désactivé, l'utilisateur ne peut pas se connecter au système. Si le terminal est désactivé, le terminal (ou l'adresse du terminal) ne peut pas être utilisé pour une connexion. Ces deux situations perdurent jusqu'à ce que la condition de ré-établissement de la session soit satisfaite.

FIA_AFL.1 Gestion d'un échec de l'authentification

Notes d'application pour l'utilisateur

954 L'auteur du PP ou de la ST peut définir le nombre de tentatives d'authentification infructueuses ou peut choisir de laisser le développeur de la TOE ou l'utilisateur autorisé définir ce nombre. Les tentatives d'authentification infructueuses ne doivent pas forcément être consécutives, mais doivent plutôt être reliées à un événement d'authentification. Un tel événement pourrait être le décompte des tentatives d'authentification faisant suite au dernier établissement réussi d'une session sur un terminal donné.

955 L'auteur du PP ou de la ST pourrait spécifier une liste d'actions que la TSF devrait effectuer dans le cas d'une défaillance de l'authentification. Un administrateur autorisé pourrait également être autorisé à gérer les événements, si cela est jugé opportun par l'auteur du PP ou de la ST. Ces actions pourraient consister, entre autres, à désactiver le terminal, le compte utilisateur ou l'alarme de l'administrateur. Les conditions pour lesquelles la situation sera restaurée à la normale doivent être spécifiées avec l'action.

956 Afin d'empêcher un déni de service, les TOE garantissent généralement qu'il existe au moins un compte utilisateur qui ne peut pas être désactivé.

957 L'auteur du PP ou de la ST peut spécifier d'autres actions de la TSF, y compris des règles pour réactiver le processus d'établissement d'une session utilisateur, ou pour envoyer une alarme à l'administrateur. Des exemples de telles actions sont : jusqu'à ce qu'une période de temps spécifiée se soit écoulée, jusqu'à ce que l'administrateur autorisé réactive le terminal ou le compte, une période de temps associée aux précédentes tentatives ayant échouées (chaque fois que la tentative échoue, la période de désactivation est doublée).

Opérations

Affectation :

958 **Dans FIA_AFL.1.1, l'auteur du PP ou de la ST doit spécifier le nombre par défaut de tentatives d'authentification infructueuses qui, lorsqu'il est atteint ou dépassé, déclenchera des actions. L'auteur du PP ou de la ST peut spécifier que ce nombre est "configurable par un administrateur autorisé".**

959 **Dans FIA_AFL.1.1, l'auteur du PP ou de la ST devrait spécifier les événements d'authentification. Des exemples de tels événements sont : les tentatives d'authentification infructueuses depuis la dernière authentification réussie pour l'identité indiquée de l'utilisateur, les tentatives d'authentification infructueuses depuis la dernière authentification réussie pour le terminal considéré, le nombre de tentatives d'authentification infructueuses qui ont eu lieu dans les 10 dernières minutes. Un événement d'authentification au moins doit être spécifié.**

960 **Dans FIA_AFL.1.2, l'auteur du PP ou de la ST devrait spécifier les actions à entreprendre dans le cas où le seuil est atteint ou dépassé. Ces actions pourraient être : la désactivation d'un compte pendant 5 minutes, la désactivation du terminal pendant une durée de plus en plus longue (2 élevé à la puissance du nombre de tentatives infructueuses, exprimé en secondes), ou la désactivation du compte jusqu'à ce que l'administrateur le déverrouille tout en informant simultanément ce dernier. Les actions devraient spécifier les mesures et, le cas échéant, la durée de la mesure (ou les conditions pour lesquelles la mesure prendra fin).**

G.2 Définition des attributs de l'utilisateur (FIA_ATD)

961 Tous les utilisateurs autorisés peuvent avoir un ensemble d'attributs de sécurité, autres que l'identité de l'utilisateur, qui sont utilisés pour appliquer la TSP. La présente famille définit les exigences pour associer les attributs de sécurité aux utilisateurs, dans la mesure où cela est nécessaire pour contribuer à l'application de la TSP.

Notes pour l'utilisateur

962 Il existe des dépendances sur les définitions des politiques de sécurité individuelles. Ces définitions individuelles devraient contenir la liste des attributs qui sont nécessaires pour l'application de la politique.

FIA_ATD.1 Définition des attributs de l'utilisateur

Notes d'application pour l'utilisateur

963 Ce composant spécifie les attributs de sécurité qui devraient être maintenus au niveau de l'utilisateur. Ceci signifie que les attributs de sécurité énumérés sont affectés aux utilisateurs et peuvent être changés à leur niveau. En d'autres termes, le fait de changer un attribut de sécurité figurant dans cette énumération associée à un utilisateur ne devrait avoir aucun impact sur les attributs de sécurité d'un autre utilisateur.

964 Dans le cas où des attributs de sécurité appartiennent à un groupe d'utilisateurs (comme la liste des privilèges pour un groupe), l'utilisateur aura besoin d'avoir une référence (en terme d'attribut de sécurité) au groupe concerné.

Opérations

Affectation :

965 **Dans FIA_ATD.1.1, l'auteur du PP ou de la ST devrait spécifier les attributs de sécurité qui sont associés à un utilisateur individuel. Une telle liste pourrait être par exemple : {'habilitation', 'identifiant de groupe', 'privilèges'}.**

G.3 Spécification de secrets (FIA_SOS)

966 La présente famille définit des exigences pour les mécanismes qui appliquent des métriques de qualité définies aux secrets fournis et qui génèrent des secrets répondant à la métrique définie. De tels mécanismes peuvent inclure par exemple la vérification automatique des mots de passe fournis par les utilisateurs, ou la génération automatique de mots de passe.

967 Un secret peut être généré à l'extérieur de la TOE (e.g. choisi par l'utilisateur et introduit dans le système). Dans de tels cas, le composant FIA_SOS.1 peut être utilisé pour garantir que le secret généré à l'extérieur respecte certaines normes, comme par exemple avoir une taille minimum, ne pas figurer dans un dictionnaire, ou ne pas avoir été utilisé auparavant.

968 Des secrets peuvent également être générés par la TOE. Dans ce cas, le composant FIA_SOS.2 peut être utilisé pour exiger que la TOE garantisse que les secrets respecteront certaines métriques spécifiées.

Notes pour l'utilisateur

969 Des secrets contiennent les données d'authentification fournies par l'utilisateur pour un mécanisme d'authentification qui est basé sur la connaissance de ce que l'utilisateur possède. Lorsque des clés cryptographiques sont employées, la classe FCS devrait être utilisée à la place de cette famille.

FIA_SOS.1 Vérification de secrets

Notes d'application pour l'utilisateur

970 Des secrets peuvent être générés par l'utilisateur. Ce composant garantit que ces secrets peuvent être vérifiés afin de répondent à une certaine métrique de qualité.

Opérations

Affectation :

971 **Dans FIA_SOS.1.1, l'auteur du PP ou de la ST devrait indiquer une métrique de qualité définie. La spécification de la métrique de qualité peut se réduire à une simple description des contrôles qualité qui doivent être effectués, ou être formalisée en référence à une norme gouvernementale publique qui définit les métriques de qualité que doivent respecter les secrets. De telles métriques de qualité pourraient comprendre par exemple la description de la structure alphanumérique ou la taille que des secrets doivent respecter pour être acceptables.**

FIA_SOS.2 Génération de secrets par la TSF

972 Ce composant permet à la TSF de générer des secrets pour des fonctions spécifiques telles que l'authentification au moyen de mots de passe.

Notes d'application pour l'utilisateur

973 Quand un générateur de nombres pseudo-aléatoires est utilisé dans un algorithme de génération de secret, il devrait accepter en entrée des données aléatoires qui donneraient en sortie des données ayant la propriété d'être hautement imprévisibles. Ces données aléatoires (graine) peuvent être élaborées à partir d'un nombre de paramètres disponibles tels que l'horloge système, des registres système, la date, l'heure, etc. Les paramètres devraient être choisis de façon à garantir que le nombre de graines différentes qui peuvent être générées à partir de ces données devrait être au moins égal au nombre minimum de secrets qui doivent être générés.

Opérations

Affectation :

974 **Dans FIA_SOS.2.1, l'auteur du PP ou de la ST devrait indiquer une métrique de qualité définie. La spécification de la métrique de qualité peut se réduire à une simple description des contrôles qualité qui doivent être effectués, ou être formalisée en référence à une norme gouvernementale publique qui définit les métriques de qualité que doivent respecter les secrets. De telles métriques de qualité pourraient comprendre par exemple la description de la structure alphanumérique de secrets acceptables ou la taille que des secrets acceptables doivent respecter.**

975 **Dans FIA_SOS.2.2, l'auteur du PP ou de la ST devrait indiquer une liste de fonctions de la TSF pour lesquelles les secrets générés par la TSF des doivent être utilisés. Une telle fonction pourrait comprendre par exemple un mécanisme d'authentification basé sur un mot de passe.**

G.4 Authentification de l'utilisateur (FIA_UAU)

976 La présente famille définit les types de mécanismes d'authentification de l'utilisateur gérés par la TSF. Cette famille définit également les attributs nécessaires sur lesquels doivent être basés les mécanismes d'authentification de l'utilisateur.

FIA_UAU.1 Programmation de l'authentification

Notes d'application pour l'utilisateur

977 Ce composant exige que l'auteur du PP ou de la ST définisse les actions transitant par la TSF pouvant être effectuées par la TSF pour le compte de l'utilisateur avant que l'identité annoncée de l'utilisateur ne soit authentifiée. Les actions transitant par la TSF ne devraient pas se préoccuper des utilisateurs qui s'identifient de manière incorrecte avant d'être authentifiés. Pour toute autre action transitant par la TSF ne figurant pas dans la liste, l'utilisateur doit être authentifié avant que l'action puisse être effectuée par la TSF pour le compte de l'utilisateur.

978 Ce composant ne peut pas contrôler si les actions peuvent également être effectuées avant que l'identification n'ait eu lieu. Pour cela il est nécessaire d'utiliser FIA_UID.1 ou FIA_UID.2 avec les affectations appropriées.

Opérations

Affectation :

979 **Dans FIA_UAU.1.1, l'auteur du PP ou de la ST devrait spécifier une liste d'actions transitant par la TSF, pouvant être effectuées par la TSF pour le compte d'un utilisateur avant que l'identité annoncée de l'utilisateur ne soit authentifiée. Cette liste ne peut pas être vide. Si aucune action n'est appropriée, alors le composant FIA_UAU.2 devrait être utilisé à la place du présent composant. Une telle action pourrait comprendre par exemple la demande d'aide lors de la procédure de connexion.**

FIA_UAU.2 Authentification de l'utilisateur avant toute action

Notes d'application pour l'utilisateur

980 Ce composant exige que les utilisateurs soient identifiés avant qu'une action transitant par la TSF puisse avoir lieu pour le compte de l'utilisateur.

FIA_UAU.3 Authentification infalsifiable

Notes d'application pour l'utilisateur

981 Ce composant couvre des exigences pour des mécanismes qui offrent une protection des données d'authentification. Les données d'authentification qui sont copiées sur celles d'un autre utilisateur, ou qui sont construites d'une certaine

manière, devraient être détectées ou rejetées. Ces mécanismes procurent la confiance dans le fait que des utilisateurs authentifiés par la TSF sont véritablement ceux qu'ils prétendent être.

982 Ce composant ne peut être utile qu'avec des mécanismes d'authentification qui sont basés sur des données d'authentification qui ne peuvent pas être partagées (e.g. des données biométriques). Il est impossible pour une TSF de détecter ou d'empêcher le partage de mots de passe effectué en dehors de son contrôle.

Opérations

Sélection :

983 **Dans FIA_UAU.3.1, l'auteur du PP ou de la ST devrait spécifier si la TSF sera en mesure de détecter ou d'empêcher, ou de détecter et d'empêcher la falsification de données d'authentification**

984 **Dans FIA_UAU.3.2, l'auteur du PP ou de la ST devrait spécifier si la TSF sera en mesure de détecter ou d'empêcher, ou de détecter et d'empêcher la copie de données d'authentification**

FIA_UAU.4 Mécanismes d'authentification à usage unique

Notes d'application pour l'utilisateur

985 Ce composant couvre des exigences pour des mécanismes d'authentification basés sur des données d'authentification à usage unique. Les données d'authentification à usage unique peuvent être quelque chose que l'utilisateur possède ou connaît, mais pas quelque chose que l'utilisateur est. Des exemples de données d'authentification à usage unique comprennent des mots de passe à usage unique, des horodatages chiffrés, ou des nombres aléatoires issus d'une table de secrets.

986 L'auteur du PP ou de la ST peut spécifier le ou les mécanisme d'authentification auxquels s'applique cette exigence.

Opérations

Affectation :

987 **Dans FIA_UAU.4.1, l'auteur du PP ou de la ST devrait spécifier la liste de mécanismes d'authentification auxquels cette exigence s'applique. Cette affectation peut être 'tous mécanismes d'authentification'. Un autre exemple d'affectcation pourrait être "le mécanisme d'authentification utilisé pour authentifier les personnes d'un réseau extérieur".**

FIA_UAU.5 Mécanismes d'authentification multiple

Notes d'application pour l'utilisateur

988 L'utilisation de ce composant permet la spécification d'exigences pour plusieurs mécanismes d'authentification à utiliser dans une TOE. Pour chaque mécanisme distinct, les exigences applicables doivent être choisies dans la classe FIA pour lui être appliquées. Il est possible que le même composant soit sélectionné plusieurs fois afin de refléter des exigences différentes pour une utilisation différente du mécanisme d'authentification.

989 Les fonctions d'administration de la classe FMT peuvent offrir des possibilités de maintenance pour l'ensemble des mécanismes d'authentification, ainsi que les règles qui déterminent si l'authentification est réussie.

990 Pour permettre à des utilisateurs anonymes de se connecter sur le système, un mécanisme d'authentification 'aucun' peut être incorporé. L'utilisation d'un tel accès devrait être clairement expliqué dans les règles de FIA_UAU.5.2.

Opérations

Affectation :

991 **Dans FIA_UAU.5.1, l'auteur du PP ou de la ST devrait définir les mécanismes d'authentification disponibles. Une telle liste pourrait être par exemple : "aucun, mécanisme de mot de passe, mécanisme biométrique (empreinte rétinienne), mécanisme S/key".**

992 **Dans FIA_UAU.5.2, l'auteur du PP ou de la ST devrait spécifier les règles qui décrivent la façon dont les mécanismes d'authentification procurent l'authentification et le moment où chacun d'entre eux doit être utilisé. Ceci signifie que pour chaque situation, l'ensemble des mécanismes qui pourraient être utilisés pour authentifier l'utilisateur doit être décrit. Une telle liste de règles pourrait être par exemple : "si l'utilisateur possède des privilèges spéciaux, un mécanisme de mot de passe et un mécanisme biométrique devront être utilisés à la fois, l'authentification n'étant réussie que si les deux mécanismes ont réussi ; pour tous les autres utilisateurs, un mécanisme de mot de passe devra être utilisé."**

993 **L'auteur du PP ou de la ST pourrait fixer les limites dans lesquelles l'administrateur autorisé peut spécifier des règles spécifiques. Une règle peut être par exemple : "l'utilisateur devra toujours être authentifié au moyen d'un jeton ; l'administrateur pourrait spécifier des mécanismes d'authentification supplémentaires qui doivent aussi être utilisés." L'auteur du PP ou de la ST pourrait également choisir de ne pas spécifier de limites mais de laisser l'administrateur autorisé choisir entièrement les mécanismes d'authentification et leurs règles.**

FIA_UAU.6 Réauthentification

Notes d'application pour l'utilisateur

994 Ce composant traite des besoins potentiels de réauthentification des utilisateurs à certains moments définis. Cela peut inclure des demandes de l'utilisateur pour que la TSF effectue des actions dédiées à la sécurité, ainsi que des demandes de réauthentification d'entités n'appartenant pas à la TSF (e.g. un serveur d'application demandant que la TSF réauthentifie le client qui est connecté).

Opérations

Affectation :

995 **Dans FIA_UAU.6.1, l'auteur du PP ou de la ST devrait spécifier la liste de conditions exigeant une réauthentification. Cette liste pourrait comprendre l'expiration d'une période d'inactivité spécifiée d'un utilisateur, la demande de l'utilisateur pour changer des attributs de sécurité actifs ou la demande de l'utilisateur pour que la TSF exécute une certaine fonction critique de sécurité.**

996 **L'auteur du PP ou de la ST pourrait indiquer les limites pour lesquelles une réauthentification devrait avoir lieu, et laisser les détails à l'administrateur autorisé. Un exemple d'une telle règle est : "l'utilisateur doit toujours être réauthentifié au moins une fois par jour ; l'administrateur pourrait spécifier que la réauthentification devrait être faite plus souvent mais pas plus d'une fois toutes les 10 minutes."**

FIA_UAU.7 Authentification avec retours protégés

Notes d'application pour l'utilisateur

997 Ce composant couvre le retour du processus d'authentification qui sera fourni à l'utilisateur. Dans certains systèmes, le retour consiste à indiquer combien de caractères ont été tapés mais sans afficher les caractères eux-mêmes, alors que dans d'autres systèmes, mêmes ces informations pourraient ne pas être appropriées.

998 Ce composant exige que les données d'authentification ne soient pas fournies telles quelles à l'utilisateur. Dans un environnement de station de travail, il pourrait afficher un caractère "factice" (e.g. une étoile) pour chaque caractère du mot de passe fourni, et non le caractère originel.

Opérations

Affectation :

999 **Dans FIA_UAU.7.1, l'auteur du PP ou de la ST devrait spécifier le retour relatif au processus d'authentification qui sera fourni à l'utilisateur. Un exemple d'affectation de retour est "le nombre de**

caractères tapés", un autre type de retour est "le mécanisme d'authentification qui a fait échouer l'authentification".

G.5 Identification d'un utilisateur (FIA_UID)

1000 La présente famille définit les conditions auxquelles sont soumis les utilisateurs pour s'identifier avant d'exécuter toute autre action devant transiter par la TSF qui nécessite l'identification de l'utilisateur.

FIA_UID.1 Programmation de l'identification

Notes d'application pour l'utilisateur

1001 Ce composant présente des exigences pour l'utilisateur devant être identifié. L'auteur du PP ou de la ST peut indiquer des actions spécifiques qui peuvent être exécutées avant que l'identification n'ait lieu.

1002 Si FIA_UID.1 est utilisé, les actions transitant par la TSF mentionnées dans FIA_UID.1 devraient également apparaître dans FIA_UAU.1.

Opérations

Affectation :

1003 **Dans FIA_UID.1.1, l'auteur du PP ou de la ST devrait spécifier une liste d'actions transitant par la TSF qui peuvent être exécutées par la TSF pour le compte d'un utilisateur avant que l'utilisateur ne doive s'identifier. Si aucune action n'est appropriée, c'est le composant FIA_UID.2 qui devrait plutôt être utilisé. Une telle action pourrait être par exemple la demande d'aide relative à la procédure de login.**

FIA_UID.2 Identification de l'utilisateur avant toute action

Notes d'application pour l'utilisateur

1004 Dans ce composant, les utilisateurs doivent être identifiés. Un utilisateur n'est pas autorisé par la TSF à exécuter une quelconque action avant d'être identifié.

G.6 Lien utilisateur-sujet (FIA_USB)

1005 Un utilisateur authentifié active habituellement un sujet afin d'utiliser la TOE. Les attributs de sécurité de l'utilisateur sont associés (en totalité ou en partie) à ce sujet. La présente famille définit des exigences pour créer et maintenir la relation entre les attributs de sécurité de l'utilisateur et un sujet agissant pour le compte de cet utilisateur.

FIA_USB.1 Lien utilisateur-sujet

Notes d'application pour l'utilisateur

1006 L'expression "agir pour le compte de" s'est révélée être un sujet prêtant à des contentieux dans les critères précédents. Il est convenu qu'un sujet agit pour le compte de l'utilisateur qui a amené le sujet à être créé ou à être activé en vue d'accomplir une certaine tâche. Par conséquent, lorsqu'un sujet est créé, ce sujet agit pour le compte de l'utilisateur qui est à l'origine de sa création. Dans le cas où l'anonymat est utilisé, le sujet agit toujours pour le compte d'un utilisateur, mais l'identité de l'utilisateur est inconnue. Une catégorie spéciale rassemble les sujets qui agissent pour le compte de plusieurs utilisateurs (e.g un processus serveur). Dans de tels cas, l'utilisateur qui a créé ce sujet est supposé être le 'propriétaire'.

Annexe H
(Informative)

Administration de la sécurité (FMT)

1007 La présente classe est destinée à définir l'administration de plusieurs aspects de la TSF : attributs de sécurité, données et fonctions de la TSF. Les différents rôles d'administration et leurs interactions, comme par exemple la séparation des privilèges, peuvent également être spécifiés.

1008 Dans un environnement où la TOE est faite de plusieurs parties physiquement séparées qui forment un système distribué, les problèmes temporels relatifs à la transmission d'attributs de sécurité, de données de la TSF et de modification de fonctions deviennent très complexes, surtout si les informations doivent être dupliquées dans les parties de la TOE. Cela devrait être pris en compte pour le choix de composants tels que FMT_REV.1 Révocation, ou FMT_SAE.1 Autorisation limitée dans le temps, là où le comportement pourrait en être affecté. Dans de telles situations, l'utilisation de composants de la famille FPT_TRC est conseillée.

