Direction centrale de la sécurité des systèmes d'information

Profil de Protection Application de chiffrement de données à la volée sur mémoire de masse

Date d'émission	**:**	Août 2008
Référence	**:**	PP-CDISK-CCv3.1
Version	**:**	1.4

Profil de protection enregistré et certifié par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) sous la référence DCSSI-PP-2008/04.

Table des matières

Table des figures

Table des tableaux

1 Introduction au profil de protection

1.1 Identification du profil de protection

Titre :	Profil de protection, Application de chiffrement de données à la volée sur mémoire de masse
Auteur :	Trusted Labs S.A.S.
Version :	1.4, Août 2008
Sponsor :	DCSSI
Version des CC :	3.1 revision 2

1.2 Contexte

Ce document est réalisé sous l'égide de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI). L'objectif est de favoriser la certification des applications de chiffrement de données à la volée sur mémoire de masse pour les besoins des secteurs public et privé en vue de leur qualification.

Ce document contient deux profils de protection (PP), appelés respectivement

- Application de chiffrement de données à la volée sur mémoire de masse *avec* génération de clé
- Application de chiffrement de données à la volée sur mémoire de masse *sans* génération de clé

Ces deux profils seront plus simplement désignés sous le vocable de « configuration » dans la suite du document, chaque section identifiant, le cas échéant, à quel profil elle appartient. En l'absence de mention particulière, une section est applicable aux deux configurations.

1.3 Présentation générale de la cible d'évaluation

1.3.1 Type de TOE

L'objectif visé est de définir les exigences de sécurité auxquelles une application de chiffrement de données à la volée sur toute mémoire persistante de stockage (éventuellement amovible) doit se conformer en vue d'une évaluation de sécurité. La cible d'évaluation (TOE) considérée dans ce PP est un logiciel permettant de protéger en confidentialité les données enregistrées sur une partie au moins de la mémoire persistante de stockage d'une machine (ou, plus généralement, sur un support de stockage éventuellement amovible), dans les deux cas suivants :

1. la TOE est hors fonctionnement,
2. la TOE est en fonctionnement mais sans qu'un utilisateur légitime ne se soit authentifié à la TOE.

Les menaces relatives au cas de la TOE en fonctionnement avec un utilisateur légitime authentifié à la TOE ne seront donc pas considérées dans le présent PP.

L'objectif principal est donc de couvrir le vol de la machine. Néanmoins, les risques de la phase opérationnelle vis-à-vis du service de protection des données en confidentialité rendu par le produit devront être couverts (comme, par exemple, l'écriture d'informations confidentielles sur des zones non chiffrées ou l'écriture de la clé en clair sur une mémoire persistante). La confidentialité des données sur la mémoire de masse doit ainsi être garantie quels que soient les états successifs de la machine lors de la phase opérationnelle (mise en veille, arrêt brutal,...).

Par souci de simplification, la partie de la mémoire persistante de stockage de masse contenant les données protégées par la TOE sera nommée « disque » dans la suite du PP lorsque cela n'introduit pas d'ambiguïté.

1.3.2 Utilisation de la TOE

Le matériel informatique d'une entreprise ou d'un service administratif peut être l'objet d'un vol au même titre que tout autre objet de valeur. Ce risque est aujourd'hui accentué par le nomadisme croissant des équipements, plus susceptibles de quitter le lieu de travail qu'auparavant. La TOE est une application de chiffrement des données à la volée sur un support informatique permettant de protéger la confidentialité de ces dernières et de réduire l'impact de la perte en cas de vol de matériel.

1.3.3 Particularités et caractéristiques de sécurité de la TOE

La TOE, une fois activée, chiffre et déchiffre les données enregistrées sur et lues depuis la mémoire de masse de manière transparente. Cette activation nécessite une authentification de l'utilisateur à travers, par exemple, la fourniture de données d'authentification de type mot ou phrase de passe. La TOE utilise aussi, durant son fonctionnement, des clés de chiffrement. La confidentialité de ces clés, comme celle des données d'authentification des utilisateurs, doit être garantie par la TOE dans les cas spécifiés dans la Section 1.3.1.

Chacune des deux configurations correspond à un type de produit spécifique, selon que la TOE génère elle-même les clés de chiffrement (configuration « avec génération de clé ») ou bien qu'elle les reçoit d'un tiers de confiance (configuration « sans génération de clé »).

1.3.4 Matériel et logiciel hors-TOE

La TOE est supposée fonctionner sur tout type de matériel informatique gérant une mémoire de masse. Elle s'appuie sur le système d'exploitation (OS) ou le micrologiciel[1] (*firmware*) présent pour communiquer avec les applications clientes et l'utilisateur. Suivant les cas, les pilotes (*drivers*) de l'OS seront utilisés par la TOE pour accéder à la mémoire de masse ou bien la TOE fera elle-même office de pilote, si elle est distribuée sous cette forme (bibliothèque applicative).

Exemples de logiciel/matériel supportés par la TOE :

- Ordinateur personnel fonctionnant sous Windows®, Linux™, Mac OS X®, BSD®, Unix®...
- Clé USB et son pilote de gestion
- Disque dur amovible et micrologiciel fourni par le constructeur

[1] Logiciel intégré dans un composant matériel (disque dur, clé USB...). Exemples : BIOS, Open Firmware (IEEE-1275), OpenBoot™...

1.3.5 Utilisation du profil de protection

Les exigences introduites dans chacune des deux configurations (profil de protection) définissent les règles minimales auxquelles une cible de sécurité d'une application de chiffrement de disque dur à la volée doit se conformer, selon qu'elle génère ou non ses clés de chiffrement ; elles ne sont aucunement limitatives. Ainsi, il est possible d'ajouter d'autres fonctionnalités ou de se référer également à un autre profil de protection. L'utilisation de ce profil dans le cadre de la certification d'un dispositif matériel de chiffrement est une autre possibilité.

Cependant, toute modification au présent profil de protection est restreinte par les règles associées à la conformité précisée dans la Section 2.4.

2 Déclaration de conformité

Ce chapitre contient les sections suivantes :

2.1 Déclaration de Conformité aux CC

Ce profil de protection est conforme aux Critères Communs version 3.1.

Ce PP a été écrit conformément aux CC version 3.1 :

- CC Partie 1 [CC1]
- CC Partie 2 [CC2]
- CC Partie 3 [CC3]
- Méthodologie d'évaluation des CC [CEM]

2.2 Déclaration de conformité à un Paquet

Ce PP est conforme au paquet d'exigences d'assurance EAL3 augmenté de ALC_FLR.3 et AVA_VAN.3 pour la qualification de niveau standard défini dans [QUA-STD].

2.3 Déclaration de conformité du PP

Ce PP ne déclare de conformité à aucun autre PP.

2.4 Déclaration de conformité au PP

La conformité retenue dans ce PP pour les Cibles de Sécurité et Profils de Protection qui s'y déclarent conformes est la conformité **démontrable** selon la définition dans la Partie 1 des CC [CC1].

3 Définition du problème de sécurité

3.1 Biens

L'objectif premier de la TOE est de protéger les données enregistrées sur le disque par les utilisateurs en cas de vol du support ou de la machine le contenant. Ces données sont elles-mêmes protégées en confidentialité via le chiffrement par une ou plusieurs clés secrètes (ou publiques), suivant des mécanismes dépendants de l'implémentation. La description de chaque bien fournit les types de protection requis pour chacun d'eux (partie *Protection*).

3.1.1 Biens protégés par la TOE

D.DONNEES_UTILISATEUR

Ce bien représente les données de l'utilisateur à protéger en confidentialité sur le disque par la TOE. Il s'agit des données en clair (les données chiffrées ne sont pas un bien sensible).

Protection: confidentialité.

Note d'application

Le rédacteur de la cible de sécurité conforme à ce profil de protection pourrait également expliciter les biens sensibles de la TOE (par exemple les clés de chiffrement et les données d'authentification), à différencier des biens protégés par la TOE.

3.2 Utilisateurs

Le fonctionnement de la TOE dans son environnement opérationnel manipule directement ou indirectement les rôles décrits ci-dessous.

Utilisateur

Utilisateur de la machine dont certaines données sont à protéger en confidentialité sur le disque de la machine.

Note d'application

Le rôle d'administrateur de sécurité en charge de l'installation et de la configuration de la TOE n'intervient pas dans la problématique de sécurité considérée et le fonctionnement de la TOE ne manipule donc pas ce rôle. En outre, les rôles d'administrateur et d'utilisateur peuvent être confondus dans certains produits.

3.3 Menaces

Les menaces présentes dans cette section sont uniquement celles portant atteinte à la sécurité de la TOE et non aux services rendus par la TOE. Les différents agents menaçants sont donc d'origine extérieure à l'environnement opérationnel de la TOE, comme toute personne externe à l'organisation tirant partie du nomadisme de la machine (par exemple, vol dans un lieu public) ou un cambrioleur. Les administrateurs et les utilisateurs légitimes ne sont pas considérés comme des attaquants.

T.ACCES_DONNEES

Un attaquant prend connaissance des données sensibles de l'utilisateur stockées sur le disque, par exemple, après avoir récupéré une ou plusieurs image(s) partielle(s) ou totale(s) du disque (éventuellement à des moments différents) ou bien après avoir volé l'équipement ou le disque.

Note d'application

Suivant l'implémentation, l'image du disque peut aussi contenir d'autres biens, comme certaines clés de chiffrement.

