Stormshield Endpoint Security

Version 7.2

Cible de Sécurité EAL3+

Document version : 1.9

Référence : KIBO/Cible

Date: 11/04/2017

Table des matières

Liste des figures

Liste des tableaux

TERMINOLOGIE ET SIGLES UTILISES

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
BIOS	Basic Input Output System (Système de base d'entrée-sortie)
EAL	Evaluation Assurance Level (Niveau d'assurance de l'évaluation)
OSP	Organisational Security Policy (Politique de sécurité organisationnelle)
Politique de sécurité	Ensemble des paramètres des fonctions de sécurité.
PP	Profil de Protection
PSSI	Politique de Sécurité du Système d'Information
SES	Stormshield Enpoint Security
TSF	TOE Security Functionality (Fonctionnalité de Sécurité de la TOE)
TOE	Target Of Evaluation (Cible d'évaluation)

DOCUMENTS DE REFERENCE

[CC]	Common Criteria for Information Technology Security Evaluation, version 3.1 revision 4 - Part 1: Introduction and general model, ref. CCMB-2012-09-001 - Part 2: Security functional requirements, ref. CCMB-2012-09-002 - Part 3: Security assurance requirements, ref. CCMB-2012-09-003
[QUALIF_STD]	Référentiel général de sécurité - Processus de qualification d'un produit de sécurité – Niveau Standard Version 1.2.
[RGS_CRYPTO]	Référentiel général de sécurité Version 2.0 Annexe B1 Mécanismes cryptographiques Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques Version 2.03 du 21 février 2014
[RGS_CLES]	Référentiel général de sécurité Version 2,0 Annexe B2 Gestion des clés cryptographiques Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques Version 2.00 du 8 juin 2012
[RGS_AUTH]	Référentiel général de sécurité Annexe B3 Authentification Règles et recommandations concernant les mécanismes d'authentification Version 1.00 du 13 janvier 2010
[CDISK]	Profil de Protection Application de chiffrement de données à la volée sur mémoire de masse PP-CDISK-CCv3.1, Version 1.4 - Août 2008

1. INTRODUCTION DE LA CIBLE DE SECURITE

1.1 Identification de la cible de sécurité

Titre :	Stormshield Endpoint Security – Cible de Sécurité
Référence :	KIBO/Cible
Version :	1.9

1.2 Identification de la cible d'évaluation (TOE)

Nom du produit :	Stormshield Enpoint Security
Développeur :	Stormshield
Version :	7.2.06 build 29579

1.3 Vue d'ensemble de la TOE

1.3.1 Type de TOE

La cible de l'évaluation est une application de chiffrement de surface, aussi appelé chiffrement de disque avec authentification pré-boot (i.e. avant le démarrage du système).

La présente cible de sécurité est conforme au profil de protection "Application de chiffrement de données à la volée sur mémoire de masse" [CDISK]. Les parties extraites de ce profil de protection sont indiquées en bleu.

1.3.2 Présentation de la TOE

1.3.2.1 Stormshield Endpoint Security

La suite logicielle Stormshield Endpoint Security (en abrégé SES) est une solution de sécurisation des postes de travail et des serveurs sous Windows : elle permet à une organisation de protéger de manière centralisée l'intégralité de son parc de serveurs, micro-ordinateurs et ordinateurs portables contre les attaques informatiques connues et inconnues, le vol ou la perte de données, les intrusions informatiques et les opérations non autorisées.

Plus précisément, cette suite modulaire réunit les fonctions de sécurité suivantes :

- **Prévention d'intrusion** (H-IPS). SES bloque les attaques en détectant la mise en œuvre d'une technique d'intrusion telle que le débordement de mémoire (buffer overflow), l'espionnage des frappes au clavier (keylogging) ou la corruption des processus en mémoire.

  SES protège également des attaques provenant du réseau à l'aide d'un pare-feu qui détecte et bloque les activités réseau suspectes.

- **Contrôle des périphériques.** SES permet de contrôler les supports de données amovibles tels que les périphériques USB, les disques durs externes, les iPod, les cartes réseaux, les graveurs de CD/DVD, les ports Série/Parallèle et les périphériques Firewire.

  SES permet par exemple de désactiver le copier/coller, la fonction Plug-and-Play des périphériques USB, le lancement automatique des CD et des DVD, la gravure, etc. Il est également possible de n'autoriser que les périphériques USB dûment identifiés à l'aide de leur numéro de série, et d'imposer le chiffrement des données copiées sur ces périphériques.

- **Contrôle d'accès au réseau.** SES applique dynamiquement ses politiques en fonction du contexte de l'utilisateur, du poste, et du réseau.

  L'administrateur peut notamment définir des règles de sécurité différentes selon que le poste est dans le réseau de l'entreprise, à l'extérieur, à l'extérieur mais connecté au travers du VPN d'entreprise, etc. Au niveau système, cette fonctionnalité permet de contrôler la conformité des postes de travail : antivirus présent, démarré, à jour, applications interdites absentes, etc.

- **Contrôle des applications**. SES permet de créer des listes blanches d'applications autorisées ou des listes noires d'applications à risque.

  L'administrateur peut affiner sa politique de sécurité en définissant, par application, des droits d'accès : au réseau, à la base de registre, aux fichiers (éventuellement en fonction de l'extension des fichiers).

- **Sécurité des réseaux sans fil**. SES permet de contrôler l'utilisation des connexions WIFI et Bluetooth.