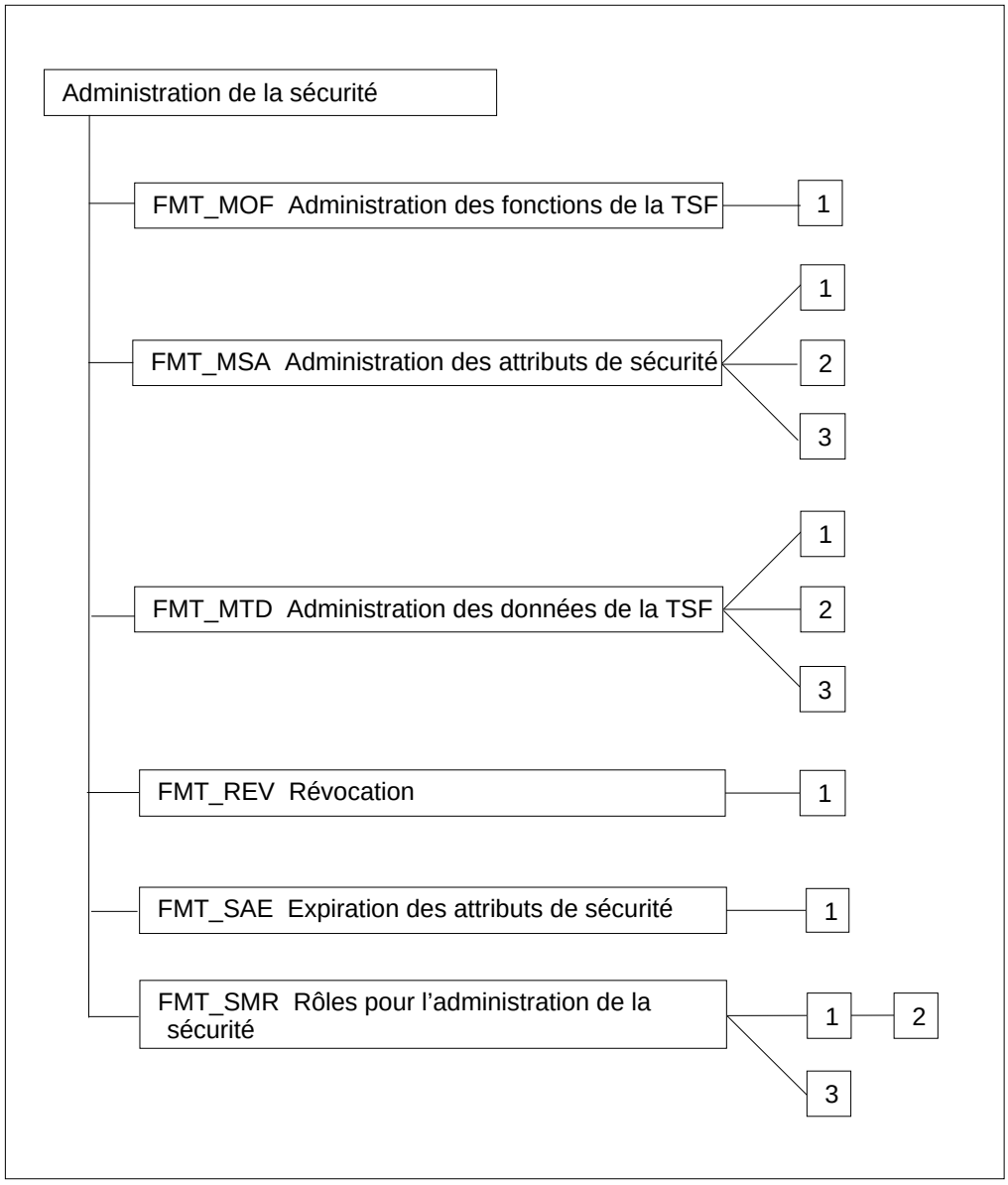


Figure 8.1 - Décomposition de la classe "Administration de la sécurité"

H.1 Administration des fonctions dans la TSF (FMT_MOF)

1009 Les fonctions d'administration de la TSF permettent à des utilisateurs autorisés de mettre en oeuvre et de contrôler le fonctionnement sécurisé de la TOE. Ces fonctions organisationnelles relèvent typiquement d'un certain nombre de catégories différentes :

a) fonctions d'administration qui se rapportent au contrôle d'accès, à l'imputabilité et aux contrôles d'authentification appliqués par la TOE. Par exemple, la définition et la mise à jour de caractéristiques de sécurité de l'utilisateur (e.g. des identifiants uniques associés aux noms des utilisateur, des comptes utilisateur, des paramètres d'entrée au système) ou la définition et la mise à jour de contrôles d'audit de système (e.g. la sélection d'événements d'audit, l'administration de trace d'audits, l'analyse de trace d'audit et la génération de rapport d'audit), la définition et la mise à jour de politiques d'attributs par utilisateur (telle que l'habilitation d'un utilisateur), la définition de labels de contrôle d'accès au système connus, ainsi que le contrôle et l'administration de groupes utilisateur.

b) fonctions d'administration qui se rapportent à des contrôle de disponibilité, par exemple définition et mise à jour de paramètres de disponibilité ou de quotas de ressources.

c) fonctions d'administration qui se rapportent à l'installation générale et à la configuration. On peut citer par exemple la configuration de la TOE, le manuel de reprise, l'installation de corrections de sécurité de la TOE (s'il y en a), la réparation et la réinstallation de matériel.

d) fonctions d'administration qui se rapportent au contrôle et à la maintenance de routine des ressources de la TOE, par exemple l'activation et la désactivation de périphériques, le montage de moyens de stockage amovibles, la sauvegarde et la reprise d'objets utilisateur et système.

1010 Il est à noter que ces fonctions doivent être présentes dans une TOE suivant les familles contenues dans le PP ou la ST. Il est de la responsabilité de l'auteur du PP ou de la ST de garantir que des fonctions adéquates seront fournies pour gérer le système de façon sûre.

1011 La TSF pourrait contenir des fonctions qui peuvent être contrôlées par un administrateur. Par exemple, les fonctions d'audit pourraient être désactivées, la synchronisation du temps pourrait être commutable, ou le mécanisme d'authentification pourrait être modifiable.

FMT_MOF.1 Administration du comportement des fonctions de sécurité

Notes d'application pour l'utilisateur

1012 Ce composant permet à des rôles identifiés de gérer les fonctions de sécurité de la TSF. Cela pourrait impliquer l'obtention du statut actuel d'une fonction de sécurité,

l'activation ou la désactivation de la fonction de sécurité ou la modification du comportement de la fonction de sécurité. Un exemple de modification du comportement des fonctions de sécurité est le changement des mécanismes d'authentification.

Opérations

Sélection :

1013 **Dans FMT_MOF.1.1, l'auteur du PP ou de la ST devrait choisir si le rôle peut déterminer le comportement, désactiver, activer, ou modifier le comportement des fonctions de sécurité.**

Affectation :

1014 **Dans FMT_MOF.1.1, l'auteur du PP ou de la ST devrait spécifier les fonctions qui peuvent être modifiées par les rôles identifiés, telles que par exemple l'audit et la détermination du temps.**

1015 **Dans le FMT_MOF.1.1, l'auteur du PP ou de la ST devrait spécifier les rôles qui sont autorisés à modifier les fonctions de la TSF. Les rôles possibles sont spécifiés dans le composant FMT_SMR.1.**

H.2 Administration des attributs de sécurité (FMT_MSA)

1016 La présente famille définit les exigences de l'administration d'attributs de sécurité.

1017 Des utilisateurs, des sujets et des objets possèdent des attributs de sécurité associés qui affecteront le comportement de la TSF. Des exemples de tels attributs de sécurité sont les groupes auxquels appartient un utilisateur, les rôles qu'il pourrait assurer, la priorité d'un processus (sujet), et les droits associés à un rôle ou à un utilisateur. Ces attributs de sécurité pourraient devoir être gérés par l'utilisateur, par un sujet ou un utilisateur autorisé particulier (un utilisateur auquel il a été donné explicitement des droits pour cette administration).

1018 Il est à noter que le droit d'attribuer des droits à des utilisateurs est lui-même un attribut de sécurité ou potentiellement soumis à l'administration par FMT_MSA.1.

1019 Le composant FMT_MSA.2 peut être utilisé pour garantir que toute combinaison acceptée d'attributs de sécurité est dans un état sûr. La définition de ce qui signifie "sûr" relève des guides de la TOE et du modèle de TSP. Si le développeur a donné une définition claire des valeurs sûres et de la raison pour laquelle elles devraient être considérées comme sûres, l'abandon de la dépendance de FMT_MSA.2 envers ADV_SPM.1 peut être justifié.

1020 Dans certains cas, des sujets, des objets ou des comptes utilisateur sont créés. Si aucune valeur explicite pour les attributs de sécurité associés n'est donnée, des valeurs par défaut doivent être utilisées. Le composant FMT_MSA.1 peut être utilisé pour spécifier que ces valeurs par défaut peuvent être gérées.

FMT_MSA.1 Administration des attributs de sécurité

Notes d'application pour l'utilisateur

1021 Ce composant permet à des utilisateurs agissant sous certains rôles de gérer des attributs de sécurité identifiés. L'affectation d'un rôle aux utilisateurs se fait avec le composant FMT_SMR.1.

1022 La valeur par défaut d'un paramètre est la valeur que prend le paramètre quand il est instancié sans avoir de valeurs spécifiquement affectées. Une valeur initiale est fournie lors de l'instanciation (la création) d'un paramètre et écrase la valeur par défaut.

Opérations

Affectation :

1023 **Dans FMT_MSA.1.1, l'auteur du PP ou de la ST devrait énumérer la SFP de contrôle d'accès ou la SFP de contrôle de flux d'information pour laquelle les attributs de sécurité sont applicables.**

Sélection :

1024 **Dans le FMT_MSA.1.1, l'auteur du PP ou de la ST devrait spécifier les opérations qui peuvent être appliquées aux attributs de sécurité identifiés. L'auteur du PP ou de la ST peut spécifier que le rôle peut modifier la valeur par défaut, interroger, modifier l'attribut de sécurité, supprimer entièrement les attributs de sécurité ou définir leur propre fonctionnement.**

Affectation :

1025 **Dans le FMT_MSA.1.1, s'il est sélectionné, l'auteur du PP ou de la ST devrait spécifier quelles autres opérations le rôle pourrait exécuter, par exemple l'opération 'créer'.**

1026 **Dans FMT_MSA.1.1, l'auteur du PP ou de la ST devrait spécifier les attributs de sécurité qui peuvent être fixés ou modifiés par les rôles identifiés. Il est possible pour l'auteur du PP ou de la ST de spécifier que la valeur par défaut telle que des droits d'accès par défaut peut être gérée. De tels attributs de sécurité sont par exemple l'habilitation d'un utilisateur, le niveau de priorité de service, une liste de contrôle d'accès, des droits d'accès par défaut.**

1027 **Dans FMT_MSA.1.1, l'auteur du PP ou de la ST devrait spécifier les rôles qui sont autorisés à fixer ou à modifier les attributs de sécurité. Les rôles possibles sont spécifiés dans le composant FMT_SMR.1.**

FMT_MSA.2 Attributs de sécurité sûrs

Notes d'application pour l'utilisateur

1028 Ce composant contient des exigences relatives aux valeurs qui peuvent être affectées à des attributs de sécurité. Les valeurs affectées devraient être telles que la TOE demeure dans un état sûr.

1029 La définition de ce que signifie un état 'sûr' n'est pas donnée dans ce composant mais relève du développement de la TOE (en particulier ADV_SPM.1 Modèle informel de politique de sécurité de la TOE) et des informations résultantes dans les guides. Par exemple, si un compte utilisateur est créé, il devrait avoir un mot de passe non trivial.

FMT_MSA.3 Initialisation statique d'attribut

Notes d'application pour l'utilisateur

1030 Ce composant exige que la TSF donne des valeurs par défaut pour les attributs de sécurité pertinents des objets, qui peuvent être écrasés par une valeur initiale. Il peut encore être possible pour un nouvel objet d'avoir différents attributs de sécurité à sa création, si un mécanisme existe pour spécifier les permissions au moment de la création.

Opérations

Affectation :

1031 **Dans FMT_MSA.3.1, l'auteur du PP ou de la ST devrait énumérer la SFP de contrôle d'accès ou la SFP de contrôle de flux d'information pour laquelle les attributs de sécurité sont applicables.**

Sélection :

1032 **Dans FMT_MSA.3.1, l'auteur du PP ou de la ST devrait choisir si la propriété par défaut de l'attribut de contrôle d'accès sera de type restrictif, permissif ou autre. Dans ce dernier cas, l'auteur du PP ou de la ST devrait raffiner celle-ci pour obtenir une propriété spécifique.**

Affectation :

1033 **Dans FMT_MSA.3.2, l'auteur du PP ou de la ST devrait spécifier les rôles qui sont autorisés à modifier les valeurs des attributs de sécurité. Les rôles possibles sont spécifiés dans le composant FMT_SMR.1.**

H.3 Administration des données de la TSF (FMT_MTD)

1034 Ce composant impose des exigences pour l'administration de données de la TSF. Des exemples de données de la TSF sont la date et la trace d'audit. Ainsi par exemple, la présente famille permet la spécification de qui peut lire, supprimer ou créer la trace d'audit.

FMT_MTD.1 Administration des données de la TSF

Notes d'application pour l'utilisateur

1035 Ce composant permet à des utilisateurs sous un certain rôle de gérer la valeur des données de la TSF. L'affectation d'un rôle aux utilisateurs se fait avec le composant FMT_SMR.1.

1036 La valeur par défaut d'un paramètre est la valeur que prend le paramètre quand il est instancié sans avoir de valeurs spécifiquement affectées. Une valeur initiale est fournie lors de l'instanciation (la création) d'un paramètre et écrase la valeur par défaut.

Opérations

Sélection :

1037 **Dans FMT_MTD.1.1, l'auteur du PP ou de la ST devrait spécifier les opérations qui peuvent être appliquées aux données identifiées de la TSF. L'auteur du PP ou de la ST peut spécifier que le rôle peut modifier la valeur par défaut, effacer, interroger ou modifier les données de la TSF ou supprimer entièrement les données de la TSF. S'il le souhaite, l'auteur du PP ou de la ST pourrait spécifier tout type d'opération. Dans un but de clarification, il est précisé que "effacer des données de la TSF" signifie que le contenu des données de la TSF est effacé, mais que l'entité elle-même demeure dans le système.**

Affectation :

1038 **Dans FMT_MTD.1.1, s'il est sélectionné, l'auteur du PP ou de la ST devrait spécifier les autres opérations que le rôle pourrait exécuter. Un exemple pourrait être 'créer'.**

1039 **Dans FMT_MTD.1.1, l'auteur du PP ou de la ST devrait spécifier les données de la TSF qui peuvent être manipulées par les rôles identifiés. Il est possible à l'auteur du PP ou de la ST de spécifier que la valeur par défaut peut être gérée.**

1040 **Dans FMT_MTD.1.1, l'auteur du PP ou de la ST devrait spécifier les rôles qui sont autorisés à manipuler les données de la TSF. Les rôles possibles sont spécifiés dans le composant FMT_SMR.1.**

FMT_MTD.2 Administration des valeurs limites des données de la TSF

Notes d'application pour l'utilisateur

1041 Ce composant spécifie des valeurs limites de données de la TSF et des actions à entreprendre si ces limites sont dépassées. Ce composant permettra par exemple de définir les limites de la taille de la trace d'audit et spécifiera les actions à entreprendre quand ces limites sont dépassées.

Opérations

Affectation :

1042 **Dans FMT_MTD.2.1, l'auteur du PP ou de la ST devrait spécifier les données de la TSF qui peuvent avoir des limites et la valeur de ces limites. Une donnée de la TSF est par exemple le nombre d'utilisateurs connectés.**

1043 **Dans FMT_MTD.2.1, l'auteur du PP ou de la ST devrait spécifier les rôles qui sont autorisés à modifier les limites des données de la TSF et les actions à entreprendre. Les rôles possibles sont spécifiés dans le composant FMT_SMR.1.**

1044 **Dans FMT_MTD.2.2, l'auteur du PP ou de la ST devrait spécifier les actions à entreprendre si les limites spécifiées aux données spécifiées de la TSF sont dépassées. Une telle action de la TSF consiste par exemple à informer l'utilisateur autorisé et à générer une trace d'audit.**

FMT_MTD.3 Données sûres de la TSF

Notes d'application pour l'utilisateur

1045 Ce composant couvre des exigences relatives aux valeurs qui peuvent être affectées aux données de la TSF. Les valeurs affectées devraient être telles que la TOE demeure dans un état sûr.

1046 La définition de ce que signifie un état 'sûr' n'est pas donnée dans ce composant mais relève du développement de la TOE (en particulier ADV_SPM.1 Modèle informel de politique de sécurité de la TOE) et des informations résultantes dans les guides. Si le développeur a donné une définition claire des valeurs sûres et de la raison pour laquelle elles devraient être considérées comme sûres, l'abandon de la dépendance de FMT_MSA.2 envers ADV_SPM.1 peut être justifié.

H.4 Révocation (FMT_REV)

1047 La présente famille couvre la révocation d'attributs de sécurité pour divers entités dans une TOE.

FMT_REV.1 Révocation

Notes d'application pour l'utilisateur

1048 Ce composant spécifie des exigences relatives à la révocation de droits. Il exige la spécification des règles de révocation, par exemple :

a) La révocation aura lieu à la prochaine connexion de l'utilisateur ;

b) la révocation aura lieu à la prochaine tentative d'ouverture du fichier ;

c) la révocation aura lieu à un moment déterminé. Cela pourrait signifier que toutes les connexions en cours sont réévaluées toutes les x minutes.

Opérations

Sélection :

1049 **Dans FMT_REV.1.1, l'auteur du PP ou de la ST devrait spécifier si la possibilité de révoquer des attributs de sécurité d'utilisateurs, de sujets, d'objets, ou de toute autre ressource doit être offerte par la TSF. Si la dernière option est choisie, alors l'auteur du PP ou de la ST devrait utiliser l'opération de raffinement pour définir les ressources.**

Affectation :

1050 **Dans FMT_REV.1.1, l'auteur du PP ou de la ST devrait spécifier les rôles qui sont autorisés à modifier les fonctions de la TSF. Les rôles possibles sont spécifiés dans le composant FMT_SMR.1.**

1051 **Dans FMT_REV.1.2, l'auteur du PP ou de la ST devrait spécifier les règles de révocation. De telles règles pourraient être par exemple : "avant la prochaine opération sur la ressource associée", ou "pour toute création de nouveau sujet".**

H.5 Expiration des attributs de sécurité (FMT_SAE)

1052 La présente famille couvre la capacité d'appliquer des limites temporelles à la validité d'attributs de sécurité. La présente famille peut être appliquée pour spécifier des exigences d'expiration pour des attributs de contrôle d'accès, des attributs d'identification et d'authentification, des certificats (certificats de clés tels que ceux définis dans la norme ANSI X509 par exemple), des attributs d'audit, etc.

FMT_SAE.1 Autorisation limitée dans le temps

Opérations

Affectation :

1053 **Dans FMT_SAE.1.1, l'auteur du PP ou de la ST devrait fournir la liste d'attributs de sécurité pour laquelle l'expiration doit être appliquée. Un tel attribut pourrait être par exemple l'habilitation de sécurité d'un utilisateur.**

1054 **Dans FMT_SAE.1.1, l'auteur du PP ou de la ST devrait spécifier les rôles qui sont autorisés à modifier les attributs de sécurité de la TSF. Les rôles possibles sont spécifiés dans le composant FMT_SMR.1.**

1055 **Dans FMT_SAE.1.2, l'auteur du PP ou de la ST devrait fournir une liste d'actions à entreprendre pour chaque attribut de sécurité quand il arrive à expiration, comme par exemple : "l'habilitation de sécurité d'un utilisateur, quand elle arrive à expiration, est fixée au plus bas niveau d'habilitation pour la TOE". Si une révocation immédiate est souhaitée dans le PP ou la ST, l'action "révocation immédiate" devrait être spécifiée.**

H.6 Rôles pour l'administration de la sécurité (FMT_SMR)

1056 La présente famille permet de réduire la probabilité de dommages dus au fait que des utilisateurs outrepassent leurs droits en entreprenant des actions en dehors du cadre des responsabilités fonctionnelles qui leurs sont attribuées. Elle couvre également la menace que des mécanismes inadéquats aient pu être fournis et utilisés pour administrer de façon sûre la TSF.

1057 La présente famille exige que des informations soient maintenues pour identifier si un utilisateur est autorisé à utiliser une fonction organisationnelle particulière touchant à la sécurité.

1058 Certaines actions d'administration peuvent être exécutées par des utilisateurs, d'autres seulement par des personnels désignés dans l'organisation. La présente famille permet la définition de différents rôles, tels que propriétaire, auditeur, administrateur, administration au jour le jour.

1059 Les rôles utilisés dans La présente famille sont des rôles liés à la sécurité. Chaque rôle peut englober un ensemble extensif de possibilités (e.g. super administrateur ou root pour UNIX), ou peut être doté d'un droit unique (e.g. droit de lire un objet unique tel que le fichier d'aide). La présente famille définit les rôles. Les capacités attachées au rôle sont définies dans les familles FMT_MOF, FMT_MSA et FMT_MTD.

1060 Certains types de rôles pourraient être mutuellement exclusifs. Par exemple l'administration au jour le jour pourrait être dotée de la possibilité de définir et d'activer des utilisateurs, mais pas de celle de supprimer des utilisateurs (qui est réservée à l'administrateur (rôle)). Cette classe permet la spécification de politiques telles que le contrôle effectué par deux personnes.

FMT_SMR.1 Rôles de sécurité

Notes d'application pour l'utilisateur

1061 Ce composant spécifie les différents rôles que la TSF devrait reconnaître. Le système effectue souvent la distinction entre le propriétaire d'une entité, un administrateur et d'autres utilisateurs.

Opérations

Affectation :

1062 **Dans FMT_SMR.1.1, l'auteur du PP ou de la ST devrait spécifier les rôles qui sont reconnus par le système. Ce sont les rôles que des utilisateurs pourraient remplir relativement à la sécurité, comme par exemple : propriétaire, auditeur et administrateur.**

FMT_SMR.2 Restrictions sur les rôles de sécurité

Notes d'application pour l'utilisateur

1063 Ce composant spécifie les différents rôles que la TSF devrait reconnaître, et les conditions dans lesquelles ces rôles pourraient être gérés. Le système effectue souvent la distinction entre le propriétaire d'une entité, un administrateur et d'autres utilisateurs.

1064 Les conditions sur ces rôles spécifient les relations entre les différents rôles, ainsi que les restrictions sur le moment où un utilisateur peut remplir le rôle.

Opérations

Affectation :

1065 Dans FMT_SMR.2.1, l'auteur du PP ou de la ST devrait spécifier les rôles qui sont reconnus par le système. Ce sont les rôles que des utilisateurs pourraient remplir relativement à la sécurité, comme par exemple : propriétaire, auditeur et administrateur.

1066 **Dans FMT_SMR.2.3, l'auteur du PP ou de la ST devrait spécifier les conditions qui régissent l'attribution d'un rôle. Des exemples de ces conditions sont : "un compte ne peut pas remplir à la fois le rôle d'auditeur et le rôle d'administrateur" ou "un utilisateur ayant le rôle d'assistant doit aussi avoir le rôle de propriétaire".**

FMT_SMR.3 Prise en charge des rôles

Notes d'application pour l'utilisateur

1067 Ce composant spécifie qu'une demande explicite doit être faite pour remplir un rôle spécifique.

Opérations

Affectation :

1068 **Dans FMT_SMR.3.1, l'auteur du PP ou de la ST devrait spécifier les rôles qui exigent qu'une demande explicite soit faite, comme par exemple pour les rôles d'auditeur et d'administrateur.**

Annexe I
(Informative)

Protection de la vie privée (FPR)

1069 La présente classe décrit les exigences qui pourraient être imposées pour satisfaire les besoins relatifs à la vie privée des utilisateurs, tout en permettant encore, autant que possible, une flexibilité du système pour maintenir un contrôle suffisant sur son fonctionnement.

1070 Les composants de cette classe sont flexibles du fait que les utilisateurs autorisés peuvent être couverts ou non par les fonctions de sécurité exigées. Par exemple, un auteur de PP ou de ST pourrait considérer qu'il est approprié de ne pas exiger de protection relative à la vie privée d'utilisateurs par rapport à un utilisateur convenablement autorisé.