T.ACCES_MEMOIRES

Après l'arrêt de l'application de chiffrement par l'utilisateur, un attaquant avec accès aux mémoires de travail de l'application (par exemple, RAM) prend connaissance des données sensibles de l'utilisateur ou des clés cryptographiques.

3.4 Politiques de sécurité organisationnelles (OSP)

Les politiques de sécurité organisationnelle présentes dans cette section portent uniquement sur les fonctions attendues de la TOE et ne concernent donc que les services rendus par la TOE au système d'information.

OSP.CRYPTO

Les mécanismes cryptographiques de la TOE doivent être conformes aux exigences pour le niveau de robustesse standard des référentiels cryptographiques [CRYPTO] et [CRYPTO_GESTION] de la DCSSI.

OSP.NON_REMANENCE_2

Des mesures organisationnelles préviennent la possible réutilisation de la rémanence des mémoires lors de l'arrêt de la machine dans laquelle s'exécute le produit.

Note d'application

Il est conseillé à l'utilisateur de s'assurer que l'accès à l'ordinateur après son arrêt n'est pas possible durant un certain temps. Ce temps dépend des caractéristiques des mémoires (cf. Hypothèse A.NON_REMANENCE). En général, quelques dizaines de secondes suffisent. Cette mesure n'a pas à être appliquée si le produit dispose d'une fonction technique d'effacement complet de la mémoire lors de l'arrêt du système ou s'il est démontré que les mémoires ne sont pas du tout rémanentes ou plus généralement, s'il est démontré que l'analyse du contenu de la mémoire après l'arrêt de son alimentation ne permet pas de retrouver une information utile pour l'attaquant. Attention: cette démonstration doit être faite pour un produit matériel donné et pas sur les seules caractéristiques du constructeur des mémoires.

3.5 Hypothèses

3.5.1 Hypothèses applicables aux deux configurations

Cette section décrit les hypothèses applicables aux deux configurations: "sans génération de clé" et "avec génération de clé".

A.ENV_OPERATIONNEL

L'environnement opérationnel ne permet pas à un attaquant d'accéder au disque lorsque des données sensibles sont accessibles à un utilisateur légitime sur l'équipement.

A.NON_REMANENCE_1

Les mémoires de travail utilisées par la machine qui exécute le produit ne sont pas rémanentes par construction.

Note d'application

En pratique, beaucoup de mémoires théoriquement non rémanentes sont rémanentes un certain temps après l'arrêt de l'alimentation. Ce phénomène justifie l'OSP.NON_REMANENCE_2.

3.5.2 Hypothèses applicables à la configuration sans génération de clé

Cette section décrit les hypothèses applicables exclusivement à la configuration: « sans génération de clé ».

A.ENV_OPERATIONNEL_CLES

L'environnement opérationnel de la TOE génère des clés de chiffrement de manière et de nature conformes aux exigences du référentiel de la DCSSI [CRYPTO].

Il fournit de plus ces clés à la TOE en assurant leur intégrité, leur confidentialité et leur authenticité.

4 Objectifs de sécurité

4.1 Objectifs de sécurité pour la TOE

4.1.1 Objectifs applicables aux deux configurations

Cette section décrit les objectifs pour la TOE applicables aux deux configurations: «sans génération de clé» et «avec génération de clé».

O.ARRET_UTILISATEUR

La TOE doit rendre inaccessibles les données sensibles, en particulier les clés cryptographiques, lorsque le disque est démonté par l'utilisateur.

Note d'application

Le sens de cet objectif est de permettre à un utilisateur de désactiver un disque, de mettre la TOE « hors fonctionnement », pour protéger effectivement ses données, notamment sur des machines n'ayant pas de mode « éteint » (assistants personnels). Cet objectif ne concerne en aucun cas l'effacement sécurisé des données.

O.CRYPTO

La TOE doit implémenter les fonctions de cryptographie et gérer les clés cryptographiques conformément aux exigences pour le niveau de robustesse standard des référentiels cryptographiques [CRYPTO] et [CRYPTO_GESTION] de la DCSSI.

O.PROTECTION_DES_DONNEES_ENREGISTREES

La TOE doit s'assurer que l'utilisateur a été authentifié avant de rendre accessibles les données enregistrées.

O.ROBUSTESSE

L'arrêt subit (intempestif) de la TOE (de l'équipement, du disque) ne doit pas permettre d'accéder aux données sensibles.

Note d'application

Cet objectif assure que, hors du cadre de fonctionnement nominal, la TOE n'enregistre pas en clair de façon persistante des données qui sont censées être chiffrées. En effet, un arrêt brutal de la TOE peut survenir avant le vol ou la copie de l'image. Dans ce cas, le support serait susceptible de contenir des données utilisateur non chiffrées.

4.1.2 Objectifs applicables à la configuration avec génération de clé

Cette section décrit les objectifs pour la TOE exclusivement applicables à la configuration «avec génération de clé».

En plus des objectifs pour la TOE précédents, la configuration «avec génération de clé» inclut l'objectif O.CLES_CHIFFREMENT ci-après.

O.CLES_CHIFFREMENT

La TOE doit générer des clés de chiffrement conformément aux exigences pour le niveau de robustesse standard des référentiels cryptographiques [CRYPTO] et [CRYPTO_GESTION] de la DCSSI.

4.2 Objectifs de sécurité pour l'environnement opérationnel

4.2.1 Objectifs applicables aux deux configurations

Cette section décrit les objectifs pour l'environnement applicables aux deux configurations: « sans génération de clé » et « avec génération de clé ».

OE.ENV_OPERATIONNEL.1

Lorsque l'utilisateur est authentifié, l'environnement opérationnel doit assurer la confidentialité des données sensibles, des clés et des données d'authentification.

Note d'application

L'équipement doit apporter des protections efficaces contre l'écoute illicite et la transmission non autorisée de données (pare-feu correctement configuré, antivirus avec base de données à jour, « anti-spyware », *etc.*).

Les applications installées sur l'équipement ne doivent pas perturber le bon fonctionnement de la TOE. Ainsi, les opérations que peut faire l'utilisateur sur les fichiers protégés par la TOE, surtout au travers de ses applications, ne doivent pas entraîner de copies totales ou partielles de ces fichiers en dehors de la TOE, sauf lorsqu'il l'a clairement demandé ou lorsque c'est une conséquence claire de l'opération demandée. La configuration de la machine/système/compte utilisateur/application doit confiner les fichiers protégés au sein même de la TOE, notamment en ce qui concerne les fichiers temporaires ou de travail des applications.

OE.ENV_OPERATIONNEL.2

L'utilisateur ne doit accéder à ses données sensibles que lorsqu'il se trouve dans un environnement de confiance (lorsqu'il se trouve seul ou avec des personnes ayant le besoin d'en connaître).

OE.NON_REMANENCE_1

Les mémoires de travail utilisées par la machine qui exécute le produit ne doivent pas être rémanentes par construction.

OE.NON_REMANENCE_2

L'environnement opérationnel de la TOE implémente des mesures pour éviter la réutilisation de la rémanence des mémoires lors de l'arrêt de la machine dans laquelle s'exécute l'application de chiffrement de disque.

4.2.2 Objectifs applicables à la configuration sans génération de clé

Cette section décrit les objectifs pour l'environnement exclusivement applicables à la configuration « sans génération de clé ».

Les objectifs pour l'environnement applicables à la configuration « sans génération de clé » sont les deux objectifs OE.ENV_OPERATIONNEL.1 et OE.ENV_OPERATIONNEL.2 (communs

aux deux configurations), ainsi que les deux objectifs OE.ENV_OPERATIONNEL.3 et OE.ENV_OPERATIONNEL.4 ci-après.

OE.ENV_OPERATIONNEL.3

L'environnement opérationnel de la TOE génère des clés de chiffrement de manière et de nature conformes aux exigences des référentiels cryptographiques [CRYPTO] et [CRYPTO_GESTION] de la DCSSI.

OE.ENV_OPERATIONNEL.4

L'environnement opérationnel de la TOE fournit les clés générées dans le cadre de l'objectif OE.ENV_OPERATIONNEL.3 en assurant leur intégrité, leur confidentialité et leur authenticité.

Dans une cible de sécurité compatible avec la configuration « sans génération de clé », il est possible, conformément à [CC1], section D.3, d'intégrer l'objectif sur l'environnement OE.ENV_OPERATIONNEL.4 sous forme d'objectif pour la TOE, par exemple sous la forme «La TOE doit assurer l'intégrité, la confidentialité et l'authenticité des clés qu'elle importe». La cible devra inclure en conséquence des exigences fonctionnelles pour couvrir ces objectifs, les familles FDP_ITC, FDP_UIT et FCO_UCT étant toutes indiquées.

5 Exigences de sécurité

5.1 Exigences de sécurité fonctionnelles

Dans les exigences de sécurité fonctionnelles, les deux termes suivants sont utilisés pour désigner un raffinement:

- *Raffiné éditorialement* (terme défini dans le [CC1]): raffinement dans lequel une modification mineure est faite sur un élément d'exigence, telle que la reformulation d'une phrase pour des raisons de respect de la grammaire anglaise. En aucun cas, cette modification ne doit changer la signification de l'exigence.
- *Raffinement non éditorial*: raffinement qui permet d'ajouter des précisions ou de limiter l'ensemble des implémentations acceptables pour un élément d'exigence.

Le modèle des exigences fonctionnelles de sécurité (SFR) est résumé dans la Figure 1**.**

Sujets

Les exigences fonctionnelles de sécurité (SFR) font référence aux sujets suivants:

Sujet	Attribut de sécurité	Valeurs possibles
S.API	-	-
S.DISK	Statut du disque (*AT.STATUS*)	*ACTIVATED/DEACTIVATED*
S.DISK	Identifiant Disque (*AT.ID*)	à préciser dans la ST

Remarque:

Dans le modèle de SFR, la convention suivante a été utilisée: l'attribut AT.X du sujet Y est appelé Y.X.

Chaque disque géré par la TOE est représenté par un sujet *S.DISK* maintenant un attribut de sécurité *AT.STATUS* qui reflète le fait que ce dernier est activé ou désactivé. Le disque n'est activé que lorsqu'un utilisateur authentifié s'est associé (*binding*) à ce sujet. Le sujet générique *S.API* correspond au point d'entrée, accessible à toutes les applications de la machine hôte, permettant d'accéder aux données d'un disque activé.

Dans la suite du PP, la TSF jouera le rôle d'un sujet mais, par définition, elle ne doit pas apparaître dans le tableau ci-dessus.

Objets

Les exigences fonctionnelles de sécurité (SFR) font référence aux objets suivants:

Objet	Attribut de sécurité	Valeurs possibles
S.DISK	*cf.* Sujets	*cf.* Sujets
Clé de chiffrement (*OB.KEY*)	Identifiant disque associé (*AT.ID*)	à préciser dans la ST
Données utilisateur chiffrées (*OB.UD*)	Identifiant disque associé (*AT.ID*)	à préciser dans la ST
Données d'Authentification (*OB.AD*)	Identifiant disque associé (*AT.ID*)	à préciser dans la ST

Remarque: Dans le modèle de SFR, la convention suivante a été utilisée: l'attribut AT.X de l'objet Y est appelé Y.X.

Les sujets *S.DISK* sont aussi des objets, en ce sens il existe des opérations dont les objets sont des *S.DISK*.

Une clé de chiffrement correspond implicitement à un disque. Ainsi, l'enregistrement des données utilisateur (D.DONNEES_UTILISATEUR) sur un disque, se traduit par la création ou la modification d'un objet *OB.UD* dont l'attribut de sécurité *Identifiant disque associé* (*AT.ID*) permet de savoir avec quelle clé (autrement dit, sur quel disque) les données sont chiffrées. L'objet OB.UD représente donc les mêmes données que le bien D.DONNEES_UTILISATEUR, mais une fois chiffrées par la TOE.

Les données d'authentification (*OB.AD*) associées à un disque représentent les données utilisées pour authentifier l'utilisateur du disque, lorsque celles-ci sont gérées par la TOE.

Opérations

Les exigences fonctionnelles de sécurité (SFR) font référence aux opérations suivantes:

Opération	Sujet	Objet
Création (*CREATE*)	TSF	S.DISK, OB.AD, OB.KEY
Activation (*MOUNT*)	S.DISK	S.DISK
Désactivation (*DISMOUNT*)	S.API, TSF	S.DISK
Accès (*ACCESS*)	S.DISK	OB.AD
Utilisation (*USE*)	S.API	OB.KEY
Lecture/Écriture/Effacement (*DECIPHER/CIPHER/ERASE*)	S.API	OB.UD

L'opération *CREATE* correspond intuitivement à la création d'un disque: une clé de chiffrement y est implicitement associée, qu'elle soit générée aléatoirement, dérivée à partir de données fournies par l'utilisateur (configuration « avec génération de clé ») ou bien importée (configuration « sans génération de clé »). De même, aucune exigence n'est placée sur le stockage des clés de chiffrement.

Pareillement, la création d'un disque crée aussi (*CREATE*) des données d'authentification (OB.AD) contenant les moyens d'authentifier le possesseur du disque ultérieurement. Une fois créées, ces données ne sont manipulables (*ACCESS*) que par leur créateur, l'opération

ACCESS pouvant être détaillée dans une cible de sécurité (effacement, modification, lecture...).

L'opération *MOUNT* correspond à l'activation du disque par l'utilisateur. Pour activer le disque, il doit fournir les données d'authentification OB.AD. La mise en oeuvre de cette opération entraîne une modification de l'attribut de sécurité S.DISK.STATUS qui prend la valeur ACTIVATED.

L'opération *DISMOUNT* permet de démonter un disque. La mise en oeuvre de cette opération entraîne une modification de l'attribut de sécurité S.DISK.STATUS qui prend la valeur DEACTIVATED.

L'opération *USE* correspond à l'utilisation d'une clé à des fins de chiffrement ou de déchiffrement d'un disque. Il s'agit d'une opération « interne » à la TOE qui ne fait pas partie de l'interface externe de celle-ci.

L'opération *DECIPHER* correspond à la lecture de données sur un disque géré par la TOE. La TOE ne lisant des données sur « son » disque que de manière chiffrée, il s'agit d'une opération cryptographique de déchiffrement.

L'opération *CIPHER* correspond à l'écriture de données sur un disque géré par la TOE. La TOE ne n'écrivant des données sur « son » disque que de manière chiffrée, il s'agit d'une opération cryptographique de chiffrement.

L'opération *ERASE* correspond à l'effacement de données sur un disque géré par la TOE.

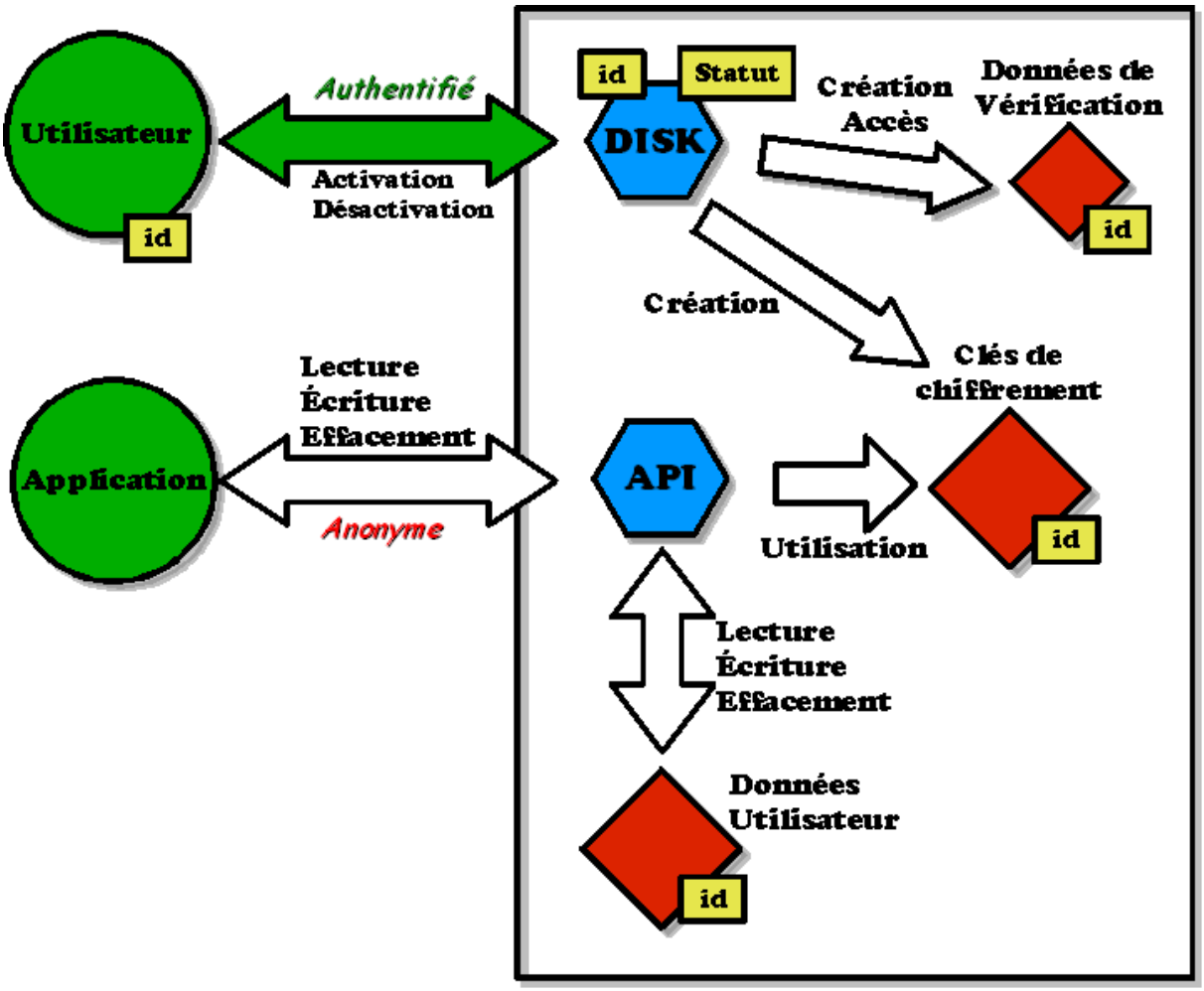

Figure 1 : Résumé de la TSP

Utilisateurs

U.User représente l'utilisateur de la machine dont certaines données sont à protéger en confidentialité sur le disque.

U.Application représente les applications effectuant les opérations de lecture, d'écriture et d'effacement en appelant le point d'entrée permettant d'accéder aux données d'un disque activé.