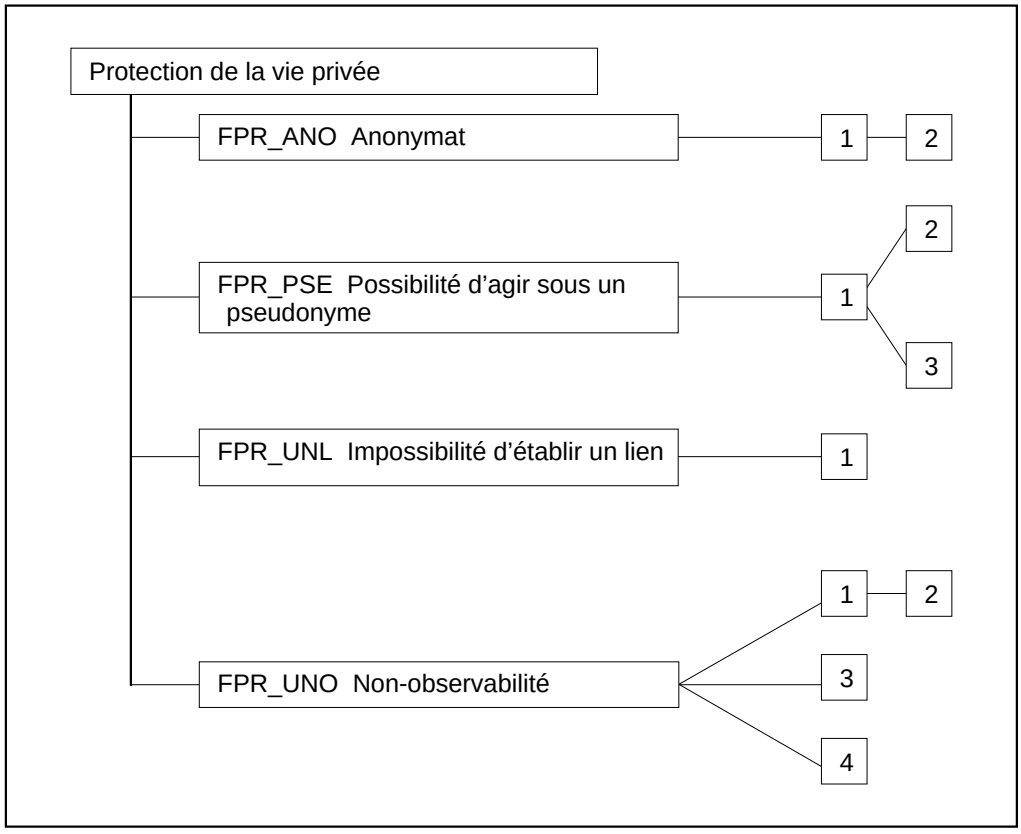


Figure 9.1 - Décomposition de la classe "Protection de la vie privée"

1071 Cette classe, ainsi que d'autres classes (telles que celles concernant l'audit, le contrôle d'accès, le chemin de confiance et la non répudiation) procure la flexibilité

pour spécifier le comportement souhaité relatif à la vie privée. D'autre part, les exigences de cette classe pourraient imposer des limitations à l'utilisation des composants d'autres classes, telles que FIA ou FAU. Par exemple, si des utilisateurs autorisés ne sont pas autorisés à voir l'identité de l'utilisateur (e.g. Anonymat ou Possibilité d'agir sous un pseudonyme), il ne sera évidemment pas possible d'imputer aux utilisateurs individuels une action quelconque effectuée par eux, touchant à la sécurité et couverte par les exigences relatives à la vie privée. Cependant, il peut encore être possible d'inclure des exigences d'audit dans un PP ou une ST, où le fait qu'un événement particulier touchant à la sécurité ait eu lieu est plus important que le fait de connaître celui qui en est la cause.

1072 Des informations supplémentaires sont fournies dans les notes d'application de la classe FAU, où il est expliqué que la définition du terme 'identité' dans le contexte de l'audit peut signifier aussi un alias ou d'autres informations qui pourraient identifier un utilisateur.

1073 Cette classe décrit quatre familles : Anonymat, Possibilité d'agir sous un pseudonyme, Impossibilité d'établir un lien et Non-observabilité. Anonymat, Possibilité d'agir sous un pseudonyme et Impossibilité d'établir un lien ont des relations complexes entre elles. Le choix d'une famille devrait dépendre des menaces identifiées. Pour certains types de menaces relatives à la vie privée, la possibilité d'agir sous un pseudonyme sera plus appropriée que l'anonymat (e.g. s'il y a une exigence d'audit). De plus, certains types de menaces relatives à la vie privée sont mieux contrées par une combinaison de composants tirés de différentes familles.

1074 Toutes les familles supposent qu'un utilisateur n'effectue pas explicitement une action qui révèle sa propre identité. Par exemple, la TSF n'est pas censée masquer le nom de l'utilisateur dans des messages électroniques ou des bases de données.

1075 Toutes les familles de cette classe ont des composants qui peuvent être adaptés au moyen d'opérations. Ces opérations permettent à l'auteur du PP ou de la ST de spécifier les utilisateurs ou les sujets coopérants auxquels la TSF doit être résistante. Une instanciation d'anonymat pourrait être par exemple : "la TSF doit garantir que les utilisateurs ou les sujets sont incapables de déterminer l'identité de l'utilisateur associé à l'application de télé-consultation".

1076 Il est à noter que la TSF ne devrait pas seulement fournir cette protection contre des utilisateurs individuels, mais aussi contre des utilisateurs coopérant pour obtenir les informations. La résistance de la protection fournie par cette classe devrait être décrite comme une résistance de fonctions ainsi qu'il est spécifié dans l'annexe B et l'annexe C de la partie 1 des CC.

I.1 Anonymat (FPR_ANO)

1077 L'anonymat garantit qu'un sujet peut utiliser une ressource ou un service sans révéler son identité d'utilisateur.

Notes pour l'utilisateur

1078 L'intention de cette famille est de spécifier qu'un utilisateur ou un sujet pourrait entreprendre une action sans dévoiler son identité d'utilisateur à d'autres entités telles que des utilisateurs, des sujets, ou des objets. La famille donne à l'auteur du PP ou de la ST un moyen d'identifier l'ensemble des utilisateurs qui ne peuvent pas voir l'identité de quelqu'un en train d'exécuter certaines actions.

1079 Par conséquent, si un sujet utilisant l'anonymat exécute une action, un autre sujet ne pourra pas déterminer l'identité ou même une référence à l'identité de l'utilisateur qui emploie le sujet. L'objectif de l'anonymat est la protection de l'identité des utilisateurs, et non la protection de l'identité du sujet ; ainsi l'identité du sujet n'est pas protégée contre une divulgation.

1080 Bien que l'identité du sujet ne soit pas dévoilée à d'autres sujets ou utilisateurs, il n'est pas interdit explicitement à la TSF d'obtenir l'identité des utilisateurs. Dans le cas où la TSF n'est pas autorisée à connaître l'identité de l'utilisateur, le composant FPR_ANO.2 pourrait être invoqué. Dans ce cas, la TSF ne devrait pas demander les informations de l'utilisateur.

1081 L'interprétation de "déterminer" devrait être prise dans le sens le plus large du terme. L'auteur du PP ou de la ST pourrait vouloir utiliser une résistance de fonctions pour indiquer la rigueur qui devrait être appliquée.

1082 La classification en composants établit une distinction entre les utilisateurs et un utilisateur autorisé. L'utilisateur autorisé est souvent exclu dans le composant, et par conséquent est autorisé à retrouver l'identité de l'utilisateur. Cependant, il n'y a pas d'exigence spécifique indiquant qu'un utilisateur autorisé doit être capable de déterminer l'identité de l'utilisateur. Pour une protection maximum relative à la vie privée, les composants indiqueraient qu'aucun utilisateur ou utilisateur autorisé ne peut voir l'identité de quiconque exécute une action, quelqu'elle soit.

1083 Bien que certains systèmes procurent l'anonymat pour tous les services qui sont fournis, d'autres systèmes procurent l'anonymat pour certains sujets ou certaines opérations. Pour permettre cette flexibilité, une opération est incluse où la portée de l'exigence est définie. Si l'auteur du PP ou de la ST veut inclure tous les sujets ou toutes les opérations, il peut indiquer "tous sujets et toutes opérations".

1084 Parmi les applications possibles, on peut citer la possibilité de faire des enquêtes de nature confidentielle dans des bases de données publiques, de répondre à des sondages électroniques, ou de faire des paiements ou des donations anonymes.

1085 Parmi des exemples d'utilisateurs ou de sujets potentiellement hostiles on trouve des fournisseurs, des opérateurs système, des partenaires et des utilisateurs de

communications, qui introduisent subrepticement des parties malveillantes (e.g. des chevaux de Troie) dans des systèmes. Tous ces utilisateurs ont la possibilité d'investiguer les profils d'utilisation (e.g. les utilisateurs qui ont utilisé tel ou tel service) et de faire un mauvais usage de ces informations.

FPR_ANO.1 Anonymat

Notes d'application pour l'utilisateur

1086 Ce composant garantit que l'identité d'un utilisateur est protégée contre une divulgation. Il peut y avoir cependant des cas dans lesquels un certain utilisateur autorisé peut déterminer qui a exécuté certaines actions. Ce composant donne la flexibilité nécessaire pour mettre en oeuvre une politique de protection limitée ou bien totale, relative à la vie privée.

Opérations

Affectation :

1087 **Dans FPR_ANO.1.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs ou des sujets contre lesquels la TSF doit offrir une protection. Par exemple, même si l'auteur du PP ou de la ST spécifie le rôle d'un utilisateur ou d'un sujet unique, la TSF ne doit pas seulement offrir une protection contre chaque utilisateur individuel ou sujet, mais doit protéger contre des utilisateurs ou des sujets coopérants. Un ensemble d'utilisateurs, par exemple, pourrait être un groupe d'utilisateurs qui peuvent travailler sous le même rôle ou qui peuvent tous utiliser le ou les mêmes processus.**

1088 **Dans FPR_ANO.1.1, l'auteur du PP ou de la ST devrait identifier la liste des sujets, des opérations ou des objets pour lesquels le véritable nom de l'utilisateur associé au sujet devrait être protégé, par exemple "l'application de vote".**

FPR_ANO.2 Anonymat sans demande d'informations

Notes d'application pour l'utilisateur

1089 Ce composant est utilisé pour garantir que la TSF n'est pas autorisée à connaître l'identité de l'utilisateur.

Opérations

Affectation :

1090 Dans FPR_ANO.2.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs ou des sujets contre lesquels la TSF doit offrir une protection. Par exemple, même si l'auteur du PP ou de la ST spécifie le rôle d'un utilisateur ou d'un sujet unique, la TSF ne doit pas seulement offrir une protection contre chaque utilisateur individuel ou sujet, mais doit protéger

contre des utilisateurs ou des sujets coopérants. Un ensemble d'utilisateurs, par exemple, pourrait être un groupe d'utilisateurs qui peuvent travailler sous le même rôle ou qui peuvent tous utiliser le ou les mêmes processus.

1091 Dans FPR_ANO.2.1, l'auteur du PP ou de la ST devrait identifier la liste des sujets, des opérations ou des objets pour lesquels le véritable nom de l'utilisateur associé au sujet devrait être protégé, par exemple "l'application de vote".

1092 **Dans FPR_ANO.2.2, l'auteur du PP ou de la ST devrait identifier la liste des services qui sont soumis à l'exigence d'anonymat, comme par exemple "l'accès aux descriptions des emplois".**

1093 **Dans FPR_ANO.2.2, l'auteur du PP ou de la ST devrait identifier la liste des sujets pour lesquels le véritable nom de l'utilisateur associé au sujet devrait être protégé quand les services spécifiés sont fournis.**

I.2 Possibilité d'agir sous un pseudonyme (FPR_PSE)

1094 La possibilité d'agir sous un pseudonyme garantit qu'un utilisateur peut utiliser une ressource ou un service sans révéler son identité, mais peut quand même avoir à répondre de cette utilisation. L'utilisateur peut être imputable en étant directement associé à une référence (alias) détenue par la TSF, ou en fournissant un alias, tel qu'un numéro compte, qui sera utilisé lors des travaux.

Notes pour l'utilisateur

1095 Sous plusieurs aspects, la possibilité d'agir sous un pseudonyme ressemble à l'anonymat. Tous deux protègent l'identité de l'utilisateur, mais avec la possibilité d'agir sous un pseudonyme, une référence à l'identité de l'utilisateur est maintenue dans un but d'imputabilité ou dans d'autres buts.

1096 Le composant FPR_PSE.1 ne spécifie pas les exigences concernant la référence à l'identité de l'utilisateur. Pour spécifier des exigences concernant cette référence, deux ensembles d'exigences sont présentées : FPR_PSE.2 et FPR_PSE.3.

1097 Un moyen d'utiliser la référence consiste à pouvoir obtenir l'identifiant original de l'utilisateur. Par exemple, dans un environnement de monnaie électronique il serait avantageux de pouvoir tracer l'identité de l'utilisateur quand un contrôle a été effectué plusieurs fois (i.e. fraude). En général, l'identité de l'utilisateur doit pouvoir être retrouvée dans des conditions spécifiques. L'auteur du PP ou de la ST pourrait vouloir incorporer le composant "FPR_PSE.2 Utilisation réversible de pseudonymes" pour décrire ces services.

1098 Un autre usage de la référence est celui de l'alias pour un utilisateur. Par exemple, un utilisateur qui ne souhaite pas être identifié peut fournir un compte sur lequel l'utilisation de la ressource devrait être imputée. Dans de tels cas, la référence à l'identité de l'utilisateur est un alias de l'utilisateur, et d'autres utilisateurs ou sujets peuvent utiliser l'alias pour réaliser leurs fonctions sans jamais obtenir l'identité de l'utilisateur (par exemple, des opérations statistiques sur l'utilisation du système). Dans ce cas, l'auteur du PP ou de la ST pourrait vouloir incorporer "FPR_PSE.3 Possibilité d'agir sous un pseudonyme en utilisant un alias" pour spécifier les règles auxquelles la référence doit se conformer.

1099 En utilisant les solutions ci-dessus, la monnaie électronique peut être créée en utilisant "FPR_PSE.2 Utilisation réversible de pseudonymes" qui spécifie que l'identité de l'utilisateur sera protégée et, si cela est spécifié dans la condition, qu'il y ait une exigence pour tracer l'identité de l'utilisateur si la monnaie électronique est dépensée deux fois. Quand l'utilisateur est honnête, l'identité de l'utilisateur est protégée ; si l'utilisateur essaye de tricher, l'identité de l'utilisateur peut être tracée.

1100 Un système différent pourrait être une carte de crédit électronique, où l'utilisateur fournit un pseudonyme qui indique un compte sur lequel le montant dépensé peut être soustrait. Dans de tels cas, "FPR_PSE.3 Possibilité d'agir sous un pseudonyme en utilisant un alias" pourrait par exemple être utilisé. Ce composant spécifierait que l'identité de l'utilisateur sera protégée et, de plus, que le même

utilisateur se verra seulement attribué les valeurs spécifiées correspondant à ses dépôts monétaires (si tel est spécifié dans les conditions).

1101 Il devrait apparaître que les composants potentiellement les plus exigeants ne peuvent pas être combinés avec d'autres exigences, telles que l'identification et l'authentification ou l'audit. L'expression "déterminer l'identité" devrait être interprétée dans le sens le plus large du terme. Les informations ne sont pas fournies par la TSF pendant l'opération, et l'entité ne peut pas non plus déterminer le sujet ou le propriétaire du sujet qui a fait appel à l'opération, de même que la TSF ne pourra pas enregistrer des informations disponibles aux utilisateurs ou aux sujets qui pourraient dévoiler l'identité de l'utilisateur dans le futur.

1102 L'objectif est que la TSF ne révèle pas toutes les informations qui compromettraient l'identité de l'utilisateur, e.g. l'identité de sujets agissant pour le compte de l'utilisateur. Les informations qui sont considérées comme sensibles dépendent de l'effort qu'un attaquant est capable de consentir. Par conséquent, la famille "FPR_PSE Possibilité d'agir sous un pseudonyme" est soumise aux exigences de la résistance de fonctions.

1103 Les applications possibles comprennent la possibilité d'imputer à un appelant le coût au taux le plus avantageux pour des services téléphoniques sans révéler son identité, ou sans lui faire payer l'utilisation anonyme d'un système de paiement électronique.

1104 Parmi des exemples d'utilisateurs ou de sujets potentiellement hostiles on trouve des fournisseurs, des opérateurs système, des partenaires et des utilisateurs de communications, qui introduisent subrepticement des parties malveillantes (e.g. des chevaux de Troie) dans des systèmes. Tous ces utilisateurs ont la possibilité d'investiguer les profils d'utilisation (e.g. les utilisateurs qui ont utilisé tel ou tel service) et de faire un mauvais usage de ces informations. En complément aux services d'anonymat, les services permettant d'agir sous un pseudonyme contiennent des méthodes d'autorisation sans identification, spécialement pour le paiement anonyme ("monnaie électronique"). Cela aide les fournisseurs à obtenir le paiement d'une façon sûre tout en maintenant l'anonymat du client.

FPR_PSE.1 Possibilité d'agir sous un pseudonyme

Notes d'application pour l'utilisateur

1105 Ce composant offre à l'utilisateur une protection contre la divulgation de son identité à d'autres utilisateurs. L'utilisateur demeure imputable pour ses actions.

Opérations

Affectation :

1106 **Dans FPR_PSE.1.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs ou des sujets contre lesquels la TSF doit offrir une protection. Par exemple, même si l'auteur du PP ou de la ST spécifie le rôle d'un utilisateur ou d'un sujet unique, la TSF ne doit pas**

seulement offrir une protection contre chaque utilisateur individuel ou sujet, mais doit protéger contre des utilisateurs ou des sujets coopérants. Un ensemble d'utilisateurs, par exemple, pourrait être un groupe d'utilisateurs qui peuvent travailler sous le même rôle ou peuvent tous utiliser le ou les mêmes processus.

1107 **Dans FPR_PSE.1.1, l'auteur du PP ou de la ST devrait identifier la liste des sujets, des opérations ou des objets pour lesquels le véritable nom de l'utilisateur associé au sujet devrait être protégé, comme par exemple "l'accès à des offres d'emplois". Il est à noter que les 'objets' comprennent tout autre attribut qui pourrait permettre à un autre utilisateur ou sujet de déduire l'identité véritable de l'utilisateur.**

1108 **Dans FPR_PSE.1.2, l'auteur du PP ou de la ST devrait identifier le nombre d'alias (un ou plusieurs) que la TSF peut fournir.**

1109 **Dans FPR_PSE.1.2, l'auteur du PP ou de la ST devrait identifier la liste des sujets auxquels la TSF peut fournir un alias.**

Sélection :

1110 **Dans FPR_PSE.1.3, l'auteur du PP ou de la ST devrait spécifier si l'alias de l'utilisateur est généré par la TSF ou fourni par l'utilisateur.**

Affectation :

1111 **Dans FPR_PSE.1.3, l'auteur du PP ou de la ST devrait identifier la métrique à laquelle l'alias généré par la TSF ou par l'utilisateur devrait se conformer.**

FPR_PSE.2 Utilisation réversible de pseudonymes

Notes d'application pour l'utilisateur

1112 Dans ce composant, la TSF doit garantir que dans des conditions spécifiées, l'identité de l'utilisateur associée à une référence fournie peut être déterminée.

1113 Dans le composant FPR_PSE.1, la TSF doit fournir un alias à la place de l'identité de l'utilisateur. Quand les conditions spécifiées sont satisfaites, l'identité de l'utilisateur auquel appartient l'alias peut être déterminée. Un exemple d'une telle condition dans un environnement avec de la monnaie électronique est le suivant : "la TSF ne doit fournir au notaire une possibilité de déterminer l'identité de l'utilisateur en fonction de l'alias fourni que sous la condition qu'un contrôle ait été effectué deux fois.".

Opérations

Affectation :

1114 Dans FPR_PSE.2.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs ou des sujets contre lesquels la TSF doit offrir une protection. Par exemple, même si l'auteur du PP ou de la ST spécifie le rôle

d'un utilisateur ou d'un sujet unique, la TSF ne doit pas seulement offrir une protection contre chaque utilisateur individuel ou sujet, mais doit protéger contre des utilisateurs ou des sujets coopérants. Un ensemble d'utilisateurs, par exemple, pourrait être un groupe d'utilisateurs qui peuvent travailler sous le même rôle ou peuvent tous utiliser le ou les mêmes processus.

1115 Dans FPR_PSE.2.1, l'auteur du PP ou de la ST devrait identifier la liste des sujets, des opérations ou des objets pour lesquels le véritable nom de l'utilisateur associé au sujet devrait être protégé, comme par exemple "l'accès à des offres d'emplois". Il est à noter que les 'objets' comprennent tout autre attribut qui pourrait permettre à un autre utilisateur ou sujet de déduire l'identité véritable de l'utilisateur.

1116 Dans FPR_PSE.2.2, l'auteur du PP ou de la ST devrait identifier le nombre d'alias (un ou plusieurs) que la TSF peut fournir.

1117 Dans FPR_PSE.2.2, l'auteur du PP ou de la ST devrait identifier la liste des sujets auxquels la TSF peut fournir un alias.

Sélection :

1118 Dans FPR_PSE.2.3, l'auteur du PP ou de la ST devrait spécifier si l'alias de l'utilisateur est généré par la TSF ou fourni par l'utilisateur.

Affectation :

1119 Dans FPR_PSE.2.3, l'auteur du PP ou de la ST devrait identifier la métrique à laquelle l'alias généré par la TSF ou par l'utilisateur devrait se conformer.

Sélection :

1120 **Dans FPR_PSE.2.4, l'auteur du PP ou de la ST devrait choisir si l'utilisateur autorisé ou des sujets de confiance peuvent déterminer le véritable nom de l'utilisateur.**

Affectation :

1121 **Dans FPR_PSE.2.4, l'auteur du PP ou de la ST devrait identifier la liste des sujets de confiance qui peuvent obtenir le véritable nom de l'utilisateur pour une condition spécifiée, par exemple un notaire ou un utilisateur autorisé particulier.**

1122 **Dans FPR_PSE.2.4, l'auteur du PP ou de la ST devrait identifier la liste des conditions pour lesquelles les sujets de confiance et l'utilisateur autorisé peuvent déterminer le véritable nom de l'utilisateur en fonction de la référence fournie. Ces conditions peuvent être "à une certaine heure", ou elles peuvent être à caractère organisationnel comme par exemple "à la suite de l'ordre d'un tribunal".**

FPR_PSE.3 Possibilité d'agir sous un pseudonyme en utilisant un alias

Notes d'application pour l'utilisateur

1123 Dans ce composant, la TSF doit garantir que la référence fournie satisfait à certaines règles de construction, et par là même peut être utilisée d'une façon sûre par des sujets potentiellement non sûrs.

1124 Si un utilisateur veut utiliser les ressources d'un disque sans révéler son identité, la possibilité d'agir sous un pseudonyme peut être utilisée. Cependant, chaque fois que l'utilisateur accède au système, le même alias doit être utilisé. De telles conditions peuvent être spécifiées dans ce composant.