5.1.1 Exigences applicables aux deux configurations

5.1.1.1 Exigences liées à l'authentification des utilisateurs

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- **CREATE,**
- **DISMOUNT,**
- **USE, DECIPHER, CIPHER and ERASE**

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Raffinement non éditorial:

TSF-mediated actions include MOUNT and ACCESS.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

- **CREATE,**
- **DISMOUNT,**
- **USE, DECIPHER, CIPHER and ERASE**

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Raffinement non éditorial:

TSF-mediated actions include MOUNT and ACCESS.

The authentication mechanism must meet the DCSSI's requirements [AUTH].

Note d'application

L'authentification des utilisateurs peut se faire par une phrase de passe, etc.

5.1.1.2 Exigences liées à la robustesse de la TOE

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- **hot/warm/cold reset of the host machine**
- **when the host machine is switched off (power shortage)**
- **[assignment: other list of failures or types of failures]**.

5.1.1.3 Divers

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **TOE access control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

Raffinement non éditorial:

The restrictive values of security attributes shall be assigned according to the following rules:

- Rule STATUS: The TSF shall assign the value DEACTIVATED to the security attribute AT.STATUS whenever a S.DISK is created.
- Rule VD: Upon creation of an object OB.AD by a subject S.DISK, the TSF shall assign the value of the attribute AT.ID of S.DISK to the security attribute AT.ID of OB.AD.
- Rule KEY: Upon creation of an object OB.KEY by a S.DISK, the TSF shall assign the value of the attribute AT.ID of S.DISK to the security attribute AT.ID of OB.KEY.
- Rule DU: Upon creation of an object OB.UD, the TSF shall assign the value referencing the associated encryption key (OB.KEY) to the security attribute AT.ID of OB.UD.

FMT_MSA.3.2 [Raffiné éditorialement] The TSF shall allow **nobody** to specify alternative initial values to override the default values when an object or information is created.

Note d'application

La valeur de l'attribut de sécurité AT.ID devra être spécifiée dans la cible de sécurité du produit conforme à ce profil de protection. Cette valeur peut correspondre, par exemple, à un hachage de la phrase de passe de l'utilisateur permettant d'activer le disque.

Pour OB.UD, cette exigence exprime simplement le fait que des données utilisateur chiffrées (OB.UD) sont implicitement associées à la clé de chiffrement utilisée (OB.KEY).

FMT_MSA.1/Disk_Status Management of security attributes

FMT_MSA.1.1/Disk_Status The TSF shall enforce the **TOE access control policy** to restrict the ability to **modify** the security attributes **S.DISK.STATUS** to **the TSF itself**.

Note d'application

Aucun sujet n'est autorisé à positionner l'attribut de sécurité S.DISK.STATUS à ACTIVATED.

FMT_MSA.1/ID Management of security attributes

FMT_MSA.1.1/ID The TSF shall enforce the **TOE access control policy** to restrict the ability to **modify** the security attributes **OB.UD.ID, OB.KEY.ID, OB.AD.ID and S.DISK.ID** to **the TSF itself**.

Note d'application

Aucun sujet n'est autorisé à positionner les attributs de sécurité OB.UD.ID, OB.KEY.ID, OB.AD.ID et S.DISK.ID.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **TOE access control policy** on **subjects, objects and operations identified by this table:**

Subjects	**TSF, S.API, S.DISK**
Objects	**OB.KEY, OB.UD, OB.AD**
Operations	**CREATE, MOUNT, DISMOUNT, USE, DECIPHER, CIPHER, ERASE**

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **TOE access control policy** to objects based on the following:

Type	element	relevant security attributes(s)
Subjects	**TSF, S.API, S.DISK**	**AT.ID, and AT.STATUS (for S.DISK)**
Objects	**S.DISK, OB.KEY, OB.UD, OB.AD**	**AT.ID**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Rule	Operation	Condition
Rule1	**The TSF is allowed to CREATE a S.DISK and the associated OB.KEY and OB.AD**	**no condititon**
Rule2	**a subject S.DISK is allowed to MOUNT a S.DISK**	**The user is authenticated by the TSF based on OB.AD, the values of security attributes S.DISK.ID and OB.AD.ID are the same and the value of the security attribute S.DISK.STATUS is DEACTIVATED**
Rule3	**a subject S.API is allowed to DISMOUNT a S.DISK**	**the value of the security attribute S.DISK.STATUS is ACTIVATED**
Rule4	**a subject S.API is allowed to USE an object OB.KEY**	**the values of the security attributes S.DISK.ID and OB.KEY.ID are the same and the value of the security attribute S.DISK.STATUS is ACTIVATED**
Rule5	**a subject S.API is allowed to CIPHER, DECIPHER, ERASE an object OB.UD**	**the values of the security attributes OB.KEY.ID and OB.UD.ID are the same and S.API is allowed to USE OB.KEY (cf. Rule4)**
Rule6	**a subject S.DISK is allowed to ACCESS an object OB.AD**	**The user is authenticated by the TSF based on OB.AD and the values of the security attributes S.DISK.ID and OB.AD.ID are the same**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **Rule7: The TSF shall perform DISMOUNT operation on S.DISK after [selection: completion of [assignment: operation], [assignement: time interval of user inactivity], [assignement: other condition]] provided the value of the security attribute S.DISK.STATUS is ACTIVATED.**
- **[assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **following rule(s):**

- **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**.

Note d'application

La TSF interdit l'accès aux données d'un disque chiffrée(CIPHER, DECIPHER et ERASE) si ce disque n'a pas été activé par une authentification utilisant l'objet OB.AD associé au disque.

L'auteur d'une ST conforme à ce profil devra spécifier les conditions sous lesquelles le fonctionnement de la TOE est terminé (déterminant ainsi la désactivation de tous les disques).

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[assignment: list of cryptographic operations]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **DCSSI's cryptographic requirements ([CRYPTO] and [CRYPTO_GESTION])**.

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **cryptographic keys and any sensible user data**.

Raffinement non éditorial:

"Resource" stands for any memory (e.g. RAM) and "deallocation" occurs upon DISMOUNT of the disk by the user.

5.1.2 Exigences applicables au PP avec génération de clé

En plus des exigences pour la TOE précédentes, la configuration « avec génération de clé » inclut les exigences ci-après.

5.1.2.1 Exigences liées à la génération de clé

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **DCSSI's cryptographic requirements ([CRYPTO] and [CRYPTO_GESTION])**.

Note d'application

La génération dont il s'agit peut être une dérivation à partir des données d'authentification.

5.2 Exigences de sécurité d'assurance

Les exigences d'assurance sont applicables aux deux configurations sans changement. Le niveau d'assurance de l'évaluation de ce profil de protection est EAL3 augmenté de ALC_FLR.3 et AVA_VAN.3 conformément au processus de qualification de niveau standard défini dans [QUA-STD].

6 Argumentaires

6.1 Objectifs de sécurité / problème de sécurité

6.1.1 Menaces

T.ACCES_DONNEES La TOE enregistre sur le disque les données sensibles de l'utilisateur (bien D.DONNEES_UTILISATEUR) sous une forme chiffrée (objet OB.UD). La protection du bien se ramène donc à celle des données chiffrées.

Cette menace est contrée par O.PROTECTION_DES_DONNEES_ENREGISTREES qui garantit la confidentialité des données enregistrées (chiffrées) sur le disque. O.ROBUSTESSE contribue également à contrer cette menace en garantissant qu'aucune donnée utilisateur n'est enregistrée, même temporairement, en clair sur le disque.

D'autre part, O.ARRET_UTILISATEUR garantit que l'utilisateur peut explicitement protéger ses données en désactivant le disque sur lequel elles sont stockées.

Enfin, O.CRYPTO garantit que les fonctions de cryptographie mises en oeuvre et la gestion des clés cryptographiques utilisées empêchent l'accès non autorisé aux données du disque par cryptanalyse. La qualité des clés utilisées est assurée par cet objectif.

Dans le cas de la configuration « avec génération de clé », **O.CLES_CHIFFREMENT** garantit la disponibilité des clés cryptographiques ainsi que la qualité de leur génération (étant capable de générer les clés dont elle a besoin, suivant les référentiels cryptographiques de la DCSSI, la TOE est sûre qu'elles seront disponibles et de qualité) contribuant ainsi à la résistance à la cryptanalyse des données utilisateurs chiffrées sur le disque.

Dans le cas de la configuration « sans génération de clé », la disponibilité des clés de chiffrement utilisées par la TOE ainsi que la qualité de leur génération est garantie par l'objectif sur l'environnement **OE.ENV_OPERATIONNEL.3**. Par ailleurs, **OE.ENV_OPERATIONNEL.4** assure le confinement et la protection (intégrité, confidentialité et authenticité) des clés hors de la TOE et durant leur transmission à celle-ci.

Dans les deux cas de configuration, la qualité de la gestion des clés est garantie par **O.CRYPTO**.

Autrement dit, OE.ENV_OPERATIONNEL.3 et OE.ENV_OPERATIONNEL.4 couvrent, dans le cas de la configuration « sans génération de clé », à peu près les mêmes aspects de sécurité que l'objectif O.CLES_CHIFFREMENT dans le cas de la configuration « avec génération de clé ».

T.ACCES_MEMOIRES Cette menace est couverte par l'objectif O.ARRET_UTILISATEUR qui garantit l'indisponibilité des données sensibles, en particulier dans les mémoires de travail, après l'arrêt de l'application par l'utilisateur.

6.1.2 Politiques de sécurité organisationnelles (OSP)

OSP.CRYPTO Cette OSP est directement couverte par les objectifs O.CRYPTO et O.CLES_CHIFFREMENT dans le cas de la configuration « avec génération de clé ». Dans le cas de la configuration « sans génération de clé », l'objectif de sécurité

O.CLES_CHIFFREMENT est remplacé par les deux objectifs sur l'environnement suivants : OE.ENV_OPERATIONNEL.3 et OE.ENV_OPERATIONNEL.4

OSP.NON_REMANENCE_2 Cette politique organisationnelle est directement couverte par l'objectif OE.NON_REMANENCE_2 qui garantit l'implémentation des mesures contre la rémanence par l'environnement opérationnel.

6.1.3 Hypothèses

6.1.3.1 Hypothèses applicables aux deux configurations

A.ENV_OPERATIONNEL Cette hypothèse est directement couverte par OE.ENV_OPERATIONNEL.1 et OE.ENV_OPERATIONNEL.2.

Lorsque la TOE est en fonctionnement et qu'un utilisateur légitime a activé un disque, les applications du poste client sont susceptibles de manipuler librement les données que celui-ci contient. L'objectif OE.ENV_OPERATIONNEL.1 assure que celles-ci ne créent pas de copies de ces données sur le même support que le disque à l'insu de l'utilisateur, et que, de manière générale, le poste client ne peut être à la source d'une perte de confidentialité des données.

OE.ENV_OPERATIONNEL.2 assure que les utilisateurs légitimes sont conscients et formés aux bonnes pratiques de sécurité afin qu'ils n'accèdent à leurs données sensibles que lorsqu'ils se trouvent dans un environnement de confiance. Il participent donc à la confiance que l'on peut porter à l'environnement opérationnel de la TOE.

A.NON_REMANENCE_1 Cette hypothèse est directement couverte par OE.NON_REMANENCE_1 qui garantit l'absence de rémanence dans les mémoires de travail du produit.

6.1.3.2 Hypothèses applicables à la configuration sans génération de clé

A.ENV_OPERATIONNEL_CLES Cette hypothèse est directement couverte par OE.ENV_OPERATIONNEL.3 et OE.ENV_OPERATIONNEL.4.

6.1.4 Tables de couverture entre définition du problème et objectifs de sécurité

Menaces	Objectifs de sécurité	Argumentaire
T.ACCES_DONNEES	O.ROBUSTESSE, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.CRYPTO, O.CLES_CHIFFREMENT, O.ARRET_UTILISATEUR	Section 6.1.1
T.ACCES_MEMOIRES	O.ARRET_UTILISATEUR	Section 6.1.1

Tableau 1 Association menaces vers objectifs de sécurité

Le Tableau 1 concerne la configuration « avec génération de clé ». Dans le cas de la configuration « sans génération de clé », conformément à l'argumentaire, l'objectif de sécurité O.CLES_CHIFFREMENT est remplacé par les deux objectifs sur l'environnement suivants : OE.ENV_OPERATIONNEL.3 et OE.ENV_OPERATIONNEL.4.

Objectifs de sécurité	Menaces
O.ARRET_UTILISATEUR	T.ACCES_DONNEES, T.ACCES_MEMOIRES
O.CRYPTO	T.ACCES_DONNEES
O.PROTECTION_DES_DONNEES_ENREGISTREES	T.ACCES_DONNEES
O.ROBUSTESSE	T.ACCES_DONNEES
O.CLES_CHIFFREMENT	T.ACCES_DONNEES
OE.ENV_OPERATIONNEL.1	
OE.ENV_OPERATIONNEL.2	
OE.NON_REMANENCE_1	
OE.NON_REMANENCE_2	

Tableau 2 Association objectifs de sécurité vers menaces

Le Tableau 2 concerne la configuration « avec génération de clé ». Dans le cas de la configuration « sans génération de clé », conformément à l'argumentaire, l'objectif de sécurité O.CLES_CHIFFREMENT n'est plus applicable et la ligne (grisée) le concernant doit être remplacée par les deux lignes suivantes :

OE.ENV_OPERATIONNEL.3	T.ACCES_DONNEES
OE.ENV_OPERATIONNEL.4	T.ACCES_DONNEES

Politiques de sécurité organisationnelles (OSP)	Objectifs de sécurité	Argumentaire
OSP.CRYPTO	O.CRYPTO, O.CLES_CHIFFREMENT	Section 6.1.2
OSP.NON_REMANENCE_2	OE.NON_REMANENCE_2	Section 6.1.2

Tableau 3 Association politiques de sécurité organisationnelles vers objectifs de sécurité

Le Tableau 3 concerne la configuration « avec génération de clé ». Dans le cas de la configuration « sans génération de clé », conformément à l'argumentaire, l'objectif de sécurité O.CLES_CHIFFREMENT est remplacé par les deux objectifs sur l'environnement suivants : OE.ENV_OPERATIONNEL.3 et OE.ENV_OPERATIONNEL.4.

Objectifs de sécurité	Politiques de sécurité organisationnelles (OSP)
O.ARRET_UTILISATEUR	
O.CRYPTO	OSP.CRYPTO
O.PROTECTION_DES_DONNEES_ENREGISTREES	
O.ROBUSTESSE	
O.CLES_CHIFFREMENT	OSP.CRYPTO
OE.ENV_OPERATIONNEL.1	
OE.ENV_OPERATIONNEL.2	
OE.NON_REMANENCE_1	
OE.NON_REMANENCE_2	OSP.NON_REMANENCE_2
OE.ENV_OPERATIONNEL.3	
OE.ENV_OPERATIONNEL.4	

Tableau 4 Association objectifs de sécurité vers politiques de sécurité organisationnelles

Le Tableau 4 est applicable à la configuration « avec génération de clé ». Dans le cas de la configuration « sans génération de clé », conformément à l'argumentaire, l'objectif de sécurité O.CLES_CHIFFREMENT n'est plus applicable et la ligne (grisée) le concernant doit être remplacée par les deux lignes suivantes :

OE.ENV_OPERATIONNEL.3	OSP.CRYPTO
OE.ENV_OPERATIONNEL.4	OSP.CRYPTO

Hypothèses	Objectifs de sécurité pour l'environnement opérationnel	Argumentaire
A.ENV_OPERATIONNEL	OE.ENV_OPERATIONNEL.1, OE.ENV_OPERATIONNEL.2	Section 6.1.3
A.NON_REMANENCE_1	OE.NON_REMANENCE_1	Section 6.1.3
A.ENV_OPERATIONNEL_CLES	OE.ENV_OPERATIONNEL.3, OE.ENV_OPERATIONNEL.4	Section 6.1.3

Tableau 5 Association hypothèses vers objectifs de sécurité pour l'environnement opérationnel

Dans le Tableau 5, la ligne grisée ne s'applique qu'à la configuration « sans génération de clé». Les autres lignes s'appliquent aux deux configurations.

Objectifs de sécurité pour l'environnement opérationnel	Hypothèses
OE.ENV_OPERATIONNEL.1	A.ENV_OPERATIONNEL
OE.ENV_OPERATIONNEL.2	A.ENV_OPERATIONNEL
OE.NON_REMANENCE_1	A.NON_REMANENCE_1
OE.NON_REMANENCE_2	
OE.ENV_OPERATIONNEL.3	A.ENV_OPERATIONNEL_CLES
OE.ENV_OPERATIONNEL.4	A.ENV_OPERATIONNEL_CLES

Tableau 6 Association objectifs de sécurité pour l'environnement opérationnel vers hypothèses

Dans le Tableau 6, les lignes grisées ne s'appliquent qu'à la configuration « sans génération de clé ». Les autres lignes s'appliquent aux deux configurations.

6.2 Exigences de sécurité / objectifs de sécurité

6.2.1 Objectifs

6.2.1.1 Objectifs de sécurité pour la TOE

Objectifs applicables aux deux configurations

O.ARRET_UTILISATEUR Cet objectif est couvert par les exigences définissant la politique de contrôle d'accès FDP_ACC.1, FDP_ACF.1 et d'indisponibilité des données résiduelles FDP_RIP.1 qui assurent que:

- Un utilisateur peut explicitement désactiver un disque,
- La désactivation protège effectivement les données puisque, en vertu de la politique de contrôle d'accès de la TOE, les données d'un disque ne sont accessibles que si le statut du disque est *ACTIVATED*,
- La désactivation du disque par l'utilisateur entraîne l'effacement des données sensibles.

O.CRYPTO Cet objectif est couvert par FCS_COP.1, qui assure que toutes les opérations cryptographiques doivent obéir aux exigences des référentiels cryptographiques de la DCSSI pour le niveau de robustesse standard ([CRYPTO] et [CRYPTO_GESTION]).

O.PROTECTION_DES_DONNEES_ENREGISTREES La TOE enregistre sur le disque les données sensibles de l'utilisateur (D.DONNEES_UTILISATEUR) sous une forme chiffrée (objet OB.UD). La protection du bien se ramène donc à la protection de celles-ci.

Le contrôle d'accès (FDP_ACC.1 et FDP_ACF.1) assure que les seuls objets accessibles à un instant donné sont associés à un disque activé. Ce contrôle impose par ailleurs le chiffrement des données utilisateurs enregistrées sur le disque (sans lequel la protection ne saurait être efficace).

D'autre part, les exigences liées à l'authentification obligatoire d'un utilisateur avant l'activation d'un disque (FIA_UID.1 et FIA_UAU.1) assurent que seul l'utilisateur légitime contrôle l'accès aux données qui y sont enregistrées. L'accès lui-même ne demande aucune authentification (FIA_UID.1).