Opérations

Affectation :

1125 Dans FPR_PSE.3.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs ou des sujets contre lesquels la TSF doit offrir une protection. Par exemple, même si l'auteur du PP ou de la ST spécifie le rôle d'un utilisateur ou d'un sujet unique, la TSF ne doit pas seulement offrir une protection contre chaque utilisateur individuel ou sujet, mais doit protéger contre des utilisateurs ou des sujets coopérants. Un ensemble d'utilisateurs, par exemple, pourrait être un groupe d'utilisateurs qui peuvent travailler sous le même rôle ou peuvent tous utiliser le ou les mêmes processus.

1126 Dans FPR_PSE.3.1, l'auteur du PP ou de la ST devrait identifier la liste des sujets, des opérations ou des objets pour lesquels le véritable nom de l'utilisateur associé au sujet devrait être protégé, comme par exemple "l'accès à des offres d'emplois". Il est à noter que les 'objets' comprennent tout autre attribut qui pourrait permettre à un autre utilisateur ou sujet de déduire l'identité véritable de l'utilisateur.

1127 Dans FPR_PSE.3.2, l'auteur du PP ou de la ST devrait identifier le nombre d'alias (un ou plusieurs) que la TSF peut fournir.

1128 Dans FPR_PSE.3.2, l'auteur du PP ou de la ST devrait identifier la liste des sujets auxquels la TSF peut fournir un alias.

Sélection :

1129 Dans FPR_PSE.3.3, l'auteur du PP ou de la ST devrait spécifier si l'alias de l'utilisateur est généré par la TSF ou fourni par l'utilisateur.

Affectation :

1130 Dans FPR_PSE.3.3, l'auteur du PP ou de la ST devrait identifier la métrique à laquelle l'alias généré par la TSF ou par l'utilisateur devrait se conformer.

1131 **Dans FPR_PSE.3.4, l'auteur du PP ou de la ST devrait identifier la liste des conditions qui indiquent quand la référence utilisée pour le nom véritable de l'utilisateur doit être unique et quand elle devra être**

différente, par exemple “quand l’utilisateur se connecte sur le même hôte” il devra utiliser un alias unique.

I.3 Impossibilité d'établir un lien (FPR_UNL)

1132 L'impossibilité d'établir un lien garantit qu'un utilisateur peut utiliser plusieurs fois des ressources ou des services sans que d'autres soient capables d'établir un lien entre ces utilisations. L'impossibilité d'établir un lien diffère de la possibilité d'agir sous un pseudonyme car, bien que pour cette dernière l'utilisateur n'est pas connu non plus, les relations entre les différentes actions peuvent être fournies.

Notes pour l'utilisateur

1133 Les exigences de la famille "Impossibilité d'établir un lien" sont destinées à protéger l'identité de l'utilisateur contre l'établissement de profils d'utilisation des opérations. Par exemple, quand une carte à puce téléphonique est employée avec un numéro unique, la compagnie de téléphone peut déterminer le comportement de l'utilisateur de cette carte de téléphone. Quand des profils d'appels téléphoniques d'utilisateurs sont connus, la carte peut être associée à un utilisateur spécifique. Masquer les relations entre les différents appels à un service ou les accès à une ressource empêchera ce type de collecte d'informations.

1134 En conclusion, une exigence concernant l'impossibilité d'établir un lien pourrait impliquer que l'identité du sujet et de l'utilisateur d'une opération doive être protégée. Sinon, ces informations pourraient être utilisées pour établir un lien entre les opérations.

1135 L'impossibilité d'établir un lien exige que des opérations différentes ne puissent pas être reliées. Ces relations peuvent prendre plusieurs formes, par exemple l'utilisateur associé à l'opération, ou le terminal où l'action a été initiée, ou le moment où l'action a été exécutée. L'auteur du PP ou de la ST peut spécifier le type de relations qui doivent être couvertes.

1136 Parmi les applications possibles, on peut citer la possibilité d'utiliser plusieurs fois un pseudonyme sans créer un profil d'utilisation qui pourrait révéler l'identité de l'utilisateur.

1137 Parmi des exemples d'utilisateurs ou de sujets potentiellement hostiles on trouve des fournisseurs, des opérateurs système, des partenaires et des utilisateurs de communications, qui introduisent subrepticement des parties malveillantes (e.g. des chevaux de Troie) dans des systèmes qu'ils n'utilisent pas mais dans lesquels ils veulent obtenir des informations. Tous ces utilisateurs ont la possibilité d'investiguer les profils d'utilisation (e.g. les utilisateurs qui ont utilisé tel ou tel service) et de faire un mauvais usage de ces informations. L'impossibilité d'établir un lien protège les utilisateurs contre les associations qui pourraient être faites entre plusieurs actions effectuées par un client. Par exemple, dans le cas d'une suite d'appels téléphoniques par un client anonyme à des personnes différentes, l'ensemble des identités de ces personnes pourrait révéler l'identité du client.

FPR_UNL.1 Impossibilité d'établir un lien

Notes d'application pour l'utilisateur

1138 Ce composant garantit que des utilisateurs ne peuvent pas relier des opérations différentes dans le système et obtenir par là même des informations.

Opérations

Affectation :

1139 **Dans FPR_UNL.1.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs ou des sujets contre lesquels la TSF doit offrir une protection. Par exemple, même si l'auteur du PP ou de la ST spécifie le rôle d'un utilisateur ou d'un sujet unique, la TSF ne doit pas seulement offrir une protection contre chaque utilisateur individuel ou sujet, mais doit protéger contre des utilisateurs ou des sujets coopérants. Un ensemble d'utilisateurs, par exemple, pourrait être un groupe d'utilisateurs qui peuvent travailler sous le même rôle ou peuvent tous utiliser le ou les mêmes processus.**

1140 **Dans FPR_UNL.1.1 l'auteur du PP ou de la ST devrait identifier la liste des opérations, comme par exemple "envoyer un message électronique", qui devraient être soumises à l'exigence d'impossibilité d'établir un lien.**

Sélection :

1141 **Dans FPR_UNL.1.1, l'auteur du PP ou de la ST devrait sélectionner les relations qui devraient être masquées. La sélection permet de spécifier soit l'identité de l'utilisateur soit des relations.**

Affectation :

1142 **Dans FPR_UNL.1.1, l'auteur du PP ou de la ST devrait identifier la liste des relations contre lesquelles il faudrait se protéger, comme par exemple, "émis par le même terminal".**

I.4 Non-observabilité (FPR_UNO)

1143 La non-observabilité garantit qu'un utilisateur peut utiliser une ressource ou un service sans que d'autres, en particulier des tierces parties, soient capables d'observer que la ressource ou le service est en cours d'utilisation.

Notes pour l'utilisateur

1144 La famille "non-observabilité" prend en compte l'identité de l'utilisateur sous un angle différent que dans les familles précédentes : Anonymat, Possibilité d'agir sous un pseudonyme et Impossibilité d'établir un lien. Dans ce cas, l'objectif est de masquer l'utilisation d'une ressource ou d'un service, plutôt que l'identité de l'utilisateur.

1145 Plusieurs techniques peuvent être appliquées pour implémenter la non-observabilité. Comme exemples de techniques permettant d'assurer la non-observabilité on peut citer :

a) Allocation d'informations ayant un impact sur la non-observabilité : des informations touchant à la non-observabilité (e.g. des informations décrivant qu'une opération a été réalisée) peuvent être allouées dans plusieurs endroits de la TOE. Les informations pourraient être allouées dans une seule partie de la TOE choisie au hasard de telle façon qu'un attaquant ne connaisse pas la partie de la TOE qui devrait être attaquée. Une autre façon de procéder pourrait consister à distribuer les informations de telle façon qu'aucune partie unique de la TOE ne contienne suffisamment d'informations qui, si elles étaient altérées, compromettraient la vie privée de l'utilisateur. Cette technique est traitée explicitement dans le composant FPR_UNO.2.

b) Diffusion : Quand des informations sont diffusées (e.g. sur un réseau ethernet, par radio), les utilisateurs ne peuvent pas déterminer qui a réellement reçu et utilisé ces informations. Cette technique est particulièrement utile quand des informations devraient atteindre des destinataires qui peuvent craindre des conséquences désagréables du fait de montrer leur intérêt pour ces informations (e.g. informations médicales sensibles).

c) Protection cryptographique et bourrage de message : les personnes qui observent un flot de messages pourraient obtenir des informations à partir du fait qu'un message est transféré et à partir des attributs associées à ce message. En faisant du bourrage de trafic, du bourrage de message, et en chiffrant le flot de messages, la transmission d'un message et de ses attributs peut être protégée.

1146 Parfois les utilisateurs ne devraient pas pouvoir observer l'utilisation d'une ressource, alors qu'un utilisateur autorisé doit pouvoir le faire afin de remplir ses missions. Dans de tels cas, le composant FPR_UNO.4 pourrait être utilisé, pour

donner la possibilité à un ou plusieurs utilisateurs autorisés d'observer l'utilisation d'une ressource.

1147 Cette famille utilise le concept de "parties de la TOE". Cela désigne toute partie de la TOE qui est séparée soit physiquement, soit logiquement, d'autres parties de la TOE. Dans le cas où la séparation est logique, la famille FPT_SEP peut s'appliquer.

1148 La non-observabilité des communications peut être un facteur important dans de nombreux domaines, tels que l'application de droits constitutionnels, de politiques organisationnelles, ou d'applications de défense.

FPR_UNO.1 Non-observabilité

Notes d'application pour l'utilisateur

1149 Ce composant exige que l'utilisation d'une fonction ou d'une ressource ne puisse pas être observée par des utilisateurs non autorisés. En complément à ce composant, un auteur de PP ou de ST pourrait vouloir incorporer l'analyse de canaux cachés.

Opérations

Affectation :

1150 **Dans FPR_UNO.1.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs ou des sujets contre lesquels la TSF doit offrir une protection. Par exemple, même si l'auteur du PP ou de la ST spécifie le rôle d'un utilisateur ou d'un sujet unique, la TSF ne doit pas seulement offrir une protection contre chaque utilisateur individuel ou sujet, mais doit protéger contre des utilisateurs ou des sujets coopérants. Un ensemble d'utilisateurs, par exemple, pourrait être un groupe d'utilisateurs qui peuvent travailler sous le même rôle ou peuvent tous utiliser le ou les mêmes processus.**

1151 **Dans FPR_UNO.1.1, l'auteur du PP ou de la ST devrait identifier la liste d'opérations qui sont soumises à l'exigence de non-observabilité. D'autres utilisateurs ou sujets ne pourront alors pas observer les opérations sur un objet couvert par la liste spécifiée (e.g. lire et écrire dans l'objet).**

1152 **Dans FPR_UNO.1.1, l'auteur du PP ou de la ST devrait identifier la liste des objets qui sont couverts par l'exigence de non-observabilité, par exemple un serveur de messagerie ou un site ftp spécifique.**

1153 **Dans FPR_UNO.1.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs ou des sujets protégés dont les informations relatives à la non-observabilité seront protégées, comme par exemple : "utilisateurs accédant au système par l'internet".**

FPR_UNO.2 Allocation des informations ayant un impact sur la non-observabilité

Notes d'application pour l'utilisateur

1154 Ce composant exige que l'utilisation d'une fonction ou d'une ressource ne puisse pas être observée par des utilisateurs ou des sujets spécifiés. De plus, ce composant spécifie que des informations liées à la vie privée de l'utilisateur sont distribuées dans la TOE de telle façon que des attaquants ne puissent pas savoir quelle partie de la TOE prendre pour cible, ou soient obligés d'attaquer plusieurs parties de la TOE.

1155 Ce composant peut servir par exemple dans l'utilisation d'un noeud de réseau alloué de façon aléatoire pour fournir une fonction. Dans un tel cas, le composant pourrait exiger que les informations à caractère privé doivent seulement être disponibles pour une partie identifiée de la TOE, et ne seront pas communiquées en dehors de cette partie de la TOE.

1156 Un exemple plus complexe peut être trouvé dans certains 'algorithmes de vote'. Plusieurs parties de la TOE seront impliquées dans le service, mais aucune partie individuelle de la TOE ne sera capable de violer la politique. Ainsi une personne peut (ou non) émettre un vote sans que la TOE ne soit capable de déterminer si un vote a été émis ni le contenu du vote (à moins que le vote ne soit fait à l'unanimité).

1157 En plus de ce composant, un auteur de PP ou de ST pourrait vouloir incorporer l'analyse de canaux cachés.

Opérations

Affectation :

1158 Dans FPR_UNO.2.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs ou des sujets contre lesquels la TSF doit offrir une protection. Par exemple, même si l'auteur du PP ou de la ST spécifie le rôle d'un utilisateur ou d'un sujet unique, la TSF ne doit pas seulement offrir une protection contre chaque utilisateur individuel ou sujet, mais doit protéger contre des utilisateurs ou des sujets coopérants. Un ensemble d'utilisateurs, par exemple, pourrait être un groupe d'utilisateurs qui peuvent travailler sous le même rôle ou peuvent tous utiliser le ou les mêmes processus.

1159 Dans FPR_UNO.2.1,l'auteur du PP ou de la ST devrait identifier la liste d'opérations qui sont soumises à l'exigence de non-observabilité. D'autres utilisateurs ou sujets ne pourront alors pas observer les opérations sur un objet couvert par la liste spécifiée (e.g. lire et écrire dans l'objet).

1160 Dans FPR_UNO.2.1, l'auteur du PP ou de la ST devrait identifier la liste des objets qui sont couverts par l'exigence de non-observabilité, par exemple un serveur de messagerie ou un site ftp spécifique.

1161 Dans FPR_UNO.2.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs ou des sujets protégés dont les informations relatives à la

non-observabilité seront protégées, comme par exemple : “utilisateurs accédant au système par l’internet”.

1162 **Dans FPR_UNO.2.2, l’auteur du PP ou de la ST devrait identifier les informations à caractère privé qui devraient être distribuées d’une manière contrôlée, telles que par exemple : adresse IP d’un sujet, adresse IP d’un objet, heure, clés de chiffrement utilisées.**

1163 **Dans FPR_UNO.2.2, l’auteur du PP ou de la ST devrait spécifier les conditions dans lesquelles la dissémination des informations devrait se faire. Ces conditions devraient être conservées pendant la durée de vie des informations à caractère privé pour chaque instanciation. Des exemples de telles conditions pourraient être : “les informations doivent seulement être présentes dans une seule partie séparée de la TOE et ne doivent pas être communiquées en dehors de cette partie de la TOE”, “les informations doivent résider seulement dans une seule partie séparée de la TOE, mais doivent être périodiquement déplacées vers une autre partie de la TOE”, “les informations doivent être distribuées entre les différentes parties de la TOE de telle façon que la compromission de 5 parties séparées quelconques de la TOE ne compromettra pas la politique de sécurité”.**

FPR_UNO.3 Non-observabilité sans sollicitation d’informations

Notes d’application pour l’utilisateur

1164 Ce composant est utilisé pour exiger que la TSF n’essaye pas d’obtenir des informations qui pourraient compromettre la non-observabilité quand des services spécifiques sont fournis. Par conséquent la TSF ne sollicitera pas (i.e. n’essaiera pas d’obtenir à partir d’autres entités) toute information qui pourrait être utilisée pour compromettre la non-observabilité.

Opérations

Affectation :

1165 **Dans FPR_UNO.3.1, l’auteur du PP ou de la ST devrait identifier la liste des services qui sont soumis à l’exigence de non-observabilité, comme par exemple “l’accès à des descriptions d’emplois”.**

1166 **Dans FPR_UNO.3.1, l’auteur du PP ou de la ST devrait identifier la liste des sujets pour lesquels les informations à caractère privé devraient être protégées quand les services spécifiés sont fournis.**

1167 **Dans FPR_UNO.3.1, l’auteur du PP ou de la ST devrait spécifier les informations à caractère privé qui seront protégées des sujets spécifiés, par exemple l’identité du sujet qui a utilisé un service et la quantité qui a été utilisée, telle que la ressource mémoire par exemple.**

FPR_UNO.4 Observabilité par un utilisateur autorisé

Notes d'application pour l'utilisateur

1168 Ce composant est utilisé pour exiger qu'il y ait un ou plusieurs utilisateurs autorisés ayant les droits d'observer l'utilisation de la ressource. Sans ce composant, cette possibilité est autorisée mais n'est pas obligatoire.

Opérations

Affectation :

1169 **Dans FPR_UNO.4.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des utilisateurs autorisés pour lesquels la TSF doit procurer la possibilité d'observer l'utilisation de la ressource. Un ensemble d'utilisateurs autorisés, par exemple, pourrait être un groupe d'utilisateurs autorisés pouvant travailler sous le même rôle ou pouvant tous utiliser le ou les mêmes processus.**

1170 **Dans FPR_UNO.4.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des ressources ou des services que l'utilisateur autorisé doit pouvoir observer.**

Annexe J
(Informative)

Protection des fonctions de sécurité de la TOE (FPT)

1171 La présente classe contient des familles d'exigences fonctionnelles qui se rapportent à l'intégrité et à la gestion des mécanismes qu'offre la TSF (indépendamment des spécificités de la TSP) et à l'intégrité des données de la TSF (indépendamment du contenu spécifique des données de la TSP). Dans une certaine mesure, les familles de cette classe peuvent apparaître comme une duplication des composants de la classe FDP (Protection des données de l'utilisateur) ; elles peuvent même être implémentées en utilisant les mêmes mécanismes. Cependant, la classe FDP porte sur la protection des données de l'utilisateur, tandis que la classe FPT porte sur la protection des données de la TSF. En fait, les composants de la classe FPT sont nécessaires pour fournir les exigences établissant que les SFP de la TOE ne peuvent pas être altérées ou court-circuitées.

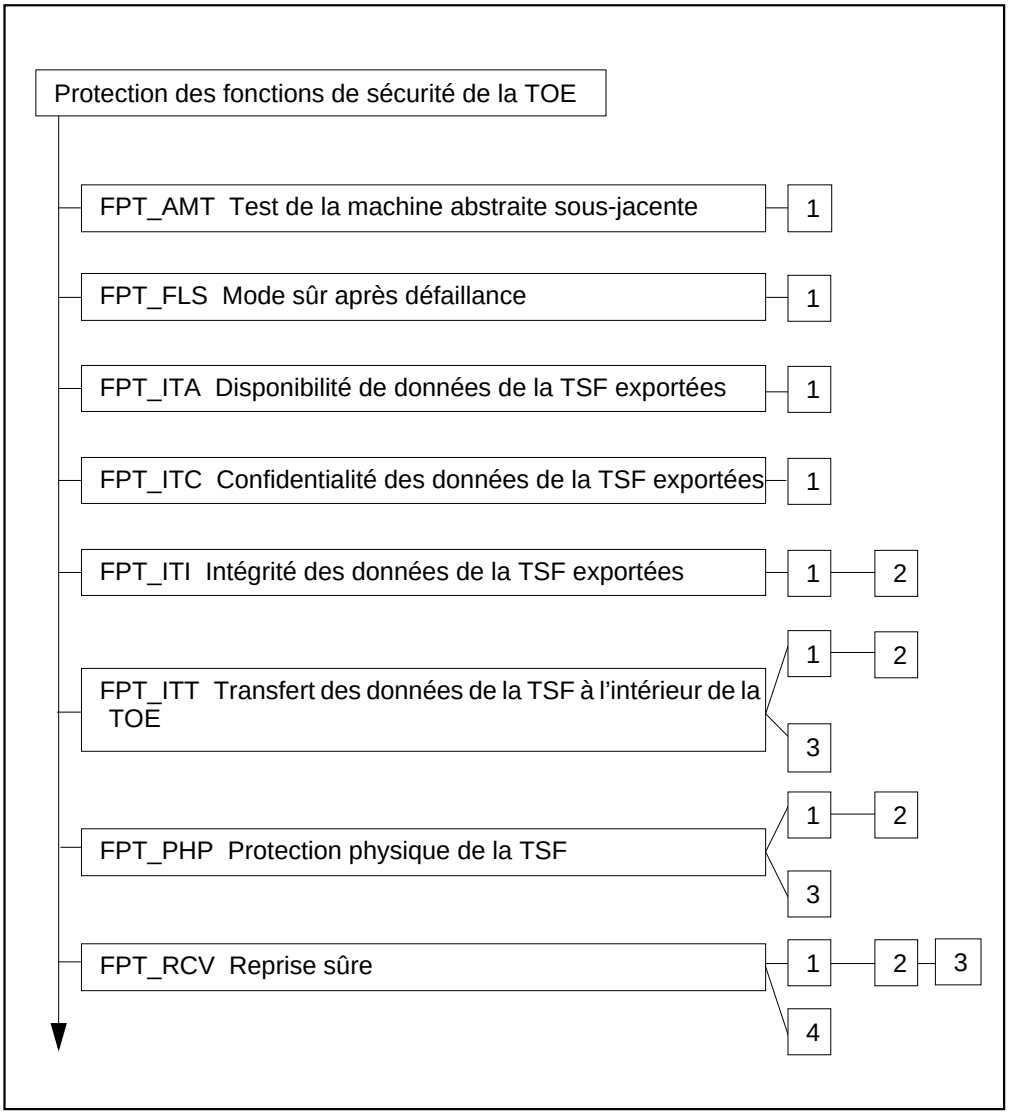


Figure 10.1 - Décomposition de la classe "Protection des fonctions de sécurité de la TOE"

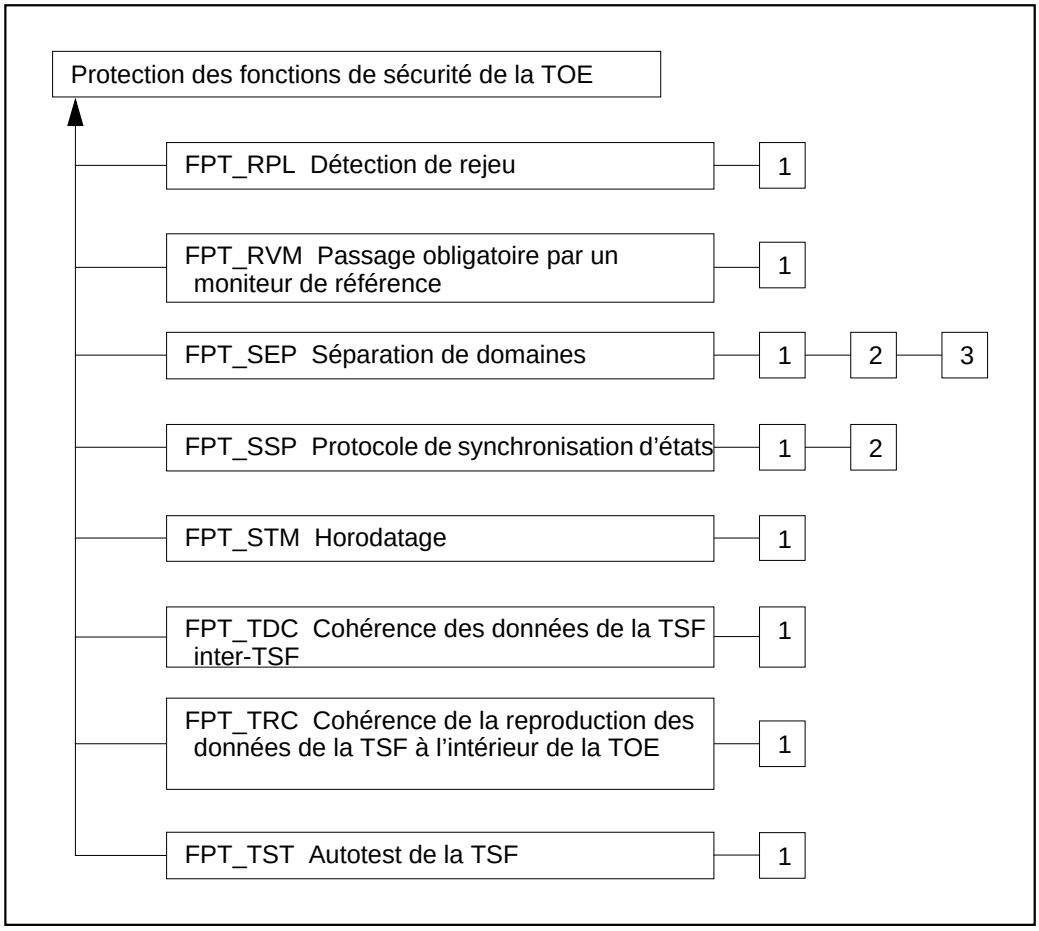


Figure 10.2 - Décomposition de la classe "Protection des fonctions de sécurité de la TOE" (suite)

1172 Du point de vue de cette classe, il y a trois parties importantes qui composent la TSF :

a) la *machine abstraite* de la TSF, qui est la machine virtuelle ou physique sur laquelle s'exécute l'implémentation spécifique de la TSF en cours d'évaluation.

b) l'*implémentation* de la TSF, qui s'exécute sur la machine abstraite et implémente les mécanismes qui mettent en oeuvre la TSP.

c) les *données* de la TSF, qui sont les bases de données d'administration qui guident l'application de la TSP.

1173 Toutes les familles de la classe FPT peuvent être liées à ces domaines, et font partie de l'un des groupes suivants:

a) FPT_PHP (Protection physique de la TSF), qui procure à un utilisateur autorisé la possibilité de détecter des attaques externes sur des parties de la TOE qui incluent la TSF.

b) FPT_AMT (Test de la machine abstraite sous-jacente) et FPT_TST (Autotest de la TSF), qui procurent à un utilisateur autorisé la possibilité de vérifier le fonctionnement correct de la machine abstraite sous-jacente et de la TSF ainsi que l'intégrité des données de la TSF et du code exécutable.

c) FPT_SEP (Séparation de domaines) et FPT_RVM (Passage obligatoire par un moniteur de référence), qui protègent la TSF pendant l'exécution et garantissent que la TSF ne peut pas être court-circuitée. Lorsque des composants appropriés de ces familles sont combinés avec les composants appropriés de ADV_INT (Parties internes de la TSF), on peut dire que la TOE possède ce qui est appelé traditionnellement un "moniteur de référence."

d) FPT_RCV (Reprise sûre), FPT_FLS (Mode sûr après défaillance) et FPT_TRC (Cohérence de la reproduction des données de la TSF à l'intérieur de la TOE), qui concernent le comportement de la TSF au moment où une défaillance se produit et immédiatement après.

e) FPT_ITA (Disponibilité de données de la TSF exportées), FPT_ITC (Confidentialité des données de la TSF exportées), FPT_ITI (Intégrité des données de la TSF exportées), qui concernent la protection et la disponibilité de données de la TSF entre la TSF et un produit TI de confiance distant.

f) FPT_ITT (Transfert des données de la TSF à l'intérieur de la TOE), qui concerne la protection de données de la TSF lorsqu'elles sont transmises entre des parties physiquement séparées de la TOE.

g) FPT_RPL (Détection de rejeu), qui concerne le rejeu de divers types d'informations ou d'opérations.

h) FPT_SSP (Protocole de synchronisation d'états), qui concerne la synchronisation d'états, en fonction de données de la TSF, entre différentes parties d'une TSF distribuée.

i) FPT_STM (Horodatage), qui concerne l'horodatage fiable.

j) FPT_TDC (Cohérence des données de la TSF inter-TSF), qui concerne la cohérence de données de la TSF partagées entre la TSF et un produit TI de confiance distant.

J.1 Test de la machine abstraite sous-jacente (FPT_AMT)

1174 La présente famille définit les exigences pour les tests par la TSF des hypothèses de sécurité faites au sujet de la machine abstraite sous-jacente sur laquelle la TSF repose. Cette machine “abstraite” pourrait être une plate-forme matérielle ou micro-programmée, ou bien être une association connue et testée de matériel et de logiciel agissant comme une machine virtuelle. Des exemples de tels tests pourraient être le test de protection de page matérielle, l’envoi d’échantillon de paquets via un réseau pour garantir la réception, et la vérification du comportement de l’interface machine virtuelle. Ces tests peuvent être menés pendant un certain état de maintenance, au démarrage, en ligne ou de façon continue. Les actions à entreprendre par la TOE au vu des résultats des tests sont définis dans la famille FPT_RCV.

Notes pour l’utilisateur

1175 L’expression “machine abstraite sous-jacente” se réfère typiquement aux composants matériels sur lesquels la TSF a été implémentée. Cependant, l’expression peut aussi être utilisée pour désigner une combinaison sous-jacente de matériel et de logiciel, préalablement évaluée, se comportant comme une machine virtuelle sur laquelle la TSF repose.

1176 Les tests de la machine abstraite peuvent prendre des formes diverses :

a) **Tests de mise en route**. Ces sont les tests qui garantissent le fonctionnement correct de la plate-forme sous-jacente. Pour du matériel et des micro-programmes, cela pourrait inclure le test d’éléments tels que des cartes mémoire, des chemins de données, des bus, des logiques de contrôle, des registres de processeur, des ports de communication, des interfaces de console, des hauts-parleurs et des périphériques. Pour des éléments logiciels (machine virtuelle), cela devrait inclure la vérification que l’initialisation et le comportement sont corrects.

b) **Tests chargeables**. Ce sont des tests qui pourraient être chargés et exécutés par un utilisateur autorisé ou être activés par des conditions spécifiques. Cela pourrait inclure des tests de fatigue de composants de processeurs (unités logiques, unités de calcul, etc.) et un contrôle de mémoire.

Notes pour l’évaluateur

1177 Les tests de la machine abstraite sous-jacente devraient être suffisants pour tester l’ensemble des caractéristiques de la machine abstraite sous-jacente sur laquelle la TSF se repose.

FPT_AMT.1 Test de la machine abstraite

Notes d'application pour l'utilisateur

1178 Ce composant contribue au test périodique des hypothèses de sécurité de la machine abstraite sous-jacente dont dépend le fonctionnement de la TSF, en exigeant la possibilité de faire appel de façon périodique aux fonctions de test.

1179 L'auteur du PP ou de la ST peut raffiner l'exigence pour spécifier si la fonction devrait être disponible dans un mode hors ligne, en ligne ou de maintenance.

Notes d'application de l'évaluateur

1180 Il est acceptable que les fonctions de test périodique soient disponibles seulement dans un mode hors ligne ou de maintenance. Des contrôles devraient être mis en place pour limiter l'accès aux utilisateurs autorisés pendant la maintenance.

Opérations

Sélection :

1181 **Dans FPT_AMT.1.1, l'auteur du PP ou de la ST devrait spécifier quand la TSF effectuera le test de la machine abstraite, pendant le démarrage initial, de façon périodique pendant le fonctionnement normal, à la demande d'un utilisateur autorisé, ou dans d'autres conditions. Dans ce dernier cas, l'auteur du PP ou de la ST devrait raffiner ces conditions. L'auteur du PP ou de la ST, par cette sélection, a la possibilité d'indiquer la fréquence avec laquelle les auto-tests seront exécutés. Si les tests sont exécutés fréquemment, alors les utilisateurs finaux devraient avoir une confiance plus grande dans le fait que la TOE fonctionne correctement que dans le cas où les tests sont exécutés moins fréquemment. Cependant, ce besoin d'avoir confiance dans le fait que la TOE fonctionne correctement doit être comparé à l'impact potentiel sur la disponibilité de la TOE, dans la mesure où souvent les auto-tests peuvent retarder le fonctionnement normal d'une TOE.**

J.2 Mode sûr après défaillance (FPT_FLS)

1182 Les exigences de cette famille garantissent que la TOE ne violera pas sa propre TSP dans le cas où se produiraient certaines catégories identifiées de défaillances dans la TSF.

FPT_FLS.1 Défaillance avec préservation d'un état sûr

Notes d'application pour l'utilisateur

1183 L'expression "état sûr" désigne un état dans lequel les données de la TSF sont cohérentes et la TSF continue à appliquer correctement la TSP. "L'état sûr" est défini dans le modèle de TSP. Si le développeur a donné une définition claire de l'état sûr et la raison pour laquelle il devrait être considéré comme sûr, la suppression de la dépendance de FPT_FLS.1 envers ADV_SPM.1 peut être justifiée.

1184 Bien qu'il soit souhaitable d'auditer des situations dans lesquelles se produit une défaillance avec préservation d'un état sûr, il n'est pas possible de le faire dans toutes les situations. L'auteur du PP ou de la ST devrait spécifier les situations dans lesquelles l'audit est souhaité et faisable.

1185 Les défaillances dans la TSF peuvent inclure des défaillances de type matériel, qui indiquent le dysfonctionnement d'un équipement et qui peuvent nécessiter une maintenance, une prestation de service ou une réparation de la TSF. Les défaillances dans la TSF peuvent aussi inclure des défaillances de type logiciel, qui peuvent être corrigées et qui peuvent seulement exiger de ré-initialiser ou de paramétrer à nouveau la TSF.

Opérations

Affectation :

1186 **Dans FPT_FLS.1.1, l'auteur du PP ou de la ST devrait énumérer les types de défaillances dans la TSF pour laquelle la TSF devrait "tomber en panne en se retrouvant dans un état sûr," c'est-à-dire qu'elle devrait préserver un état sûr et continuer d'appliquer correctement la TSP.**

J.3 Disponibilité de données de la TSF exportées (FPT_ITA)

1187 La présente famille définit les règles pour prévenir la perte de disponibilité des données de la TSF transitant entre la TSF et un produit TI de confiance distant. Ces données pourraient, par exemple, être des données critiques pour la TSF telles que des mots de passe, des clés, des données d'audit ou du code exécutable de la TSF.

Notes d'application pour l'utilisateur

1188 Cette famille est utilisée dans le contexte d'un système distribué où la TSF fournit des données de la TSF à un produit TI de confiance distant. La TSF peut seulement prendre des mesures sur le site où elle est installée et ne peut pas être tenue responsable de la TSF de l'autre produit TI de confiance.

1189 S'il existe une métrique de disponibilités différente pour les différents types de données de la TSF, alors ce composant devrait être itéré pour chaque couple unique de métrique et de type de données de la TSF.

FPT_ITA.1 Disponibilité inter-TSF dans la limite d'une métrique de disponibilité définie

Opérations

Affectation :

1190 **Pour FPT_ITA.1.1, l'auteur du PP ou de la ST devrait spécifier les types de données de la TSF qui sont soumis à la métrique de disponibilité.**

1191 **Pour FPT_ITA.1.1, le PP ou la ST devrait spécifier la métrique de disponibilité pour les données applicables de la TSF.**

1192 **Pour FPT_ITA.1.1, l'auteur du PP ou de la ST devrait spécifier les conditions dans lesquelles la disponibilité doit être assurée, telle que par exemple : il doit y avoir une connexion entre la TOE et le produit TI de confiance distant.**

J.4 Confidentialité des données de la TSF exportées (FPT_ITC)

1193 La présente famille définit les règles pour la protection contre une divulgation non autorisée de données de la TSF transitant entre la TSF et un produit TI de confiance distant. De telles données sont par exemple des données critiques pour la TSF telles que des mots de passe, des clés, des données d'audit ou du code exécutable de la TSF.

Notes d'application pour l'utilisateur

1194 Cette famille est utilisée dans le contexte d'un système distribué où la TSF fournit des données de la TSF à un produit TI de confiance distant. La TSF peut seulement prendre des mesures sur le site où elle est installée et ne peut pas être tenue responsable de la TSF de l'autre produit TI de confiance.

FPT_ITC.1 Confidentialité inter-TSF pendant une transmission

Notes d'application de l'évaluateur

1195 La confidentialité de données de la TSF pendant une transmission est nécessaire pour protéger de telles informations contre une divulgation. Certaines implémentations possibles qui pourraient procurer la confidentialité comprennent l'utilisation d'algorithmes cryptographiques ainsi que des techniques à large spectre.

J.5 Intégrité des données de la TSF exportées (FPT_ITI)

1196 La présente famille définit les règles pour la protection contre une modification non autorisée des données de la TSF pendant leur transmission entre la TSF et un produit TI de confiance distant. De telles données sont par exemple des données critiques pour la TSF telles que des mots de passe, des clés, des données d'audit ou du code exécutable de la TSF.

Notes d'application pour l'utilisateur

1197 Cette famille est utilisée dans le contexte d'un système distribué où la TSF fournit des données de la TSF à un produit TI de confiance distant. Il est à noter qu'une exigence qui concerne la modification, la détection ou la reprise dans un produit TI de confiance distant ne peut pas être spécifiée, car les mécanismes qu'un produit TI de confiance distant utilisera pour protéger ses données ne peuvent pas être déterminés à l'avance. Pour cette raison, ces exigences sont exprimées en des termes tels que "la TSF procure une possibilité" que le produit TI de confiance distant peut utiliser.

FPT_ITI.1 Détection inter-TSF d'une modification

Notes d'application pour l'utilisateur

1198 Ce composant devrait être utilisé dans des situations où il est suffisant de détecter quand des données ont été modifiées. Un exemple d'une telle situation est celle où le produit TI de confiance distant peut exiger que la TSF de la TOE retransmette les données quand la modification a été détectée, ou réponde à de tels types de requêtes.

1199 La force souhaitée de la détection d'une modification est basée sur une métrique de modification spécifiée qui est une fonction de l'algorithme utilisé ; ce dernier peut consister en une somme de contrôle faible et des mécanismes de parité pouvant ne pas réussir à détecter plusieurs changements de bits, ou des sommes de contrôle cryptographiques plus compliquées.

Opérations

Affectation :

1200 **Pour FPT_ITI.1.1, le PP ou la ST devrait spécifier la métrique de modification que le mécanisme de détection doit satisfaire. Cette métrique de modification doit spécifier la force souhaitée de la détection de modification.**

1201 **Pour FPT_ITI.1.2, le PP ou la ST devrait spécifier les actions à entreprendre si une modification de données de la TSF a été détectée. Un exemple d'action est : "ignorer les données de la TSF et exiger que le produit de confiance émetteur envoie à nouveau les données de la TSF".**

FPT_ITI.2 Détection et correction inter-TSF d'une modification

Notes d'application pour l'utilisateur

1202 Ce composant devrait être utilisé dans des situations où il est nécessaire de détecter ou de corriger des modifications de données critiques de la TSF.

1203 La force souhaitée de la détection d'une modification est basée sur une métrique de modification spécifiée qui est une fonction de l'algorithme utilisé ; ce dernier peut consister en une somme de contrôle faible et des mécanismes de parité pouvant ne pas réussir à détecter plusieurs changements de bits, ou des sommes de contrôle cryptographiques plus compliquées. La métrique qui doit être définie peut soit désigner les attaques auxquelles elle résistera (e.g. seulement 1 modification pour 1000 messages aléatoires sera acceptée), soit des mécanismes qui sont reconnus dans la littérature publique (e.g. la résistance doit être conforme à la résistance offerte par l'algorithme "Secure Hash Algorithm").

1204 L'approche choisie pour corriger une modification pourrait être satisfaite au moyen de certaines sommes de contrôle correctrices d'erreurs.

Notes pour l'évaluateur

1205 Certains moyens possibles pour satisfaire cette exigence impliquent l'utilisation de fonctions cryptographiques ou de certaines sommes de contrôle.

Opérations

Affectation :

1206 Pour FPT_ITI.2.1, le PP ou la ST devrait spécifier la métrique de modification que le mécanisme de détection doit satisfaire. Cette métrique de modification doit spécifier la force souhaitée de la détection de modification.

1207 Pour FPT_ITI.2.2, le PP ou la ST devrait spécifier les actions à entreprendre si une modification de données de la TSF a été détectée. Un exemple d'action est : "ignorer les données de la TSF et exiger que le produit de confiance émetteur envoie à nouveau les données de la TSF".

1208 **Pour FPT_ITI.2.3, l'auteur du PP ou de la ST devrait définir les types de modifications à partir desquelles la TSF devrait être capable d'effectuer une reprise.**

J.6 Transfert des données de la TSF à l'intérieur de la TOE (FPT_ITT)

1209 Cette famille fournit des exigences qui traitent de la protection des données de la TSF quand elles sont transférées entre des parties séparées d'une TOE via un canal interne.

Notes pour l'utilisateur

1210 La détermination du degré de séparation (i.e., physique ou logique) qui rendrait utile l'application de cette famille dépend de l'environnement d'utilisation prévu. Dans un environnement hostile, il peut y avoir des risques provenant de transferts entre des parties de la TOE séparées seulement par un bus système ou par un canal de communication inter-processus. Dans des environnements moins hostiles, les transferts peuvent être effectués via des réseaux plus traditionnels.

Notes pour l'évaluateur

1211 Un mécanisme pratique dont dispose une TSF pour procurer cette protection est basé sur la cryptographie.

FPT_ITT.1 Protection élémentaire des données de la TSF lors d'un transfert interne

Opérations

Sélection :

1212 **Dans FPT_ITT.1.1, l'auteur du PP ou de la ST devrait spécifier le type de protection souhaité à procurer à partir des choix suivants : contre la divulgation ou contre la modification.**

FPT_ITT.2 Séparation des données de la TSF pendant un transfert

Notes d'application pour l'utilisateur

1213 Un des moyens de parvenir à la séparation de données de la TSF en fonction d'attributs touchant à la SFP est d'utiliser des canaux logiques ou physiques séparés.

Opérations

Sélection :

1214 Dans FPT_ITT.2.1, l'auteur du PP ou de la ST devrait spécifier le type de protection souhaité à procurer à partir des choix suivants : contre la divulgation ou contre la modification.

FPT_ITT.3 Contrôle de l'intégrité des données de la TSF

Opérations

Sélection :

1215 **Dans FPT_ITT.3.1, l'auteur du PP ou de la ST devrait spécifier le type de modification souhaité que la TSF doit être capable de détecter. L'auteur du PP ou de la ST devrait le choisir à partir de la liste suivante : modification de données, substitution de données, ré-ordonnancement de données, suppression de données ou toute autre erreur d'intégrité.**

Affectation :

1216 **Dans FPT_ITT.3.1, si l'auteur du PP ou de la ST choisit la dernière option mentionnée dans le paragraphe précédent, alors l'auteur devrait aussi spécifier les autres erreurs d'intégrité que la TSF devrait être capable de détecter.**

1217 **Dans FPT_ITT.3.2, l'auteur du PP ou de la ST devrait spécifier l'action à entreprendre quand une erreur d'intégrité est identifiée.**

J.7 Protection physique de la TSF (FPT_PHP)

1218 Les composants de protection physique de la TSF se réfèrent à des restrictions concernant l'accès physique non autorisé à la TSF, et à la dissuasion ainsi qu'à la résistance contre une modification physique non autorisée ou une substitution de la TSF.

1219 Les exigences de cette famille garantissent que la TSF est protégée contre des intrusions physique et des interférences. La satisfaction des exigences de ces composants fait que la TSF est conditionnée et utilisée d'une telle manière que les intrusions physiques soient détectables, ou que la résistance aux intrusions physiques soit mesurable en fonction de facteurs de travail définis. Sans ces composants, les fonctions de protection d'une TSF perdent leur efficacité dans des environnements où les dégâts physiques ne peuvent pas être empêchés. Ce composant présente également des exigences concernant la façon dont la TSF doit répondre aux tentatives d'intrusion physique.

1220 Des exemples de scénarios d'intrusion physique comprennent une attaque mécanique, des radiations, un changement de température.

Notes pour l'utilisateur

1221 Il est acceptable que les fonctions dont dispose un utilisateur autorisé pour détecter une intrusion physique ne soient disponibles que dans un mode hors ligne ou de maintenance. Des contrôles devraient être mis en place pour limiter l'accès aux utilisateurs autorisés pendant de tels modes. Comme la TSF peut ne pas être "opérationnelle" pendant ces modes, elle peut ne pas être capable d'assurer l'accès normal pour les utilisateurs autorisés. L'implémentation physique d'une TOE pourrait consister en plusieurs structures : par exemple un blindage externe, des cartes et des circuits intégrés. Ces "éléments" dans leur ensemble doivent protéger (protéger, notifier et résister) la TSF des intrusions physiques. Cela ne signifie pas que tous les dispositifs doivent offrir ces caractéristiques, mais la structure physique complète dans son ensemble devrait le faire.

1222 Il y a seulement un audit minimal associé à ces composants dû au fait qu'il est possible que les mécanismes de détection et d'alarme soient entièrement implémentés dans du matériel, en deçà du niveau d'interaction d'un sous-système d'audit (par exemple, un système de détection basé sur du matériel dans le cas d'une coupure de circuit et qui alimente une diode à émission de lumière (LED) si le circuit est coupé quand l'utilisateur autorisé appuie sur un bouton). Néanmoins, un auteur de PP ou de ST peut déterminer qu'il est nécessaire d'auditer les intrusions physiques pour une menace particulière prévue dans l'environnement. Si tel est le cas, l'auteur du PP ou de la ST devrait inclure des exigences appropriées dans la liste des événements d'audit. Il est à noter que l'inclusion de ces exigences peut avoir des implications sur la conception du matériel et sur son interface avec le logiciel.

FPT_PHP.1 Détection passive d'une attaque physique

Notes d'application pour l'utilisateur

1223 Le composant FPT_PHP.1 devrait être utilisé quand des menaces d'intrusion physique non autorisée dans des parties de la TOE ne sont pas contrées par des méthodes procédurales. Il couvre la menace d'intrusions physiques non détectées dans la TSF. Typiquement, un utilisateur autorisé se verrait attribuer la fonction destinée à vérifier si une intrusion a eu lieu. Tel qu'il est écrit, ce composant offre simplement à une TSF la possibilité de détecter des intrusions. La dépendance envers le composant FMT_MOF.1 est nécessaire pour spécifier qui peut utiliser cette possibilité et la façon de l'utiliser. Si cette fonction est réalisée par des mécanismes non TI (e.g. par une inspection physique) on pourrait justifier de ne pas satisfaire la dépendance envers FMT_MOF.1.