Enfin, l'association définitive, à un disque donné (S.DISK), des données sensibles de l'utilisateur enregistrées (OB.UD) et des données d'authentification (OB.AD, OB.KEY) permettant son authentification, évite les « fuites » d'information d'un disque à l'autre sans que les disques soient activés. En effet, tous ces objets et sujets sont reliés par un attribut de sécurité AT.ID fixé une fois pour toutes lors de leur création (FMT_MSA.3, FMT_MSA.1/Disk_Status et FMT_MSA.1/ID).

O.ROBUSTESSE Cet objectif est couvert par les exigences qui assurent que toute interruption de la TOE, fortuite (FPT_FLS.1), automatique ou délibérée (FDP_ACF.1), laissent la TOE, et surtout les données qu'elle protège, dans un état robuste, à savoir un état où les disques concernés sont désactivés; autrement dit, les clés de chiffrement ne sont plus accessibles hors-fonctionnement.

Objectifs applicables à la configuration avec génération de clé

O.CLES_CHIFFREMENT Cet objectif est directement couvert par l'exigence FCS_CKM.1.

6.2.2 Tables de couverture entre objectifs et exigences de sécurité

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.ARRET_UTILISATEUR	FDP_ACC.1, FDP_ACF.1, FDP_RIP.1	Section 6.2.1
O.CRYPTO	FCS_COP.1	Section 6.2.1
O.PROTECTION_DES_DONNEES_ENREGISTREES	FDP_ACF.1, FIA_UID.1, FIA_UAU.1, FMT_MSA.3, FMT_MSA.1/Disk_Status, FMT_MSA.1/ID, FDP_ACC.1	Section 6.2.1
O.ROBUSTESSE	FPT_FLS.1, FDP_ACF.1	Section 6.2.1
O.CLES_CHIFFREMENT	FCS_CKM.1	Section 6.2.1

Tableau 7 Association objectifs de sécurité de la TOE vers les exigences fonctionnelles

Dans le Tableau 7, la ligne grisée ne s'applique qu'à la configuration « avec génération de clé». Les autres lignes s'appliquent aux deux configurations.

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FIA_UID.1	O.PROTECTION_DES_DONNEES_ENREGISTREES
FIA_UAU.1	O.PROTECTION_DES_DONNEES_ENREGISTREES
FPT_FLS.1	O.ROBUSTESSE
FMT_MSA.3	O.PROTECTION_DES_DONNEES_ENREGISTREES
FMT_MSA.1/Disk_Status	O.PROTECTION_DES_DONNEES_ENREGISTREES
FMT_MSA.1/ID	O.PROTECTION_DES_DONNEES_ENREGISTREES
FDP_ACC.1	O.ARRET_UTILISATEUR, O.PROTECTION_DES_DONNEES_ENREGISTREES
FDP_ACF.1	O.ARRET_UTILISATEUR, O.PROTECTION_DES_DONNEES_ENREGISTREES , O.ROBUSTESSE
FCS_COP.1	O.CRYPTO
FDP_RIP.1	O.ARRET_UTILISATEUR
FCS_CKM.1	O.CLES_CHIFFREMENT

Tableau 8 Association exigences fonctionnelles vers objectifs de sécurité de la TOE

Dans le Tableau 8, la ligne grisée ne s'applique qu'à la configuration « avec génération de clé». Les autres lignes s'appliquent aux deux configurations.

6.3 Dépendances

6.3.1 Dépendances des exigences de sécurité fonctionnelles

Exigences	Dépendances CC	Dépendances Satisfaites
FMT_MSA.3	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/Disk_Status, FMT_MSA.1/ID
FMT_MSA.1/Disk_Status	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1
FMT_MSA.1/ID	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1
FDP_ACC.1	(FDP_ACF.1)	FDP_ACF.1
FDP_ACF.1	(FDP_ACC.1) et (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1
FCS_COP.1	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FCS_CKM.1
FDP_RIP.1	Pas de dépendance	
FIA_UID.1	Pas de dépendance	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FPT_FLS.1	Pas de dépendance	
FCS_CKM.1	(FCS_CKM.2 ou FCS_COP.1) et (FCS_CKM.4)	FCS_COP.1

Tableau 9 Dépendances des exigences fonctionnelles

Dans le Tableau 9, la ligne grisée n'est applicable qu'à la configuration « avec génération de clé ». Les autres lignes s'appliquent aux deux configurations.

6.3.1.1 Argumentaire pour les dépendances non satisfaites

La dépendance FMT_SMR.1 de FMT_MSA.3 n'est pas supportée. Cette dépendance n'est pas requise puisque le modèle n'utilise pas la notion de rôle.

La dépendance FMT_SMF.1 de FMT_MSA.1/Disk_Status n'est pas supportée. La TOE ne gère pas de fonction de gestion. Cette dépendance n'est donc pas requise.

La dépendance FMT_SMR.1 de FMT_MSA.1/Disk_Status n'est pas supportée. Cette dépendance n'est pas requise puisque le modèle n'utilise pas la notion de rôle.

La dépendance FMT_SMF.1 de FMT_MSA.1/ID n'est pas supportée. La TOE ne gère pas de fonction de gestion. Cette dépendance n'est donc pas requise.

La dépendance FMT_SMR.1 de FMT_MSA.1/ID n'est pas supportée. Cette dépendance n'est pas requise puisque le modèle n'utilise pas la notion de rôle.

La dépendance FCS_CKM.4 de FCS_COP.1 n'est pas supportée. La phase de destruction des clés n'entre pas dans le périmètre de la TOE; cette exigence n'a donc pas besoin d'être satisfaite.

La dépendance FCS_CKM.4 de FCS_CKM.1 n'est pas supportée. La phase de destruction des clés n'entre pas dans le périmètre de la TOE; cette exigence n'a donc pas besoin d'être satisfaite.

6.3.2 Dépendances des exigences de sécurité d'assurance

Exigences	Dépendances CC	Dépendances Satisfaites
ADV_ARC.1	(ADV_FSP.1) et (ADV_TDS.1)	ADV_FSP.3, ADV_TDS.2
ADV_FSP.3	(ADV_TDS.1)	ADV_TDS.2
ADV_TDS.2	(ADV_FSP.3)	ADV_FSP.3
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.3
AGD_PRE.1	Pas de dépendance	
ALC_CMC.3	(ALC_CMS.1) et (ALC_DVS.1) et (ALC_LCD.1)	ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	Pas de dépendance	
ALC_DEL.1	Pas de dépendance	
ALC_FLR.3	Pas de dépendance	
ALC_DVS.1	Pas de dépendance	
ALC_LCD.1	Pas de dépendance	
ASE_CCL.1	(ASE_ECD.1) et (ASE_INT.1) et (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	Pas de dépendance	

Exigences	Dépendances CC	Dépendances Satisfaites
ASE_INT.1	Pas de dépendance	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) et (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	Pas de dépendance	
ASE_TSS.1	(ADV_FSP.1) et (ASE_INT.1) et (ASE_REQ.1)	ADV_FSP.3, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) et (ATE_FUN.1)	ADV_FSP.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) et (AGD_OPE.1) et (AGD_PRE.1) et (ATE_COV.1) et (ATE_FUN.1)	ADV_FSP.3, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) et (ADV_TDS.2) et (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) et (ADV_FSP.2) et (ADV_IMP.1) et (ADV_TDS.3) et (AGD_OPE.1) et (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.3, AGD_OPE.1, AGD_PRE.1

Tableau 10 Dépendances des exigences d'assurance

6.3.2.1 Argumentaire pour les dépendances non satisfaites

La dépendance ADV_IMP.1 de AVA_VAN.3 n'est pas supportée. Cette dépendance n'est pas nécessaire conformément à l'EAL requis pour la qualification standard [QUA-STD].

La dépendance ADV_TDS.3 de AVA_VAN.3 n'est pas supportée. Cette dépendance n'est pas nécessaire conformément à l'EAL requis pour la qualification standard [QUA-STD].

6.4 Argumentaire pour l'EAL

Le niveau d'assurance de l'évaluation de ce profil de protection est EAL3 augmenté de ALC_FLR.3 et AVA_VAN.3 conformément au processus de qualification de niveau standard défini dans [QUA-STD].

6.5 Argumentaire pour les augmentations à l'EAL

6.5.1 AVA_VAN.3 Focused vulnerability analysis

Augmentation requise par le processus de qualification standard [QUA-STD].

6.5.2 ALC_FLR.3 Systematic flaw remediation

Augmentation requise par le processus de qualification standard [QUA-STD].

7 Notice

Ce document a été généré avec TL SET version 2.2.8 (for CC3). Pour plus d'informations sur l'outil d'édition sécuritaire de Trusted Labs consultez le site internet www.trusted-labs.com.

Annexe A Compléments de description de la TOE et de son environnement

Cette annexe est informative.

A.1 Domaine d'application

Le terme « disque » doit être compris comme toute **mémoire de masse persistante**, indépendamment du support électronique sous-jacent (clé USB, RAMDisk, *etc.*).

On parlera également de « support » pour désigner le matériel hébergeant le disque.

Le Tableau 11 présente les différentes unités d'allocation de données d'un disque considéré comme un espace de stockage de données, des unités les plus vastes aux plus réduites.

Tableau 11 : Unités d'allocation

Nom	*Définition*	*Périmètre du PP*
Disque complet	Le disque physique, sans distinction des différents plateaux (disques RAID) éventuels.	Inclus
Partition	Découpage du disque en pseudo-disques distincts. Au niveau du BIOS. Par exemple, Windows identifie partitions et disques sous le nom de « volume ».	Inclus
Sous-partition	N'existe que sur certains OS (par exemple, *slices* des systèmes BSD). En-dessous du système de fichiers.	Inclus
Répertoire	Au niveau du système de fichiers de l'OS. Par exemple, les OS de la famille Unix ne font pas la différence entre les répertoires et les (sous-)partitions.	Inclus
Groupe de fichiers	Ensemble de fichiers « marqués » d'une façon ou d'une autre, généralement un attribut du fichier, géré par la TOE ou l'OS. La notion de groupe est indépendante de la hiérarchie du système de fichiers.	Inclus
Fichier	Contient les données utilisateur et est identifié par un nom.	Hors-contexte
Bloc (cluster)	Unité d'allocation du système de gestion de fichiers. Le Bloc est généralement une abstraction du secteur.	Hors-contexte
Secteur	Unité d'allocation élémentaire d'un disque formaté contenant les données utiles.	Hors-contexte
Piste	Pour un disque, données contenues sur une circonférence d'un plateau d'un disque. Typiquement, une piste contient des secteurs, des informations de gestion du disque (n° de secteur, CRC de secteur, n° de piste, etc.), d'espaces intersecteurs (GAP) et d'espace de fin de piste (GAP) ne contenant normalement pas d'informations utiles.	Hors-contexte

La TOE concernée par ce PP est une application chiffrant de manière transparente (« à la volée ») une ou plusieurs unités d'allocation parmi les cinq plus grandes : disque, partition, sous-partition, répertoire ou groupe de fichiers. Par abus de langage, on désigne dans ce PP par « disque » l'espace de stockage chiffré par la TOE, indépendamment du type d'unité d'allocation effectivement concerné.

Une application proposant des « disques virtuels » qui enregistre les données chiffrées dans un fichier de l'OS, mais les présente comme des disques à part entière pour l'utilisateur, entre aussi dans le cadre de ce profil.

Il importe de ne pas confondre cette notion de disque avec l'unité logique de chiffrement utilisée par les algorithmes cryptographiques de l'application. La TOE peut par exemple chiffrer des partitions complètes, mais par bloc ou par secteur, en utilisant une clé dérivée pour chaque bloc ou chaque secteur. L'unité logique de chiffrement n'a d'impact que pour l'évaluation du produit (analyse de vulnérabilité) et son implémentation.

A.2 Utilisation de la TOE

A.2.1 Analogie du coffre-fort

Pour mieux cerner l'utilisation de la TOE, il peut être utile de comparer une application de chiffrement à la volée à un coffre-fort ou une armoire renforcée. Le premier objectif d'un coffre-fort est de protéger son contenu contre le vol, **une fois fermé**. De même, une application de chiffrement vise à protéger des données logicielles une fois celles-ci chiffrées et le disque « désactivé ».

Pour pousser l'analogie plus loin, durant la journée, lorsque le personnel est présent dans les locaux, le coffre-fort est susceptible d'être ouvert et son contenu manipulé par les personnes présentes. L'accès au contenu du coffre est alors réglementé par des mesures organisationnelles et matérielles (contrôle d'accès au local contenant le coffre, caméras de surveillance, *etc.*). Il apparaît donc clairement que la protection apportée par un coffre-fort lui-même ne concerne pas les données en cours d'utilisation mais uniquement lorsqu'elles sont stockées (enregistrées sur le disque). Cela signifie notamment que les aspects critiques de la sécurité d'un coffre-fort concernent son ouverture et sa fermeture :

- Qui peut l'ouvrir ? Dans quelles circonstances ?
- Qui peut le fermer ? Dans quelles circonstances ?
- En quoi cela consiste-t-il ?

Pareillement, une application de chiffrement de disque peut ne pas protéger les données enregistrées une fois celui-ci « activé » ou lorsqu'elles sont manipulées par une application (dans la mémoire du poste de travail). En particulier, les questions de partage de disque sont souvent du ressort de la gestion des droits du système d'exploitation ou du réseau. Bien que cela n'exclue pas que l'application intègre aussi de tels mécanismes, ceux-ci n'entrent pas dans le périmètre de la TOE.

A.2.2 Clés et données d'authentification

Les données d'authentification permettent aux utilisateurs (et aux éventuels administrateurs) de s'authentifier vis-à-vis de la TOE pour activer un disque ou bien le configurer.

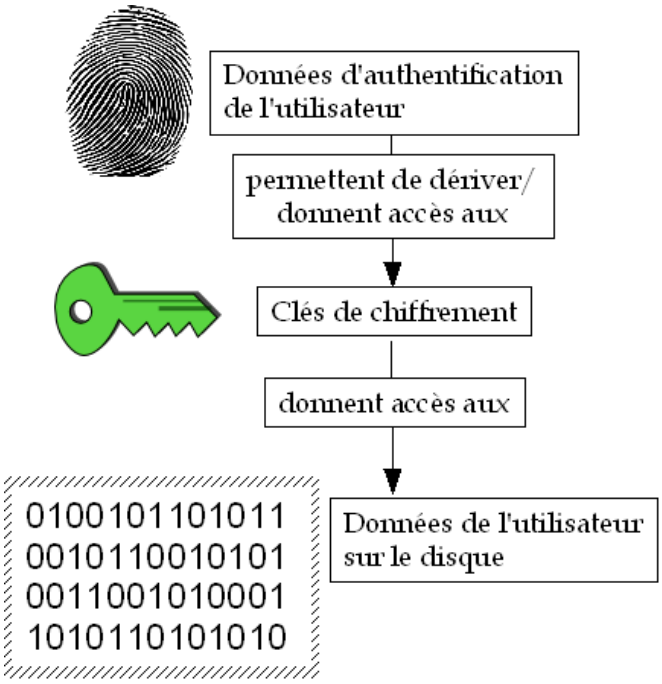

Figure 2 : Principe illustratif d'activation du disque.

Les clés sont les données cryptographiques utilisées par la TOE pour chiffrer (et déchiffrer) les données enregistrées sur le disque.

La connaissance de certaines de ces clés donne accès au contenu du disque ou d'une portion de celui-ci, indépendamment de la TOE, et la connaissance des données d'authentification donne accès aux clés[2].

La distinction entre ces deux notions s'appuie sur les propriétés suivantes :

- Les données d'authentification sont normalement connues de l'utilisateur tandis que les clés n'ont à être connues que de la TOE.
- Les données d'authentification devraient être modifiables aisément (par exemple, un changement de mot de passe ne devrait pas nécessiter de rechiffrer tout le disque), ce qui n'est pas le cas des clés.
- Les données d'authentification ne sont utilisées que de façon ponctuelle (notamment pour activer le disque) tandis que les clés de chiffrement restent en mémoire pour déchiffrer les données à la demande de l'utilisateur authentifié.

En pratique, la relation entre ces données peut être extrêmement variable d'une implémentation à l'autre. Ainsi, les données d'authentification peuvent servir à dériver directement la clé de chiffrement ou bien n'être utilisées que pour chiffrer (déchiffrer) la clé de chiffrement du disque, *etc.* Dans le premier cas, un changement de donnée d'authentification nécessitera de « transchiffrer » le disque alors que dans le second cas, seule la clé de chiffrement du disque devra être « transchiffrée ».

A.2.3 Fonctionnement de la TOE

La TOE est un intermédiaire transparent entre les applications que l'utilisateur emploie pour manipuler ses données (lecture, modification, sauvegarde), et le support de stockage contenant le disque chiffré. L'utilisateur n'a d'interaction explicite avec la TOE que de deux

[2] Conformément au principe de Kerchoff, on suppose que la relation entre les données d'authentification et les clés est une information connue de l'attaquant.

façons : au moment où il accède au disque chiffré pour la première fois en activant le disque et au moment où il désactive explicitement le disque.

L'activation du disque requiert l'authentification de l'utilisateur. Une fois activé, rien ne distingue le disque chiffré des autres mémoires de masse auxquelles l'utilisateur a accès.

En cours de fonctionnement, la TOE chiffre (respectivement, déchiffre) de façon transparente pour l'utilisateur, les données enregistrées (respectivement, lues) sur le disque. Les caractéristiques du procédé de chiffrement dépendent de la mise en œuvre (primitives et algorithmes cryptographiques, taille des clés, *etc.*).

A.3 Fonctionnalités de la TOE

La fonctionnalité principale de la TOE est de protéger en confidentialité les données enregistrées sur une mémoire de masse persistante pour faire face à un vol du support ou de la machine le contenant, tout en permettant à un utilisateur autorisé de les consulter :

- Protection en confidentialité des données stockées sur le disque

De plus, pour son bon fonctionnement, la TOE requiert les services suivants :

- Authentification
  - Authentification de l'utilisateur

A.3.1 Services fournis par la TOE

Protection en confidentialité des données sensibles stockées sur le disque

Le service principal fourni par la TOE est de protéger en confidentialité les données sensibles enregistrées sur le disque. Cette protection en confidentialité doit s'appliquer notamment aux versions temporaires des données gérées par d'autres applications ou par le système d'exploitation de la machine.

A.3.2 Services nécessaires au bon fonctionnement de la TOE

Authentification de l'utilisateur

L'utilisation de l'application de chiffrement de disque est conditionnée à l'authentification préalable de l'utilisateur (par exemple, à travers la saisie d'une phrase de passe). Cette authentification permet d'activer le disque et d'accéder aux données qui y sont stockées.