FPT_PHP.2 Notification d'une attaque physique

Notes d'application pour l'utilisateur

1224 Le composant FPT_PHP.2 devrait être utilisé quand des menaces d'intrusion physique non autorisée dans des parties de la TOE ne sont pas contrées par des méthodes procédurales et qu'il est exigé de notifier les intrusions physiques à des individus désignés. Il couvre la menace que des intrusions physiques dans des éléments de la TSF, bien que détectées, puisse ne pas être notifiées.

Opérations

Affectation :

1225 **Dans FPT_PHP.2.3, l'auteur du PP ou de la ST devrait fournir une liste des dispositifs ou éléments de la TSF pour lesquels la détection active d'intrusion physique est exigée.**

1226 **Dans FPT_PHP.2.3, l'auteur du PP ou de la ST devrait désigner un utilisateur ou un rôle auquel les intrusions doivent être notifiées quand elles sont détectées. Les types d'utilisateurs ou de rôles peuvent varier en fonction du composant d'administration de sécurité particulier (tiré de la famille FMT_MOF.1) inclus dans le PP ou la ST.**

FPT_PHP.3 Résistance à une attaque physique

1227 Pour certaines formes d'intrusion, il est nécessaire que la TSF non seulement détecte les intrusions, mais lui résiste effectivement ou retarde l'attaquant.

Notes d'application pour l'utilisateur

1228 Ce composant devrait être utilisé quand des dispositifs et des éléments de la TSF sont prévus pour fonctionner dans un environnement où des intrusions physiques (e.g. une observation, une analyse ou une modification) à l'intérieur d'un dispositif ou d'un élément de la TSF elle-même constituent une menace.

Opérations

Affectation :

1229 **Dans FPT_PHP.3.1, l'auteur du PP ou de la ST devrait spécifier les scénarios d'intrusion pour une liste de dispositifs ou d'éléments de la TSF pour lesquels la TSF devrait opposer une résistance aux intrusion physique. Cette liste peut être appliquée à un sous-ensemble défini de dispositifs et éléments physiques de la TSF en fonction de considérations telles que les limitations de technologie et l'exposition physique relative du dispositif. Un tel paramétrage devrait être clairement défini et justifié. De plus, la TSF devrait répondre automatiquement aux intrusions physiques. La réponse automatique devrait être telle que la politique du dispositif soit préservée ; par exemple, avec une politique de confidentialité, il serait acceptable de désactiver physiquement le dispositif de telle façon que les informations protégées ne puissent pas être retrouvées.**

1230 **Dans FPT_PHP.3.1, l'auteur du PP ou de la ST devrait spécifier la liste des dispositifs ou des éléments de la TSF pour lesquels la TSF devrait opposer une résistance aux intrusions physiques pour les scénarios qui ont été identifiés.**

J.8 Reprise sûre (FPT_RCV)

1231 Les exigences de cette famille garantissent que la TSF peut déterminer que le démarrage de la TOE a été fait sans compromettre sa protection et qu'elle peut reprendre son fonctionnement à la suite d'une interruption des opérations sans compromettre sa protection. Cette famille est importante parce que l'état au démarrage de la TSF détermine la protection des états suivants.

1232 Les composants de reprise reconstruisent les état sûrs de la TSF ou empêchent les transitions vers des états non sûrs, en réponse directe à des occurrences de défaillances attendues, des interruptions de fonctionnement ou de démarrage. Les défaillances qui doivent être généralement prévues comprennent :

a) Des défaillances non modifiables d'actions qui aboutissent toujours à un crash système (e.g. incohérence persistante de tables critiques du système, transferts non contrôlés dans le code de la TSF provoqué par des défaillances transitoires du matériel ou des micro-programmes, défaillances d'alimentation, défaillances du processeur, défaillances dans les communications).

b) Des défaillances de support provoquant la non accessibilité ou l'altération de tout ou partie du support représentant les objets de la TSF (e.g. erreurs de parité, détérioration du support magnétique par la de tête de disque, défaillance persistante en lecture et écriture provoquée par un mauvais alignement des têtes du disque, revêtement magnétique usé, présence de poussières sur la surface du disque).

c) Une interruption de fonctionnement provoquée par une action erronée ou effectuée au mauvais moment (e.g. arrêts non prévus dus à une coupure d'alimentation, à l'absence de prise en compte de l'épuisement de ressources critiques, à une configuration d'installation inadéquate).

1233 Il est à noter que la reprise peut être faite à partir d'un scénario de défaillance complet ou partiel. Bien qu'une défaillance totale pourrait se produire dans un système d'exploitation monolithique, il est moins vraisemblable dans un environnement distribué. Dans de tels environnements, des sous-systèmes peuvent tomber en panne, mais les autres parties restent opérationnelles. De plus, les composants critiques peuvent être redondants (disques miroirs, routages alternatifs), et des points de reprise peuvent être disponibles. Ainsi, la reprise est exprimée en termes de reprise dans un état sûr.

1234 Cette famille identifie un mode de maintenance. Dans ce mode de maintenance, le fonctionnement normal pourrait être impossible ou sévèrement restreint, car sinon des situations non sûres pourraient se produire. De façon typique, seuls des utilisateurs autorisés devraient être autorisés à accéder à ce mode, les détails des personnes qui peuvent accéder à ce mode sont donnés dans une fonction de la Classe FMT Administration de la sécurité. Si la classe FMT n'impose aucun contrôle sur les personnes qui peuvent accéder à ce mode, alors il peut être acceptable de permettre à tout utilisateur de restaurer le système si la TOE se trouve

dans un tel un état. Cependant, en pratique, cela n'est probablement pas souhaitable car l'utilisateur, en restaurant le système a la possibilité de configurer la TOE de manière telle qu'il peut violer la TSP.

1235 Les mécanismes conçus pour détecter des conditions exceptionnelles pendant le fonctionnement sont couverts par la famille FPT_TST (Autotest de la TSF), FPT_FLS (Mode sûr après défaillance), et d'autres parties qui traitent du concept de "sûreté du logiciel."

Notes pour l'utilisateur

1236 Dans cette famille, l'expression "état sûr" est utilisée. Elle désigne un certain état dans lequel la TOE contient des données de la TSF cohérentes et une TSF qui peut appliquer correctement la politique. Cet état peut être le démarrage initial (boot) d'un système sain, ou ce pourrait être un certain état issu d'un point de reprise. L'"état sûr" est défini dans le modèle de TSP. Si le développeur a donné une définition claire de l'état sûr et la raison pour laquelle il devrait être considéré comme sûr, la suppression de la dépendance de FPT_FLS.1 envers ADV_SPM.1 peut être justifiée.

FPT_RCV.1 Reprise manuelle

1237 Dans la hiérarchie de la famille "Reprise sûre", la reprise qui exige seulement une intervention manuelle est la moins souhaitable, car elle exclut un fonctionnement automatique du système.

Notes d'application pour l'utilisateur

1238 Ce composant est destiné à être utilisé dans des TOE qui n'exigent pas une reprise automatique vers un état sûr. Les exigences de ce composant réduisent la menace d'une détérioration de la protection résultant du retour dans un état non sûr d'une TOE surveillée par un opérateur, après reprise à la suite d'une défaillance ou d'une autre interruption.

Notes d'application de l'évaluateur

1239 Le fait que les fonctions disponibles à un utilisateur autorisé pour une reprise sûre soient seulement disponibles dans un mode de maintenance est acceptable. Des contrôles devraient être mis en place pour limiter l'accès aux utilisateurs autorisés pendant la maintenance.

FPT_RCV.2 Reprise automatisée

1240 La reprise automatisée est considérée comme plus utile que la reprise manuelle, car elle permet à la machine de fonctionner sans opérateur.

Notes d'application pour l'utilisateur

1241 Le composant FPT_RCV.2 étend la propriété de couverture de FPT_RCV.1 en exigeant qu'il y ait au moins une méthode automatisée de reprise à la suite d'une

défaillance ou d'une interruption de service. Il couvre la menace d'une détérioration de la protection résultant du retour dans un état non sûr d'une TOE non surveillée par un opérateur, après reprise à la suite d'une défaillance ou d'une autre interruption.

Notes d'application de l'évaluateur

1242 Le fait que les fonctions disponibles à un utilisateur autorisé pour une reprise sûre soient seulement disponibles dans un mode de maintenance est acceptable. Des contrôles devraient être mis en place pour limiter l'accès aux utilisateurs autorisés pendant la maintenance.

1243 Dans FPT_RCV.2.1, il est de la responsabilité du développeur de la TSF de déterminer l'ensemble des défaillances et des interruptions de service récupérables.

1244 La robustesse des mécanismes de reprise automatisée est supposée être vérifiée.

Opérations

Affectation :

1245 **Dans FPT_RCV.2.2, l'auteur du PP ou de la ST devrait spécifier la liste des défaillances ou autres interruptions de service pour lesquelles une reprise automatisée doit être possible.**

FPT_RCV.3 Reprise automatisée sans perte indue

1246 La reprise automatisée est considérée comme plus utile que la reprise manuelle, mais le risque de perdre d'un nombre substantiel d'objets existe. Empêcher la perte indue d'objets procure une utilité supplémentaire à l'effort de reprise.

Notes d'application pour l'utilisateur

1247 Le composant FPT_RCV.3 étend la propriété de couverture de FPT_RCV.2 en exigeant qu'il n'y ait pas de perte indue de données de la TSF ou d'objets dans le TSC. Dans FPT_RCV.2, on pourrait imaginer que les mécanismes de reprise automatisée effectuent la reprise en supprimant tous les objets et en retournant la TSF dans un état sûr connu. Ce type de reprise automatisée drastique est exclue dans FPT_RCV.3.

1248 Ce composant couvre la menace d'une détérioration de la protection résultant du retour dans un état non sûr d'une TOE non surveillée par un opérateur, après reprise à la suite d'une défaillance ou d'une autre interruption accompagnée de pertes importantes de données de la TSF et d'objets dans le TSC.

Notes d'application de l'évaluateur

1249 Le fait que les fonctions disponibles à un utilisateur autorisé pour une reprise sûre soient seulement disponibles dans un mode de maintenance est acceptable. Des

contrôles devraient être mis en place pour limiter l'accès aux utilisateurs autorisés pendant la maintenance.

1250 La robustesse des mécanismes de reprise automatisée est supposée être vérifiée.

Opérations

Affectation :

1251 Dans FPT_RCV.3.2, l'auteur du PP ou de la ST devrait spécifier la liste des défaillances ou d'autres discontinuities pour lesquelles une reprise automatisée doit être possible.

1252 **Dans FPT_RCV.3.3, l'auteur du PP ou de la ST devrait quantifier les pertes acceptables de données ou d'objets de la TSF.**

FPT_RCV.4 Reprise de fonction

1253 La reprise de fonction exige que, dans le cas où il devrait y avoir une défaillance dans la TSF, certaines SF de la TSF devraient soit se terminer avec succès, soit reprendre leur exécution dans un état sûr.

Opérations

Affectation :

1254 **Dans FPT_RCV.4.1, l'auteur du PP ou de la ST devrait spécifier une liste de SF et de scénarios de défaillance. Dans le cas où l'un des scénarios de défaillance identifiés se produit, les SF qui ont été spécifiées doivent soit se terminer avec succès, soit reprendre leur exécution dans un état sûr.**

J.9 Détection de rejeu (FPT_RPL)

1255 Cette famille traite de la détection de rejeu pour divers types d'entités et des actions de correction qui s'ensuivent.

FPT_RPL.1 Détection de rejeu

Notes d'application pour l'utilisateur

1256 Les entités comprises ici sont par exemple des messages, des demandes de service, des réponses de service, ou des sessions.

Opérations

Affectation :

1257 **Dans FPT_RPL.1.1, l'auteur du PP ou de la ST devrait fournir une liste des entités identifiées pour lesquelles la détection de rejeu devrait être possible. De telles entités pourraient inclure par exemple des messages, des demandes de service, des réponses de service, et des sessions utilisateur.**

1258 **Dans FPT_RPL.1.2, l'auteur du PP ou de la ST devrait spécifier la liste des actions à entreprendre par la TSF quand un rejeu est détecté. L'ensemble potentiel des actions qui peuvent être entreprises inclut les actions suivantes : ignorer l'entité objet du rejeu, demander confirmation de l'entité à la source identifiée et clore le sujet d'où provient l'entité qui a fait l'objet du rejeu.**

J.10 Passage obligatoire par un moniteur de référence (FPT_RVM)

1259 Les composants de cette famille couvrent l'aspect "systématiquement appelé" d'un moniteur de référence traditionnel. Le but de ces composants est de garantir, par rapport au TSC, que toutes les actions exigeant la mise en œuvre de la politique par des sujets non sûrs vis-à-vis de tout ou partie de cette SFP sur des objets contrôlés par cette SFP, sont validées par la TSF par rapport à la SFP. Si la partie de la TSF qui applique la SFP satisfait également aux exigences des composants appropriés des familles FPT_SEP (Séparation de domaines) et ADV_INT (Parties internes de la TSF), alors cette partie de la TSF fournit un "moniteur de référence" pour cette SFP.

1260 Le moniteur de référence est la partie de la TSF responsable de la mise en œuvre de la TSP ; il possède les trois caractéristiques suivantes :

a) Des sujets non sûrs ne peuvent pas interférer avec son fonctionnement, i.e. il est à l'épreuve d'une intrusion physique. Cela est pris en compte par les composants de la famille FPT_SEP.

b) Des sujets non sûrs ne peuvent pas court-circuiter les contrôles qu'il effectue, i.e. il est systématiquement appelé. Cela est pris en compte par les composants de la famille FPT_RVM.

c) Il est suffisamment simple pour être analysé et pour que son comportement soit compris (i.e. sa conception est simple). Cela est pris en compte par les composants de la famille ADV_INT.

1261 Le composant de cette famille stipule que "la TSF doit garantir que les fonctions d'application de la TSP sont appelées et s'achèvent avec succès avant que la moindre fonction dans le TSC ne soit autorisée à démarrer." Dans tout système (distribué ou autre), il existe un nombre fini de fonctions responsables de l'application de la TSP. Il n'y a rien dans cette exigence qui oblige ou prescrive qu'une fonction unique soit appelée pour gérer la sécurité. Au contraire, elle permet à plusieurs fonctions de remplir le rôle de moniteur de référence et l'ensemble de ces fonctions responsables de la mise en œuvre de la TSP est tout simplement appelé le moniteur de référence. Cependant, cela doit être relativisé par l'objectif de faire en sorte que le "moniteur de référence" reste simple.

1262 Une TSF qui implémente une SFP procure une protection efficace contre des fonctions non autorisées, si et seulement si toutes les actions applicables (e.g. accès à des objets) exigées par des sujets non sûrs vis-à-vis de tout ou partie de cette SFP sont validées par la TSF avant de s'exécuter. Si l'action applicable est exécutée de façon incorrecte ou court-circuitée, l'application de la SFP dans son ensemble est compromise. Des sujets "non sûrs" pourraient alors court-circuiter la SFP de plusieurs façons non autorisées (e.g. contourner des vérifications d'accès pour certains sujets ou objets, court-circuiter des vérifications pour des objets dont la protection était supposée réalisée par des applications, prolonger des droits d'accès au delà de leur durée de vie prévue, court-circuiter l'audit d'actions auditées ou

court-circuiter l'authentification). Il est à noter que l'expression "sujets non sûrs" désigne des sujets non sûrs vis-à-vis de tout ou partie de la SFP spécifique qui est appliquée ; un sujet peut être sûr vis-à-vis d'une SFP et non sûr vis-à-vis d'une SFP différente.

FPT_RVM.1 Capacité de la TSP à ne pas être contournée

Notes d'application pour l'utilisateur

1263 Afin d'obtenir l'équivalent d'un moniteur de référence, ce composant doit être utilisé soit avec FPT_SEP.2 (Séparation de domaines pour la SFP) soit avec FPT_SEP.3 (Moniteur de référence complet) et ADV_INT.3 (Minimisation de la complexité). De plus, si un moniteur de référence complet est exigé, les composants de la Classe FDP Protection des données de l'utilisateur doivent couvrir tous les objets.

J.11 Séparation de domaines (FPT_SEP)

1264 Les composants de cette famille garantissent qu'au moins un domaine de sécurité soit disponible pour l'exécution de la TSF elle-même et que la TSF est protégée contre des interférences et des intrusions d'origines externes (e.g. par modification du code de la TSF ou des structures de données) par des sujets non sûrs. La satisfaction des exigences de cette famille rend la TSF auto-protectrice, ce qui signifie qu'un sujet non sûr ne peut pas modifier ou endommager la TSF.

1265 Cette famille exige que :

a) les ressources du domaine de sécurité de la TSF ("domaine protégé") et celles des sujets et des entités libres externes au domaine soient séparées, de telle façon que les entités externes au domaine protégé ne puissent pas observer ou modifier des données de la TSF ou du code de la TSF à l'intérieur du domaine protégé ;

b) les transferts entre domaines soient contrôlés, de telle sorte qu'il ne soit pas possible d'entrer dans le domaine protégé ou d'en sortir de façon arbitraire ;

c) les paramètres de l'utilisateur ou de l'application passés dans le domaine protégé par adresses soient validés en fonction de l'espace adressable du domaine protégé et ceux passés par valeurs soient validés en fonction des valeurs attendues par le domaine protégé ;

d) les domaines de sécurité des sujets soient distincts sauf pour les parties communes contrôlées via la TSF.

Notes pour l'utilisateur

1266 Cette famille est exigée chaque fois que la confiance dans le fait que la TSF n'a pas été altérée est requise.

1267 Afin d'obtenir l'équivalent d'un moniteur de référence, les composants FPT_SEP.2 (Séparation de domaines pour la SFP) ou FPT_SEP.3 (Moniteur de référence complet) de cette famille doivent être utilisés en combinaison avec le composant FPT_RVM.1 (Capacité de la TSP à ne pas être contournée), et ADV_INT.3 (Minimisation de la complexité). De plus, si un moniteur de référence complet est exigé, les composants de la Classe FDP Protection des données de l'utilisateur doivent couvrir tous les objets.

FPT_SEP.1 Séparation de domaines pour la TSF

1268 Sans un domaine séparé protégé pour la TSF, il ne peut y avoir aucune assurance que la TSF n'a pas fait l'objet d'attaques d'intrusion par des sujets non sûrs. De telles attaques peuvent impliquer la modification du code de la TSF ou de structures de données de la TSF.

FPT_SEP.2 Séparation de domaines pour la SFP

1269 La fonction la plus importante fournie par une TSF est la mise en oeuvre de ses SFP. Afin de simplifier la conception et d'augmenter la probabilité que ces SFP importantes possèdent les caractéristiques d'un moniteur de référence (RM), en particulier être à l'épreuve d'une intrusion physique, elles doivent se trouver dans un domaine distinct du reste de la TSF.

Notes d'application de l'évaluateur

1270 Il est possible qu'un moniteur de référence dans le cadre d'une conception en niveaux puisse procurer des fonctions autres que celles des SFP. Cela provient de la nature pratique de la conception en niveaux du logiciel. Le but devrait être de minimiser le nombre de fonctions non reliées à la SFP.

1271 Il est à noter qu'il est acceptable pour un moniteur de référence que toutes les SFP qu'il applique se trouvent dans un domaine unique et distinct du moniteur de référence, ou qu'il y ait plusieurs domaines dans le moniteur de référence (chacun appliquant une SFP ou plus). Si plusieurs domaines du moniteur de référence appliquant des SFP sont présents, il est acceptable qu'ils aient des relations d'égaux à égaux ou bien hiérarchiques.

1272 Pour FPT_SEP.2.1, l'expression "partie non isolée de la TSF" désigne la partie de la TSF comprenant les fonctions de la TSF qui ne sont pas couvertes par FPT_SEP.2.3.

Opérations

Affectation :

1273 **Pour FPT_SEP.2.3, l'auteur du PP ou de la ST devrait spécifier les SFP de contrôle d'accès ou de contrôle de flux d'information de la TSP qui devraient avoir un domaine séparé.**

FPT_SEP.3 Moniteur de référence complet

1274 La fonction la plus importante fournie par une TSF est la mise en oeuvre de ses SFP. Ce composant développe les objectifs du composant précédent en exigeant que *toutes* les SFP de contrôle d'accès ou de contrôle de flux d'information soient appliquées dans un domaine distinct du reste de la TSF. Cela simplifie encore la conception et augmente la probabilité que les caractéristiques d'un moniteur de référence (RM), en particulier être à l'épreuve d'une intrusion physique, se retrouvent dans la TSF.

Notes d'application de l'évaluateur

1275 Il est possible qu'un moniteur de référence dans le cadre d'une conception en niveaux puisse procurer des fonctions autres que celles des SFP. Cela provient de la nature pratique de la conception en niveaux du logiciel. Le but devrait être de minimiser le nombre de fonctions non reliées à la SFP.

1276 Il est à noter qu'il est acceptable pour un moniteur de référence que toutes les SFP qu'il applique se trouvent dans un domaine unique et distinct du moniteur de référence, ou qu'il y ait plusieurs domaines dans le moniteur de référence (chacun appliquant une SFP ou plus). Si plusieurs domaines du moniteur de référence appliquant des SFP sont présents, il est acceptable qu'ils aient des relations d'égaux à égaux ou bien hiérarchiques.

J.12 Protocole de synchronisation d'états (FPT_SSP)

1277 Les systèmes distribués peuvent occasionner une complexité supérieure à celle des systèmes monolithiques à cause du potentiel de différence des états entre des parties du système, et à cause de retards dans les communications. Dans la plupart des cas, la synchronisation d'état entre fonctions distribuées implique un protocole d'échange, et non une simple action. Quand la malveillance est présente dans l'environnement distribué de ces protocoles, des protocoles défensifs plus complexes sont exigés.

1278 La famille FPT_SSP établit l'exigence pour certaines fonctions de sécurité critiques de la TSF d'utiliser ce protocole de confiance. La famille FPT_SSP garantit que deux parties distribuées de la TOE (e.g. des hôtes) ont synchronisé leurs états après une action touchant à la sécurité.

Notes pour l'utilisateur

1279 Certains états ne peuvent jamais être synchronisés, ou alors le coût de la transaction peut être trop élevé pour une utilisation pratique ; la révocation d'une clé de chiffrement constitue un exemple où la connaissance de l'état qui suit l'initiation de l'action de révocation n'est jamais possible. Soit l'action a été entreprise et l'accusé de réception ne peut pas être envoyé, soit le message a été ignoré par des partenaires de communication hostiles et la révocation n'a jamais eu lieu. L'indétermination est une caractéristique unique aux systèmes distribués. L'indétermination et le synchronisme d'états sont liés et la même solution peut s'appliquer. Il est futile de concevoir des états indéterminés ; l'auteur du PP ou de la ST devrait exprimer d'autres exigences dans de tels cas (e.g. mettre en place une alarme, auditer l'événement).

FPT_SSP.1 Accusé de réception de confiance simple

Notes d'application pour l'utilisateur

1280 Dans ce composant, la TSF doit envoyer un accusé de réception à une autre partie de la TSF quand cela est exigé. Cet accusé de réception devrait indiquer qu'une partie d'une TOE distribuée a reçu avec succès un message non modifié transmis par une partie différente de la TOE distribuée.

FPT_SSP.2 Accusé de réception de confiance mutuel

Notes d'application pour l'utilisateur

1281 Dans ce composant, outre le fait que la TSF soit capable d'envoyer un accusé de réception pour la réception de données transmises, la TSF doit satisfaire à une requête d'une autre partie de la TSF pour accuser réception de l'accusé de réception.

1282 Par exemple, la TSF locale transmet certaines données à une partie distante de la TSF. La partie distante de la TSF accuse réception pour avoir reçu avec succès les

données et demande que la TSF émettrice confirme qu'elle a bien reçu l'accusé de réception. Ce mécanisme procure une confiance supplémentaire dans le fait que les deux parties de la TSF impliquées dans la transmission de données savent que la transmission s'est réalisée avec succès.

J.13 Horodatage (FPT_STM)

1283 Cette famille traite des exigences pour une fonction d'horodatage fiable dans une TOE.

Notes pour l'utilisateur

1284 Il est de la responsabilité de l'auteur du PP ou de la ST de clarifier la signification de l'expression "horodatage fiable" et d'indiquer à qui incombe la responsabilité d'accepter de lui faire confiance.

FPT_STM.1 Horodatage fiable

Notes d'application pour l'utilisateur

1285 Certaines utilisations possibles de ce composant comprennent la fourniture d'horodatages fiables pour les buts d'un audit ainsi que pour l'expiration d'un attribut de sécurité.

J.14 Cohérence des données de la TSF inter-TSF (FPT_TDC)

1286 Dans l'environnement d'un système distribué ou composé, une TOE peut avoir besoin d'échanger des données de la TSF (e.g. les attributs de la SFP associés à des données, des informations d'audit, des informations d'identification) avec un autre produit TI de confiance. La présente famille définit les exigences pour un partage et une interprétation cohérente de ces attributs entre la TSF de la TOE et celle d'un produit TI de confiance différent.

Notes pour l'utilisateur

1287 Les composants de cette famille sont destinés à fournir des exigences pour un support automatisé destiné à la cohérence des données de la TSF quand de telles données sont transmises entre la TSF de la TOE et un autre produit TI de confiance. Il est également possible que des moyens entièrement procéduraux soient utilisés pour obtenir la cohérence d'attributs de sécurité ; ceux-ci ne sont pas donnés ici.

1288 Cette famille est différente des familles FDP_ETC et FDP_ITC, car ces deux familles ne concernent que la résolution des attributs de sécurité entre la TSF et un support d'importation ou d'exportation.

1289 Si l'intégrité des données de la TSF constitue une préoccupation, des exigences devraient être choisies dans la famille FPT_ITI. Ces composants spécifient des exigences pour que la TSF puisse détecter ou détecter et corriger des modifications des données de la TSF en transit.

FPT_TDC.1 Cohérence élémentaire des données de la TSF inter-TSF

Notes d'application pour l'utilisateur

1290 La TSF est responsable du maintien de la cohérence des données utilisées par la fonction spécifiée ou associées à celle-ci et qui sont communes à deux systèmes de confiance ou plus. Par exemple, les données de la TSF de deux systèmes différents peuvent avoir des conventions internes différentes. Pour que les données de la TSF soient utilisées correctement (e.g. pour procurer aux données de l'utilisateur la même protection que dans la TOE) par le produit TI de confiance destinataire, la TOE et l'autre produit TI de confiance doivent utiliser un protocole pré-établi pour échanger des données de la TSF.

Opérations

Affectation :

1291 **Dans FPT_TDC.1.1, l'auteur du PP ou de la ST devrait définir la liste des types de données de la TSF pour lesquelles la TSF doit offrir la possibilité d'une interprétation cohérente, quand elles sont partagées entre la TSF et un autre produit TI de confiance.**

1292 **Dans FPT_TDC.1.2, le PP ou la ST devrait spécifier la liste des règles d'interprétation qui doivent être appliquées par la TSF.**

J.15 Cohérence de la reproduction des données de la TSF à l'intérieur de la TOE (FPT_TRC)

1293 Les exigences de cette famille sont nécessaires pour garantir la cohérence des données de la TSF quand de telles données sont reproduites à l'intérieur de la TOE. Celles-ci peuvent devenir incohérentes si un canal interne entre des parties de la TOE devient inopérant. Si la TOE est structurée en interne comme un réseau de parties de la TOE, cette incohérence peut se produire quand des parties de la TOE sont désactivées, des éléments de connexion du réseau sont détruits, etc.

Notes pour l'utilisateur

1294 La méthode pour garantir la cohérence n'est pas spécifiée dans ce composant. Elle pourrait être obtenue au moyen d'une forme de connexion par transaction (où des transactions appropriées font l'objet d'une annulation sur un site à la reconnexion) ; elle pourrait mettre à jour les données reproduites au moyen d'un protocole de synchronisation. Si un protocole particulier est nécessaire pour un PP ou une ST, il peut être spécifié par un raffinement.

1295 Il peut être impossible de synchroniser certains états, ou bien le coût d'une telle synchronisation peut se révéler trop élevé. Des exemples de cette situation sont fournies par la révocation d'un canal de communication et la révocation d'une clé de chiffrement. Des états indéterminés peuvent aussi survenir ; si un comportement spécifique est souhaité, il devrait être spécifié par un raffinement.

FPT_TRC.1 Cohérence interne de la TSF

Opérations

Affectation :

1296 **Dans FPT_TRC.1.2, l'auteur du PP ou de la ST devrait spécifier la liste des SF qui dépendent de la cohérence de la reproduction des données de la TSF.**

J.16 Autotest de la TSF (FPT_TST)

1297 La famille définit les exigences pour l'autotest de la TSF relativement à une certaine opération dont l'exécution correcte est attendue. On peut citer comme exemples des interfaces vers des fonctions de mise en œuvre et des opérations arithmétiques d'échantillonnage sur des parties critiques de la TOE. Ces tests peuvent être menés au démarrage, de façon périodique, à la demande de l'utilisateur autorisé ou quand d'autres conditions sont remplies. Les actions à entreprendre par la TOE à la suite de l'autotest sont définies dans d'autres familles.

1298 Les exigences de cette famille sont également nécessaires pour détecter l'altération du code exécutable de la TSF (i.e. du logiciel de la TSF) et des données de la TSF dues à diverses défaillances qui ne provoquent pas nécessairement l'arrêt du fonctionnement de la TOE (qui serait pris en compte par d'autres familles). Ces vérifications doivent être effectuées car ces défaillances ne peuvent pas toujours être empêchées. De telles défaillances peuvent survenir soit parce qu'il existe des modes de défaillance non prévus ou des contrôles non prévus associés à ces modes de défaillance dans la conception du matériel, des micro-programmes ou du logiciel, soit à cause de l'altération malveillante de la TSF due à une protection logique ou physique inadaptée.

1299 De plus, l'utilisation de ce composant peut, dans des conditions appropriées, contribuer à empêcher que des changements de la TSF inappropriés ou destructeurs ne soient appliqués à une TOE opérationnelle à la suite d'activités de maintenance.

Notes pour l'utilisateur

1300 L'expression "fonctionnement correct de la TSF" désigne principalement le fonctionnement du logiciel de la TSF et l'intégrité des données de la TSF. La machine abstraite sur laquelle le logiciel de la TSF est implémenté est testée via la dépendance envers la famille FPT_AMT.

FPT_TST.1 Test de la TSF

Notes d'application pour l'utilisateur

1301 Ce composant offre un support pour le test des fonctions critiques pour le fonctionnement de la TSF en exigeant la possibilité de faire appel aux fonctions test et de vérifier l'intégrité des données de la TSF et du code exécutable.

Notes d'application de l'évaluateur

1302 Le fait que les fonctions disponibles à l'utilisateur autorisé pour le test périodique ne soient disponibles que dans un mode hors ligne ou un mode de maintenance est acceptable. Des contrôles devraient être mis en place pour limiter l'accès aux utilisateurs autorisés dans ces modes.

Opérations

Sélection :

1303 **Dans FPT_TST.1, l'auteur du PP ou de la ST devrait spécifier quand la TSF devra exécuter le test de la TSF : pendant le démarrage initial, de façon périodique pendant le fonctionnement normal, à la demande d'un utilisateur autorisé, ou dans d'autres conditions. Dans le dernier cas, l'auteur du PP ou de la ST devrait aussi spécifier ces conditions comme indiqué dans l'affectation suivante.**

Affectation :

1304 **Dans FPT_TST.1.1, l'auteur du PP ou de la ST devrait spécifier les conditions dans lesquelles l'autotest devrait avoir lieu, s'il est sélectionné.**

Annexe K
(Informative)

Utilisation des ressources (FRU)

1305 Cette classe inclut trois familles qui concernent la disponibilité des ressources nécessaires telles que la capacité de calcul ou la capacité de stockage. La famille “Tolérance aux pannes” fournit une protection contre l’indisponibilité de capacités due à une défaillance de la TOE. La famille “Priorité de service” garantit que les ressources seront allouées aux tâches les plus importantes ou dont l’exécution immédiate est critique et ne pourront pas être monopolisées par des tâches de moindre priorité. La famille “Allocation des ressources” fournit des limites à l’utilisation des ressources disponibles, empêchant ainsi les utilisateurs de monopoliser les ressources.

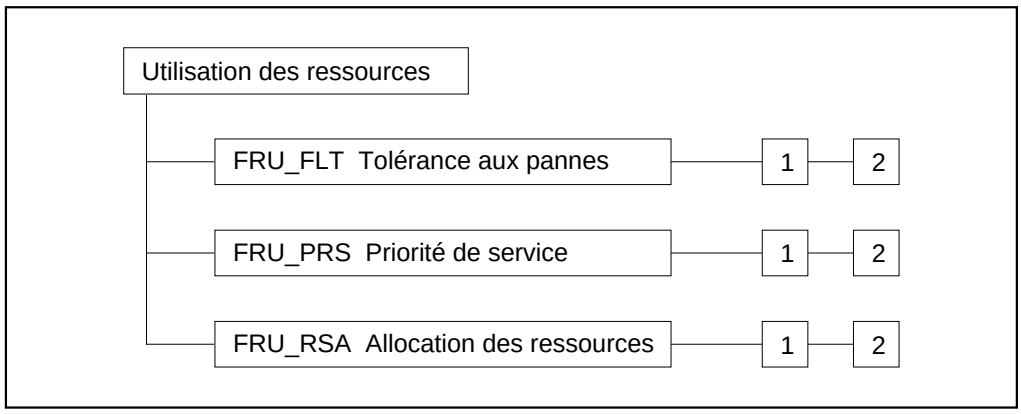


Figure K.1 - Décomposition de la classe “Utilisation d’une ressource”

K.1 Tolérance aux pannes (FRU_FLT)

1306 Cette famille contient des exigences pour la disponibilité de capacités même dans le cas de défaillances. Comme exemples de telles défaillances, on peut citer les défaillances d'alimentation, les défaillances du matériel ou les erreurs logicielles. Dans le cas où de telles erreurs se produisent, s'il en est spécifié ainsi, la TOE maintiendra les capacités spécifiées disponibles. L'auteur du PP ou de la ST pourrait spécifier, par exemple, qu'une TOE utilisée dans une centrale nucléaire devra continuer à effectuer la procédure d'arrêt dans le cas d'une défaillance de l'alimentation ou d'une défaillance de la communication.

Notes pour l'utilisateur

1307 Parce que la TOE ne peut continuer à fonctionner correctement que si la TSP est mise en œuvre, il y a une exigence indiquant que le système doit conserver un état sûr à la suite d'une défaillance. Cette capacité est exigée dans le composant "FPT_FLS.1".

1308 Les mécanismes offrant une tolérance aux pannes pourraient être actifs ou passifs. Dans le cas d'un mécanisme actif, des fonctions spécifiques sont en place, qui sont activées si l'erreur se produit. Une alarme incendie est par exemple un mécanisme actif : la TSF détectera l'incendie et pourra entreprendre des actions telles que le basculement de l'exploitation en mode de sauvegarde. Dans un schéma passif, l'architecture de la TOE lui procure la capacité de réagir face à une erreur. Par exemple, l'utilisation d'un schéma de vote majoritaire dans un contexte multi-processeurs constitue une solution passive ; la défaillance d'un processeur n'interrompra pas le fonctionnement de la TOE (bien qu'elle nécessite d'être détectée pour permettre une correction).

1309 Dans cette famille, le fait que la défaillance ait une origine accidentelle (telle qu'une inondation ou le débranchement malencontreux du mauvais dispositif) ou intentionnelle (telle que la monopolisation de ressources) n'a pas d'importance.

FRU_FLT.1 Tolérance aux pannes avec mode dégradé

Notes d'application pour l'utilisateur

1310 Ce composant est destiné à spécifier les capacités que la TOE devra toujours fournir à la suite d'une défaillance du système. Comme il serait difficile de décrire toutes les défaillances spécifiques, des catégories de défaillances peuvent être spécifiées. Comme exemples de défaillances générales, on peut citer l'inondation de la salle machine, l'interruption brève de l'alimentation, la panne de la CPU ou de la machine hôte, la défaillance d'un logiciel, ou le débordement d'un tampon.

Operations

Affectation :

1311 **Dans FRU_FLT.1.1, l'auteur du PP ou de la ST devrait spécifier la liste des capacités que la TOE devra maintenir disponibles pendant et après une défaillance spécifiée.**

1312 **Dans FRU_FLT.1.1, l'auteur du PP ou de la ST devrait spécifier la liste des types de défaillances contre lesquelles la TOE doit être explicitement protégée. Si une défaillance figurant dans cette liste survient, la TOE sera capable de poursuivre son fonctionnement.**

FRU_FLT.2 Tolérance aux pannes limitée

Notes d'application pour l'utilisateur

1313 Ce composant est destiné à spécifier les types de défaillances auxquelles la TOE doit résister. Comme il serait difficile de décrire toutes les défaillances spécifiques, des catégories de défaillances peuvent être spécifiées. Comme exemples de défaillances générales, on peut citer l'inondation de la salle machine, l'interruption brève de l'alimentation, la panne de la CPU ou de la machine hôte, la défaillance d'un logiciel, ou le dépassement d'un tampon.

Operations

Affectation :

1314 Dans FRU_FLT.2.1, l'auteur du PP ou de la ST devrait spécifier la liste des types de défaillances contre lesquelles la TOE doit être explicitement protégée. Si une défaillance figurant dans cette liste survient, la TOE sera capable de poursuivre son fonctionnement.

K.2 Priorité de service (FRU_PRS)

1315 Les exigences de cette famille permettent à la TSF de contrôler l'utilisation de ressources au sein du TSC par des utilisateurs et des sujets de telle sorte que les activités prioritaires au sein du TSC soient toujours exécutées sans interférence ou retard dû à des activités de faible priorité. En un mot, les tâches urgentes ne seront pas retardées par des tâches qui le sont moins.

1316 Cette famille pourrait s'appliquer à plusieurs types de ressources, comme par exemple des capacités de calcul et des capacités de canal de communication.

1317 Le mécanisme de priorité de service peut être passif ou actif. Dans le cas où il est passif, le système choisira la tâche ayant la priorité la plus élevée parmi deux applications en attente d'exécution. En utilisant des mécanismes passifs de priorité de service, une tâche de priorité faible en cours d'exécution ne peut pas être interrompue par une tâche de priorité élevée. En utilisant des mécanismes de priorité de service actifs, des tâches de priorité faible pourraient être interrompues par de nouvelles tâches de priorité élevée.

Notes pour l'utilisateur

1318 Les exigences d'audit stipulent que toutes les raisons ayant motivé un rejet devraient être auditées. C'est au développeur qu'il revient d'argumenter qu'une opération n'est pas rejetée mais retardée.

FRU_PRS.1 Priorité de service limitée

Notes d'application pour l'utilisateur

1319 Ce composant définit des priorités pour un sujet et les ressources pour lesquelles cette priorité sera utilisée. Si un sujet essaye d'entreprendre une action sur une ressource contrôlée par les exigences de la famille "Priorité de service", l'accès ou le temps d'accès dépendra de la priorité du sujet, de la priorité du sujet en activité, et de la priorité des sujets qui sont encore en file d'attente.

Operations

Affectation :

1320 **Dans FRU_PRS.1.2, l'auteur du PP ou de la ST devrait spécifier la liste des ressources contrôlées pour lesquelles la TSF applique une priorité de service (e.g. des ressources telles que des processus, de l'espace disque, de la mémoire, de la bande passante).**

FRU_PRS.2 Priorité de service totale

Notes d'application pour l'utilisateur

1321 Ce composant définit des priorités pour un sujet. Toutes les ressources partageables du TSC seront soumises au mécanisme de priorité de service. Si un sujet essaye

d’entreprendre une action sur une ressource contrôlée par les exigences de la famille “Priorité de service”, l’accès ou le temps d’accès dépendra de la priorité du sujet, de la priorité du sujet en activité, et de la priorité des sujets qui sont encore en file d’attente.

K.3 Allocation des ressources (FRU_RSA)

1322 Les exigences de cette famille permettent à la TSF de contrôler l'utilisation des ressources dans le TSC par les utilisateurs et les sujets de telle sorte qu'un déni de service non autorisé ne pourra survenir du fait de la monopolisation de ressources par d'autres utilisateurs ou sujets.

Notes pour l'utilisateur

1323 Les règles de l'allocation de ressources autorisent la création de quotas ou d'autres moyens pour définir des limites sur la quantité de ressources de type espace ou temps qui peuvent être allouées pour le compte d'un utilisateur ou de sujets spécifiques. Ces règles peuvent par exemple :

- Définir des quotas d'objets qui limitent le nombre ou la taille d'objets qu'un utilisateur spécifique peut allouer.

- Contrôler l'allocation ou la désallocation d'unités de ressource préassignées quand ces unités sont sous le contrôle de la TSF.

1324 En général, ces fonctions seront implémentées par l'utilisation d'attributs assignés à des utilisateurs et à des ressources.

1325 L'objectif de ces composants est de garantir une certaine équité entre les utilisateurs (e.g. un seul utilisateur ne devrait pas allouer tout l'espace disponible) et les sujets. Comme l'allocation de ressources se prolonge au delà de la durée de vie d'un sujet (i.e. souvent des fichiers existent encore alors que les applications qui les ont générés sont terminées), et comme des instanciations multiples de sujets par le même utilisateur ne devraient pas trop affecter les autres utilisateurs, les composants permettent que les limitations relatives aux allocations soient associées aux utilisateurs. Dans certaines situations, les ressources sont allouées par un sujet (e.g. la mémoire centrale ou des cycles CPU). Dans ces cas, les composants permettent que l'allocation des ressources se fasse au niveau des sujets.

1326 Cette famille impose des exigences pour l'allocation de la ressource, et non pour l'utilisation de la ressource elle-même. Par conséquent les exigences d'audit, comme indiqué, s'appliquent également à l'allocation de la ressource, et non à l'utilisation de la ressource.

FRU_RSA.1 Quotas maximums

Notes d'application pour l'utilisateur

1327 Ce composant contient des exigences pour des mécanismes de quota qui s'appliquent seulement à un ensemble spécifié de ressources partageables de la TOE. Les exigences permettent que les quotas soient associés à un utilisateur, ou éventuellement à des groupes d'utilisateurs ou de sujets si cela s'applique à la TOE.

Operations

Affectation :

1328 **Dans FRU_RSA.1.1, l'auteur du PP ou de la ST devrait spécifier la liste des ressources contrôlées pour lesquelles les limites maximum d'allocation de ressources sont requises (e.g. processus, espace disque, mémoire, bande passante). Si toutes les ressources du TSC doivent être incluses, l'expression "toutes les ressources du TSC" peut être spécifiée.**

Sélection:

1329 **Dans FRU_RSA.1.1, l'auteur du PP ou de la ST devrait choisir si les quotas maximum s'appliquent à des utilisateurs individuels, à un groupe défini d'utilisateurs, de sujets ou à une combinaison des trois.**

1330 **Dans FRU_RSA.1.1, l'auteur du PP ou de la ST devrait choisir si les quotas maximum s'appliquent à n'importe quel moment (simultanément), ou pendant un intervalle de temps particulier.**

FRU_RSA.2 Quotas minimums et maximums

Notes d'application pour l'utilisateur

1331 Ce composant contient des exigences pour des mécanismes de quota qui s'appliquent à un ensemble spécifié de ressources partageables de la TOE. Les exigences permettent que les quotas soient associés à un utilisateur, ou éventuellement à des groupes d'utilisateurs si cela s'applique à la TOE.

Operations

Affectation :

1332 Dans FRU_RSA.2.1, l'auteur du PP ou de la ST devrait spécifier la liste des ressources contrôlées pour lesquelles les limites d'allocation maximum et **minimum** de ressources sont requises (e.g. processus, espace disque, mémoire, bande passante). Si toutes les ressources du TSC doivent être incluses, l'expression "toutes les ressources du TSC" peut être spécifiée.

Sélection:

1333 Dans FRU_RSA.2.1, l'auteur du PP ou de la ST devrait choisir si les quotas maximum s'appliquent à des utilisateurs individuels, à un groupe défini d'utilisateurs, de sujets ou à une combinaison des trois.

1334 Dans FRU_RSA.2.1, l'auteur du PP ou de la ST devrait choisir si les quotas maximum s'appliquent à n'importe quel moment (simultanément), ou pendant un intervalle de temps particulier.

Affectation :

1335 **Dans FRU_RSA.2.2, l'auteur du PP ou de la ST devrait spécifier les ressources contrôlées pour lesquelles une limite minimum d'allocation doit s'appliquer (e.g. processus, espace disque, mémoire, bande passante). Si toutes les ressources du TSC doivent être incluses, l'expression "toutes les ressources du TSC" peut être spécifiée.**

Sélection:

1336 **Dans FRU_RSA.2.2, l'auteur du PP ou de la ST devrait choisir si les quotas minimum s'appliquent à des utilisateurs individuels, à un groupe défini d'utilisateurs, de sujets ou à une combinaison des trois.**

1337 **Dans FRU_RSA.2.2, l'auteur du PP ou de la ST devrait choisir si les quotas minimum s'appliquent à n'importe quel moment (simultanément), ou pendant un intervalle de temps particulier.**

Annexe L
(Informative)

Accès à la TOE (FTA)

1338 L'établissement d'une session utilisateur consiste typiquement à créer un ou plusieurs sujets qui exécutent des opérations dans la TOE pour le compte de l'utilisateur. À la fin de la procédure d'établissement de la session, à condition que les exigences d'accès à la TOE soient satisfaites, les sujets créés portent les attributs déterminés par les fonctions d'identification et d'authentification. La présente classe spécifie des exigences fonctionnelles pour contrôler l'établissement d'une session utilisateur.

1339 Une session utilisateur est définie comme étant la période qui commence au moment de l'identification et de l'authentification, ou si cela est plus approprié, au début d'une interaction entre l'utilisateur et le système, et se termine au moment où tous les sujets (ressources et attributs) associés à cette session ont été désalloués.