A.4 Éléments relatifs à la conception

A.4.1 Périmètre physique et logique de la TOE

La TOE définie dans ce PP fonctionne sur tout type de matériel informatique disposant d'une mémoire de stockage persistante (éventuellement amovible). La procédure d'authentification des utilisateurs et le fonctionnement de la TOE (chiffrement et déchiffrement) peuvent faire appel à des matériels spécifiques (clés USB, cartes à puce, *etc.*) en fonction de la mise en œuvre mais ce PP ne pose aucune exigence particulière concernant le matériel hors-TOE.

Par ailleurs, il sera supposé que les applications présentes sur la machine peuvent être configurées pour qu'elles puissent sauvegarder les données de l'utilisateur de manière transparente sur la mémoire persistante protégée et gérée par la TOE.

A.4.2 À propos des configurations

Les deux configurations introduites dans ce document visent à couvrir deux types de produits courants tout en gardant un maximum de souplesse pour la rédaction d'une cible : les produits orientés « mono-poste », générant les clés de chiffrement par eux-mêmes, et les produits orientés « grande organisation », fonctionnant en coopération avec un serveur de clés centralisé, pouvant par exemple faire office de séquestre (cf. section suivante).

Dans tous les cas, le principe est d'assurer que la qualité des clés générées est d'un niveau suffisant pour que la TOE puisse contrer la menace du vol du disque. Dans le cas de la configuration « avec génération », les algorithmes de génération des clés font partie du périmètre de la TOE et sont donc évalués avec le produit ; dans le cas « sans génération », la formulation des hypothèses pointe explicitement sur l'importance de la génération des clés, et il est raisonnable de penser que l'utilisateur devra s'appuyer sur un produit de confiance, éventuellement certifié indépendamment.

A.5 Services supplémentaires

Cette section présente différents services additionnels susceptibles d'être implémentés par un produit conforme à ce PP.

A.5.1 Auto-verrouillage

Le produit désactive automatiquement le disque après une limite de temps d'inactivité définie par un administrateur de sécurité lors de la configuration initiale. Une ré-authentification de l'utilisateur est alors nécessaire pour activer à nouveau le disque.

Ce type de mécanisme permet d'améliorer la protection des données en cas d'absence plus ou moins prolongée de l'utilisateur loin de son poste de travail ou bien de l'oubli de la part de celui-ci de désactiver son disque. Certaines implémentations sont coordonnées avec d'autres logiciels analogues, comme l'économiseur d'écran de la machine hôte.

A.5.2 Séquestre et recouvrement

Dans le cadre d'une utilisation professionnelle, le recouvrement des données peut être aussi important que leur protection. Les produits offrent alors la possibilité d'exporter une ou plusieurs clés de séquestre ou de recouvrement pour un stockage distant. Il s'agit d'assurer la disponibilité de ces données dans les cas suivants :

- · perte/oubli des données d'authentification par l'utilisateur,
- · sur demande au sein de l'organisme (en cas de commission rogatoire, par exemple).

Les solutions de recouvrement peuvent être multiples. Il peut s'agir, par exemple, d'un export en clair des clés de chiffrement ou des données d'authentification des utilisateurs permettant leur stockage sur un autre support. Il peut s'agir aussi d'un chiffrement sur le disque de copies des clés de chiffrement à l'aide d'une clé de séquestre.

Au niveau organisationnel, il importe de définir précisément les rôles des différents acteurs impliqués dans la procédure de recouvrement, notamment pour éviter le détournement de

celle-ci par des attaquants (*i.e.* un attaquant ayant volé un disque se fait passer pour l'utilisateur légitime auprès du service de recouvrement).

A.5.3 Sauvegarde

Le chiffrement des données s'oppose parfois aux exigences de sauvegarde[3]. Le produit peut ou non permettre la sauvegarde des données chiffrées (image disque), ou bien celle des données en clair (ce qui revient à avoir plusieurs utilisateurs d'un même disque).

A.5.4 Gestion des rôles

Le produit peut distinguer différentes catégories d'utilisateurs et leur attribuer des droits spécifiques. Dans le cadre d'un déploiement dans le cadre d'une administration ou d'une entreprise les personnes installant, configurant et utilisant un poste de travail peuvent être distinctes (administrateur système, administrateur de sécurité, utilisateur), et le produit peut refléter cette séparation des tâches en distinguant les rôles suivants :

- **Utilisateur :** utilisateur de la machine dont certaines données sont à protéger en confidentialité sur la mémoire de masse persistante de la machine.
- **Administrateur système et réseaux :** administrateur responsable de la machine. Il configure les paramètres de la machine (les comptes utilisateurs et les noms de volume par exemple), mais il n'installe ni ne configure l'application de chiffrement.
- **Administrateur de sécurité :** administrateur en charge de l'installation et de la configuration de l'application de chiffrement. L'administrateur de sécurité définit les données qui doivent être chiffrées et à quel endroit.

Parmi les paramètres exclusivement contrôlables par un de ces rôles, citons :

- la taille des clés et la nature des algorithmes de chiffrement utilisés par le produit,
- le contrôle par le produit de la qualité des données d'authentification choisies par les utilisateurs (taille minimale, présence de caractères non-alphanumériques, *etc.*)
- le renouvellement obligatoire des clés ou des données d'authentification à période déterminée
- la possibilité ou non de désactiver le produit
- la configuration du poste de travail, comme le fait que les partitions de *swap* soient sous le contrôle de la TOE, la gestion des fichiers temporaires par les applications clientes, la désactivation de la mise en veille de la machine hôte...

A.5.5 Effacement sécurisé

La TOE définie dans ce profil définit une opération d'effacement des données sur un disque actif. Un produit peut définir des exigences relatives à l'effacement sécurisé des données s'appliquant à cette opération, par exemple pour assurer l'impossibilité de récupérer les données supposées effacées.

Dans le même ordre d'idée, il peut être nécessaire de définir une procédure spécifiant sous quelles conditions et de quelle façon un administrateur de sécurité doit détruire de manière irréversible les données contenues sur le disque d'un utilisateur. Cette procédure est susceptible de s'appliquer, par exemple, en cas de départ ou de démission d'un utilisateur de l'organisation, ou bien lorsque le disque est attribué à un nouvel usage ou utilisateur. La

[3] Ainsi, les données chiffrées ne permettent généralement pas de sauvegarder incrémentalement les données de manière efficace.

façon dont ces données sont détruites ou rendues indisponibles peut ou non s'appuyer sur des mécanismes du produit comme, par exemple, le transchiffrement du disque ou l'effacement par écrasement (bruit) systématique.

Ces exigences pourront s'exprimer en utilisant le composant FDP_RIP.2 (*Full residual information protection*).

Annexe B Définitions et acronymes

Cette annexe donne la définition des principaux termes utilisés dans ce document. Pour la définition des termes Critères Communs, se référer à [CC1], Section 4.

B.1 Abréviations et acronymes

BIOS	(*Basic Input Output System*) Système de base d'entrée-sortie
CC	(*Common Criteria*) Critères Communs
EAL	(*Evaluation Assurance Level*) Niveau d'assurance de l'évaluation
IT	(*Information Technology*) Technologies de l'information
OS	(*Operating System*) Système d'exploitation
OSP	(*Organisational Security Policy*) Politique de sécurité organisationnelle
PP	(*Protection Profile*) Profil de protection
SFR	(*Security Function Requirement*) Exigence fonctionnelle de sécurité
ST	(*Security Target*) Cible de sécurité
TI	Technologie de l'Information
TOE	(*Target Of Evaluation*) Cible d'évaluation

B.2 Définitions

Cible d'évaluation (TOE)

Le produit à évaluer et sa documentation associée.

Cible de sécurité (ST)

Document servant de référence à l'évaluation de la cible d'évaluation : le certificat délivré par la DCSSI attestera de la conformité du produit et de sa documentation aux exigences formulées dans la cible de sécurité.

Disque

Mémoire de masse persistante contenant les données chiffrées par la TOE.

Image (du) disque

Ensemble des données (chiffrées) de la mémoire de masse persistante.

Machine

Équipement qui héberge l'application de chiffrement de la mémoire de masse persistante (ordinateur portable, serveur en réseau, *etc.*).

Support

Périphérique physique hébergeant la mémoire de masse persistante. Le support n'est pas forcément complètement sous le contrôle de la TOE, en ce sens que la mémoire protégée ne peut n'être qu'une partie de celui-ci.

Annexe C Traduction des termes anglais

Les exigences étant exprimées intégralement en anglais dans le PP, une traduction des termes anglais spécifiques à la TOE utilisés dans la Section 5 est fournie ci-dessous.

Disk	Disque
Encryption key	Clé de chiffrement
Identifier	Identifiant
Object	Objet
Operation	Opération
Security attribute	Attribut de sécurité
Security policy	Politique de sécurité
Subject	Sujet
User	Utilisateur

Annexe D Références

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006. CCMB-2006-09-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 2, September 2007. CCMB-2007-09-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 2, September 2007. CCMB-2007-09-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 2, September 2007. CCMB-2007-09-004.

[CRYPTO] Mécanismes de cryptographie : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications

[CRYPTO_GESTION] Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications

[AUTH] Authentification : Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard. DCSSI. http://www.ssi.gouv.fr/fr/sciences/publications

[QUA-STD] Processus de qualification d'un produit de sécurité – niveau standard. Version 1.1, 18 mars 2008. N°549/SGDN/DCSSI/SDR.

PP-CDISK Profil de Protection « Application de chiffrement de données à la volée sur mémoire de masse », version CC 3.0.

Index