1340 La figure 12.1 montre la décomposition de cette classe en ses composants constitutifs.

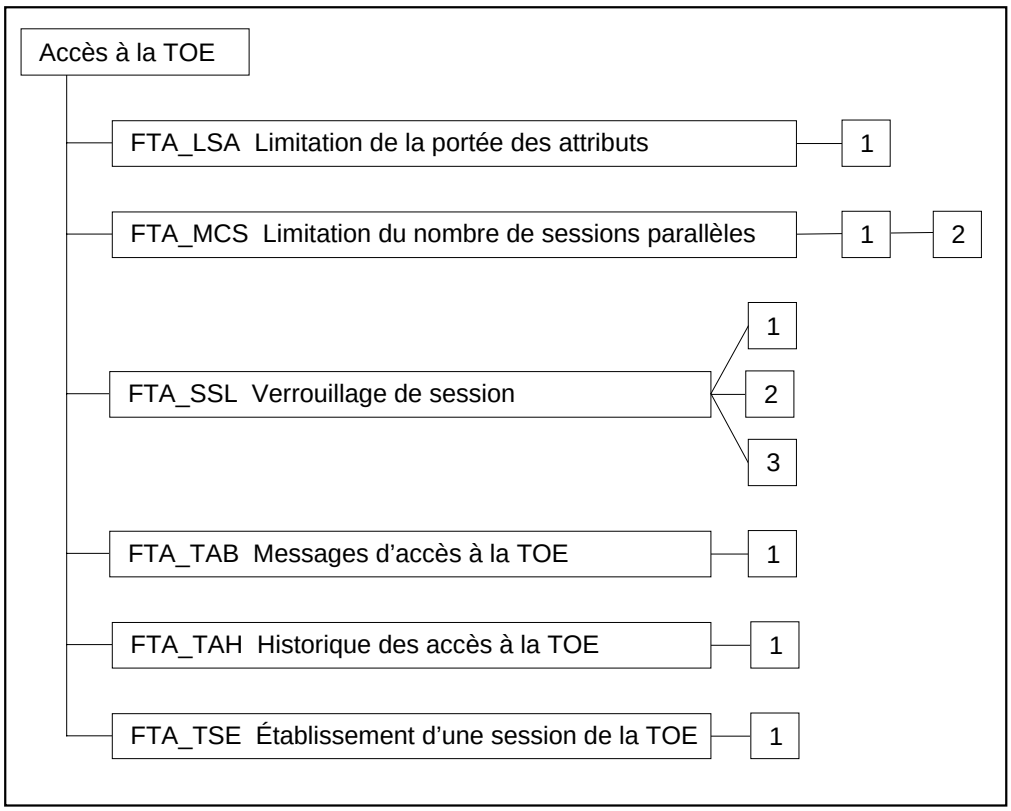


Figure 12.1 - Décomposition de la classe "Accès à la TOE"

L.1 Limitation de la portée des attributs sélectionnables (FTA_LSA)

1341 La présente famille définit les exigences qui vont délimiter les attributs de sécurité de la session qu'un utilisateur peut sélectionner et les sujets auxquels un utilisateur peut être lié en fonction de la méthode d'accès, du lieu ou du port d'accès ou de la date (e.g. heure du jour, jour de la semaine).

Notes pour l'utilisateur

1342 Cette famille donne la possibilité à un auteur de PP ou de ST de spécifier des exigences pour que la TSF définisse des limites relatives au domaine des attributs de sécurité d'un utilisateur autorisé en fonction d'une condition liée à l'environnement. Par exemple, un utilisateur peut être autorisé à établir une "session secrète" pendant les heures de travail habituelles, mais en dehors de ces heures ce même utilisateur peut se voir contraint de n'établir que des "sessions non classifiées". L'identification des contraintes applicables au domaine des attributs sélectionnables peut être faite en utilisant l'opération de sélection. Ces contraintes peuvent être appliquées attribut par attribut. Quand il est nécessaire de spécifier des contraintes pour plusieurs attributs, ce composant devra être appliqué à nouveau pour chaque attribut. Des exemples d'attributs qui pourraient être utilisés pour limiter le domaine des attributs de sécurité de la session sont cités ci-dessous :

a) La méthode d'accès peut être utilisée pour spécifier dans quel type d'environnement l'utilisateur devra opérer (e.g. protocole de transfert de fichiers, terminal, vtam).

b) Le lieu d'accès peut être utilisé pour limiter le domaine des attributs sélectionnables d'un utilisateur en fonction du lieu ou du port d'accès de cet utilisateur. Cette possibilité est particulièrement intéressante dans des environnements offrant des possibilités d'appel téléphonique ou de connexion à un réseau.

c) La date d'accès peut être utilisée pour limiter le domaine des attributs sélectionnables d'un utilisateur. Par exemple, des plages temporelles peuvent être établies en heures, en jours ou en dates calendaires. Ces limites permettent une certaine protection opérationnelle contre les actions d'un utilisateur qui pourraient avoir lieu à un moment où il n'y aurait pas de contrôle ni de mesures procédurales appropriés.

FTA_LSA.1 Limitation de la portée des attributs sélectionnables

Operations

Affectation :

1343 **Dans FTA_LSA.1.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des attributs de sécurité d'une session qui doivent être**

limités. Comme exemple d'attributs de sécurité d'une session, on peut citer le niveau d'habilitation d'un utilisateur, le niveau d'intégrité et les rôles.

1344 **Dans FTA_LSA.1.1, l'auteur du PP ou de la ST devrait spécifier l'ensemble des attributs qui peuvent être utilisés pour déterminer le domaine d'application des attributs de sécurité d'une session. Comme exemple d'attributs de sécurité d'une session, on peut citer l'identité d'un utilisateur, le lieu d'établissement de la session, la date d'accès, et la méthode d'accès.**

L.2 Limitation du nombre de sessions parallèles (FTA_MCS)

1345 La présente famille définit le nombre de sessions auxquelles un utilisateur peut participer au même moment (sessions parallèles). Ce nombre de sessions parallèles peut aussi bien être fixé pour un groupe d'utilisateurs ou pour chaque utilisateur individuellement.

FTA_MCS.1 Limitation élémentaire du nombre de sessions parallèles

Notes d'application pour l'utilisateur

1346 Ce composant permet au système de limiter le nombre de sessions afin d'utiliser les ressources de la TOE de façon efficace.

Operations

Affectation :

1347 **Dans FTA_MCS.1.2, l'auteur du PP ou de la ST devrait spécifier le nombre maximum par défaut de sessions parallèles.**

FTA_MCS.2 Limitation du nombre de sessions parallèles par les attributs de l'utilisateur

Notes d'application pour l'utilisateur

1348 Ce composant offre des possibilités supplémentaires par rapport à celles du composant FTA_MCS.1, en permettant de fixer de nouvelles limites au nombre de sessions parallèles que les utilisateurs peuvent établir. Ces limites portent sur les attributs de sécurité d'un utilisateur, tels que l'identité d'un utilisateur ou sa participation à un rôle.

Operations

Affectation :

1349 **En utilisant le composant "FTA_MCS.2.1, l'auteur du PP ou de la ST devrait spécifier les règles qui déterminent le nombre maximum de sessions parallèles. Exemple de règle : "le nombre maximum de sessions parallèles est fixé à un si l'utilisateur est habilité au 'secret' et à cinq dans les autres cas".**

1350 Dans FTA_MCS.2.2, l'auteur du PP ou de la ST devrait spécifier le nombre maximum par défaut de sessions parallèles.

L.3 Verrouillage de session (FTA_SSL)

1351 La présente famille définit des exigences pour que la TSF offre la capacité de verrouiller et de déverrouiller des sessions interactives (e.g. verrouillage du clavier).

1352 Quand un utilisateur interagit directement avec des sujets de la TOE (session interactive), le terminal de l'utilisateur est vulnérable s'il est laissé sans surveillance. Cette famille contient des exigences pour que la TSF désactive (verrouille) le terminal ou termine la session après une période d'inactivité d'une durée spécifiée, et pour que l'utilisateur initie la désactivation (verrouillage) du terminal. Pour réactiver le terminal, il est nécessaire qu'un événement spécifié par l'auteur du PP ou de la ST se produise, tel qu'une nouvelle authentification de l'utilisateur.

1353 Un utilisateur est considéré comme inactif, s'il n'a envoyé aucun stimulus à la TOE pendant une certaine période de temps.

1354 Un auteur de PP ou de ST devrait se demander s'il doit inclure le composant "**FTP_TRP.1 Chemin de confiance**". Le cas échéant, la fonction 'verrouillage d'une session' devrait être introduite dans les opérations sur FTP_TRP.1.

FTA_SSL.1 Verrouillage de session, initié par la TSF

Notes d'application pour l'utilisateur

1355 Le composant "FTA_SSL.1 Verrouillage de session, initié par la TSF", donne la possibilité à la TSF de verrouiller une session utilisateur active au bout d'une période de temps spécifiée. Le verrouillage d'un terminal devrait empêcher toute interaction ultérieure avec une session active en utilisant ce terminal.

1356 Si des périphériques d'affichage sont rafraîchis, les nouveaux contenus ne nécessitent pas d'être statiques (i.e. des économiseurs d'écran sont autorisés).

1357 Ce composant permet à l'auteur du PP ou de la ST de spécifier les événements qui permettront de déverrouiller la session. Ces événements peuvent être associés au terminal (e.g. ensemble défini de touches pour déverrouiller la session), à l'utilisateur (e.g. nouvelle authentification), ou dépendre du temps.

Operations

Affectation :

1358 **Dans FTA_SSL.1.1, l'auteur du PP ou de la ST devrait spécifier la durée d'inactivité de l'utilisateur qui déclenchera le verrouillage d'une session interactive. S'il le désire, l'auteur du PP ou de la ST peut, en utilisant l'opération d'affectation, indiquer que la définition de la durée d'inactivité est confiée à l'administrateur autorisé ou à l'utilisateur. Les fonctions d'administration de la classe FMT peuvent spécifier la**

possibilité de modifier cette durée en la définissant comme valeur par défaut.

1359 **Dans FTA_SSL.1.2, l'auteur du PP ou de la ST devrait spécifier le ou les événements qui devraient survenir avant que la session ne soit déverrouillée. Comme exemples de tels événements, on peut citer une ré-authentification d'un utilisateur ou une suite de touches de déverrouillage frappées sur le clavier par un utilisateur.**

FTA_SSL.2 Verrouillage de session, initié par l'utilisateur

Notes d'application pour l'utilisateur

1360 Le composant "FTA_SSL.2 Verrouillage de session, initié par l'utilisateur", donne la possibilité à un utilisateur autorisé de verrouiller et de déverrouiller son propre terminal. Cela procure aux utilisateurs autorisés la possibilité de bloquer effectivement toute utilisation ultérieure de leurs sessions actives sans avoir besoin de clore cette session.

1361 Si des périphériques d'affichage sont rafraîchis, les nouveaux contenus ne nécessitent pas d'être statiques (i.e. des économiseurs d'écran sont autorisés).

Operations

Affectation :

1362 **Dans FTA_SSL.2.2, l'auteur du PP ou de la ST devrait spécifier le ou les événements qui devrait survenir avant que la session ne soit déverrouillée. Comme exemples de tels événements, on peut citer une nouvelle authentification d'un utilisateur ou une suite de touches de déverrouillage sur le clavier frappées par un utilisateur.**

FTA_SSL.3 Clôture de session, initiée par la TSF

Notes d'application pour l'utilisateur

1363 Le composant "FTA_SSL.3 Clôture de session, initiée par la TSF" exige que la TSF termine une session utilisateur interactive après une certaine durée d'inactivité.

1364 L'auteur du PP ou de la ST devrait être conscient qu'une session peut se poursuivre après que l'utilisateur ne soit plus actif ; tel est le cas par exemple d'un processus en tâche de fond. Cette exigence provoquerait la désactivation du sujet en tâche de fond après une certaine durée d'inactivité de l'utilisateur sans aucune considération du statut du sujet.

Operations

Affectation :

1365 **Dans FTA_SSL.3.1, l'auteur du PP ou de la ST devrait spécifier la durée d'inactivité de l'utilisateur qui déclenchera la clôture d'une session interactive. S'il le désire, l'auteur du PP ou de la ST peut, en utilisant l'opération d'affectation, indiquer que la définition de la durée d'inactivité est confiée à l'administrateur autorisé ou à l'utilisateur. Les fonctions d'administration de la classe FMT peuvent spécifier la possibilité de modifier cette durée en la faisant devenir la valeur par défaut.**

L.4 Messages d’accès à la TOE (FTA_TAB)

1366 Avant toute identification et authentification, des exigences d’accès à la TOE donnent la possibilité d’afficher un message d’avertissement aux utilisateurs potentiels, relatif à une utilisation appropriée de la TOE.

FTA_TAB.1 Messages par défaut d’accès à la TOE

1367 Ce composant exige qu’un message d’avertissement relatif à une utilisation non autorisée de la TOE soit affiché. Un auteur de PP ou de ST peut raffiner cette exigence pour inclure un message d’accès par défaut.

L.5 Historique des accès à la TOE (FTA_TAH)

1368 La présente famille définit des exigences pour que la TSF affiche aux utilisateurs, après l'établissement réussi d'une session avec la TOE, un historique des tentatives infructueuses pour accéder à leur compte. Cet historique peut comprendre la date, l'heure, les moyens d'accès et le port de la dernière tentative réussie d'accès à la TOE, ainsi que le nombre d'essais infructueux pour accéder à la TOE depuis la dernière tentative réussie par l'utilisateur identifié.

FTA_TAH.1 Historique des accès à la TOE

1369 Cette famille peut procurer aux utilisateurs autorisés des informations qui peuvent indiquer une éventuelle utilisation indue de leur compte.

Notes d'application pour l'utilisateur

1370 Ce composant exige qu'on présente ces informations à l'utilisateur. Ce dernier devrait être capable de revoir les informations, sans y être toutefois obligé. Si un utilisateur le souhaite, il pourrait par exemple créer des scripts qui ignorent ces informations et démarrent d'autres processus.

Operations

Sélection :

1371 **Dans FTA_TAH.1.1, l'auteur du PP ou de la ST devrait sélectionner les attributs de sécurité de la dernière tentative d'établissement réussie d'une session, qui seront affichés sur l'interface de l'utilisateur. Ces attributs comprennent : la date, l'heure, la méthode d'accès (e.g. ftp) ou le lieu d'accès (e.g. terminal numéro 50).**

1372 **Dans FTA_TAH.1.2, l'auteur du PP ou de la ST devrait sélectionner les attributs de sécurité de la dernière tentative d'établissement infructueuse d'une session, qui seront affichés sur l'interface de l'utilisateur. Ces attributs comprennent : la date, l'heure, la méthode d'accès (e.g. ftp) ou le lieu d'accès (e.g. terminal numéro 50).**

L.6 Établissement d'une session de la TOE (FTA_TSE)

1373 La présente famille définit des exigences permettant de refuser à un utilisateur la permission d'établir une session avec la TOE en fonction d'attributs tels que le lieu ou le port d'accès, les attributs de sécurité de l'utilisateur (e.g. identité, niveau d'habilitation, niveau d'intégrité, participation dans un rôle), des plages de temps (e.g. plage horaire, plage de jours, périodes calendaires) ou des combinaisons de paramètres.

Notes pour l'utilisateur

1374 Cette famille donne la possibilité à l'auteur du PP ou de la ST de spécifier des exigences pour que la TOE limite la possibilité qu'un utilisateur autorisé établisse une session avec la TOE. L'identification de limitations pertinentes peut se faire en utilisant l'opération de sélection. Des exemple d'attributs qui pourraient être utilisés pour spécifier les limites à l'établissement de la session sont cités ci-dessous :

a) Le lieu d'accès peut être utilisé pour limiter la possibilité qu'un utilisateur autorisé établisse une session active avec la TOE, en fonction du lieu ou du port d'accès de l'utilisateur. Cette possibilité est particulièrement intéressante dans des environnements offrant des possibilités d'appel téléphonique ou de connexion à un réseau.

b) Les attributs de sécurité de l'utilisateur peuvent être utilisés pour limiter la possibilité qu'un utilisateur autorisé établisse une session active avec la TOE. Par exemple, ces attributs donneraient la possibilité de refuser l'établissement d'une session en fonction :

- de l'identité d'un utilisateur ;
- du niveau d'habilitation d'un utilisateur ;
- du niveau d'intégrité d'un utilisateur ;
- de la participation d'un utilisateur dans un rôle.

1375 Cette possibilité est particulièrement appropriée dans des situations où l'autorisation ou la connexion a lieu dans un endroit différent de celui où les contrôles d'accès à la TOE sont effectués.

a) L'heure d'accès peut être utilisée pour limiter le domaine des attributs sélectionnables d'un utilisateur. Par exemple, des plages temporelles peuvent être établies en heures, en jours, ou en dates calendaires. Ces limites permettent une certaine protection opérationnelle contre les actions d'un utilisateur qui pourraient avoir lieu à un moment où il n'y aurait pas de contrôle approprié ni de mesures procédurales appropriées.

FTA_TSE.1 Établissement d'une session de la TOE

Operations

Affectation :

1376 **Dans FTA_TSE.1.1, l'auteur du PP ou de la ST devrait spécifier les attributs qui peuvent être utilisés pour limiter l'établissement de la session. Comme exemple d'attributs de sécurité d'une session, on peut citer l'identité d'un utilisateur, le lieu d'établissement de la session (e.g. pas de terminal distant), la date d'accès (e.g. en dehors des heures ouvrables), et la méthode d'accès (e.g. X-windows).**

Annexe M
(Informative)

Chemins et canaux de confiance (FTP)

1377 Les utilisateurs ont souvent besoin d'exécuter des fonctions au moyen d'une interaction directe avec la TSF. Un chemin de confiance procure la confiance dans le fait qu'un utilisateur communique directement avec la TSF chaque fois qu'elle est appelée. Le fait que la réponse d'un utilisateur se fasse via le chemin de confiance garantit que des applications non sûres ne peuvent pas intercepter ou modifier cette réponse. De même, les canaux de confiance constituent une approche pour une communication sûre entre la TSF et des produits TI distants.

1378 La figure 1.2 de cette partie des CC illustre les relations entre les divers types de communication qui peuvent avoir lieu dans une TOE ou un réseau de TOE (i.e. des transferts internes à la TOE, des transferts inter-TSF et des importations ou exportations de données en dehors du contrôle de la TSF) et les différentes sortes de chemins et de canaux de confiance.

1379 L'absence d'un chemin de confiance peut provoquer des violations dans l'imputabilité ou dans le contrôle d'accès pour des environnements où des applications non sûres sont utilisées. Ces applications peuvent intercepter des informations à caractère personnel d'utilisateurs, telles que des mots de passe, et les utiliser pour se faire passer pour d'autres utilisateurs. En conséquence, la responsabilité d'entreprendre une action quelconque sur le système ne peut pas être confiée en toute fiabilité à une entité imputable. En outre, ces applications pourraient afficher des informations erronées sur l'écran d'un utilisateur insoupçonnable, ce qui pourrait avoir pour résultat de provoquer des actions erronées de la part de cet utilisateur et une violation de la sécurité.

1380 La figure 13.1 montre la décomposition de cette classe en ses composants constitutifs.

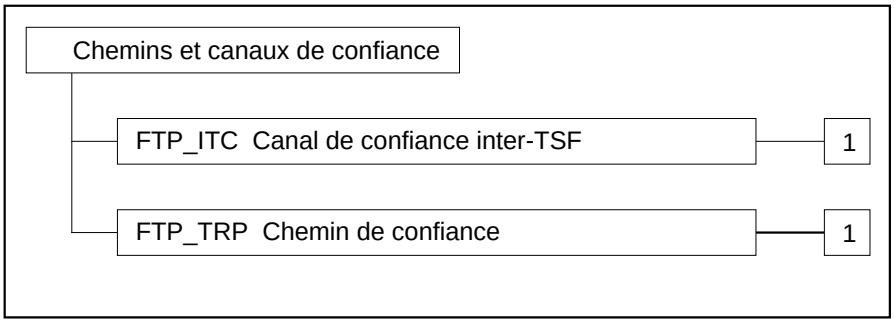


Figure 13.1 - Décomposition de la classe "Chemin et canaux de confiance"

M.1 Canal de confiance inter-TSF (FTP_ITC)

1381 La présente famille définit les règles pour créer une connexion pour un canal de confiance entre la TSF et un autre produit TI de confiance pour l'exécution d'opérations critiques pour la sécurité entre les produits. Comme exemple d'une telle opération critique pour la sécurité on peut citer la mise à jour de la base de données d'authentification de la TSF par le transfert de données depuis un produit de confiance dont la fonction consiste à collecter des données d'audit.

FTP_ITC.1 Canal de confiance inter-TSF

Notes d'application pour l'utilisateur

1382 Ce composant devrait être utilisé quand un canal de communication de confiance entre la TSF et un autre produit TI de confiance est nécessaire.

Operations

Sélection:

1383 **Dans FTP_ITC.1.2, l'auteur du PP ou de la ST doit spécifier si la TSF locale, le produit TI de confiance distant ou les deux auront la possibilité d'initier le canal de confiance.**

Affectation :

1384 **Dans FTP_ITC.1.3, l'auteur du PP ou de la ST devrait spécifier les fonctions qui nécessitent un canal de confiance. Ces fonctions peuvent inclure par exemple le transfert d'attributs de sécurité d'un utilisateur, d'un sujet, ou d'un objet et garantir la cohérence des données de la TSF.**

M.2 Chemin de confiance (FTP_TRP)

1385 La présente famille définit des exigences pour établir et maintenir une communication sûre en provenance d'utilisateurs ou de la TSF ou vers ces derniers. Un chemin de confiance peut être exigé pour toute interaction touchant à la sécurité. Les échanges via un chemin de confiance peuvent être initiés par un utilisateur au cours d'une interaction avec la TSF, ou bien la TSF peut établir la communication avec l'utilisateur via un chemin de confiance.

FTP_TRP.1 Chemin de confiance

Notes d'application pour l'utilisateur

1386 Ce composant devrait être utilisé quand une communication de confiance entre un utilisateur et la TSF est nécessaire, soit pour effectuer seulement une authentification initiale soit pour des opérations utilisateur supplémentaires spécifiées.

Operations

Sélection:

1387 **Dans FTP_TRP.1.1, l'auteur du PP ou de la ST devrait spécifier si le chemin de confiance doit être étendu à des utilisateurs distants ou des utilisateurs locaux.**

1388 **Dans FTP_TRP.1.2, l'auteur du PP ou de la ST devrait spécifier si la TSF, des utilisateurs locaux ou des utilisateurs distants devraient pouvoir initier le chemin de confiance.**

1389 **Dans FTP_TRP.1.3, l'auteur du PP ou de la ST devrait spécifier si le chemin de confiance doit être utilisé pour l'authentification initiale d'un utilisateur ou pour d'autres services spécifiés.**

Affectation :

1390 **Dans FTP_TRP.1.3, dans le cas où il est sélectionné, l'auteur du PP ou de la ST devrait identifier les autres services qui nécessitent le chemin de confiance, le cas échéant.**