  Il est par exemple possible d'imposer l'authentification et le chiffrement protocolaires (WEP, WPA, WPA2, etc), d'imposer le passage par le VPN de l'entreprise, d'interdire les connexions en mode ad-hoc, de limiter les points d'accès accessibles. Les connexions Bluetooth peuvent être contrôlées de la même manière.

- **Chiffrement de contenu.** SES permet de préserver la confidentialité des données hébergées sur le poste de travail.

  Il offre pour cela deux niveaux de chiffrement qui peuvent être combinés : le **chiffrement complet du disque** (ou chiffrement de surface), et le chiffrement **à la volée des fichiers**.

- **Anti-Virus**. En complément de son module H-IPS, SES propose une protection traditionnelle anti-virus et anti-spyware basée sur des techniques de signature.

  SES analyse les fichiers, les emails reçus, le trafic internet, la messagerie instantanée et supprime toute trace de logiciel malveillant.

La politique de sécurité du parc protégé est définie de manière centralisée par l'administrateur de la sécurité à l'aide d'un outil d'administration dédié (appelé "console"). Toute modification de cette politique est déployée et appliquée dynamiquement et automatiquement sur tous les postes.

La présente cible de sécurité concerne la fonction de **chiffrement complet du disque**, disponible dans le pack Secure Edition de Stormshield Endpoint Security.

1.3.2.2 Chiffrement du disque

Le chiffrement du disque permet de préserver la confidentialité des données stockées sur le disque en cas de perte ou de vol de l'ordinateur.

Quand le disque est chiffré, avant le démarrage du système proprement dit, l'utilisateur doit s'authentifier à l'aide d'un mot de passe pour pouvoir déchiffrer le disque et lancer le système d'exploitation.

L'administrateur peut choisir entre :

- Chiffrer uniquement **la partition système** : seule la partition système où le système d'exploitation est installé, est chiffrée.
- Chiffrer **toutes les partitions** : toutes les partitions du disque sur lequel Stormshield Endpoint Security est installé sont chiffrées.

Chiffrement initial

Le chiffrement initial du disque est déclenché automatiquement dès lors que la politique de sécurité stipule que le disque doit être chiffré.

L'utilisateur choisit lui-même le mot de passe qui protège le disque : ce mot de passe doit respecter le niveau de sécurité (force) défini par l'administrateur.

Le chiffrement initial s'effectue en tâche de fond et ne peut être ni arrêté ni annulé par l'utilisateur (une barre de progression indique l'avancement de l'opération). En cas d'interruption (suite par exemple à l'arrêt brutal de l'ordinateur), le processus de chiffrement reprend automatiquement.

Les secteurs non affectés peuvent être effacés de façon sécuritaire (par surcharge) avant leur chiffrement.

Une fois le chiffrement du disque terminé, la liste des partitions chiffrées est transmise au Serveur Stormshield.

L'utilisateur peut ensuite à tout moment changer son mot de passe.

Authentification unique (SSO)

L'administrateur peut activer l'authentification unique sur les postes de travail : elle consiste à mutualiser les authentifications à Stormshield Endpoint Security et à Windows.

Lorsque l'utilisateur s'authentifie pour la première fois avec son login/mot de passe Windows via le service d'authentification de SES, ses informations d'authentification sont conservées par l'agent qui assurera dès lors à chaque démarrage, sans intervention de l'utilisateur, l'authentification et l'ouverture de session Windows.

Recouvrement

Lors du chiffrement initial du disque, le serveur Stormshield génère un mot de passe de recouvrement (32 -caractères hexadécimaux) et transmet à l'agent les éléments cryptographiques permettant de démarrer le poste avec ce mot de passe de secours.

Ce mot de passe pourra être communiqué plus tard à l'utilisateur s'il oublie son mot de passe ou utilisé par un administrateur pour intervenir sur le poste.

Ce mot de passe peut être défini à usage unique par l'administrateur (One Time Password) : dans ce cas, dès qu'il est utilisé sur le poste, un nouveau mot de passe de recouvrement est automatiquement généré par le serveur et les éléments cryptographiques associés.

Si une défaillance du disque empêche le démarrage de la machine, il est toujours possible de déchiffrer le disque à l'aide d'un CD "amorçable" préparé depuis la console d'administration.

Notion d'invité

Si l'administrateur l'a autorisé, l'utilisateur peut définir un mot de passe temporaire qui permet à une autre personne (un invité) de déverrouiller et d'utiliser l'ordinateur.

Le mot de passe invité peut expirer automatiquement au bout d'une durée déterminée par la politique de sécurité, ou être invalidé à la demande de l'utilisateur.

Hibernation

Lorsque que le poste est mis en veille prolongée (hibernation), l'état du système (applications lancées, fichiers ouverts) est sauvegardé sur le disque, chiffré et donc protégé par SES .

Au redémarrage, l'utilisateur doit saisir à nouveau son mot de passe pour relancer le système.

1.3.2.3 Rôles

Il existe trois rôles mettant en œuvre les fonctionnalités du produit :

- **L'administrateur de la sécurité** (administrateur Stormshield) installe le produit, définit la politique de sécurité, gère les postes et les utilisateurs et assure le recouvrement des disques.

- **L'utilisateur** de la machine dont certaines données sont à protéger en confidentialité sur le disque de la machine. Il utilise le produit conformément à la politique de sécurité.

- L'**invité**, sous la responsabilité de l'utilisateur, utilise la machine de façon temporaire.

1.3.2.4 Schéma global de sécurité

Un disque est chiffré à l'aide d'un ensemble de secrets générés lors du chiffrement initial.

Ces secrets sont les mêmes pour toutes les partitions du disque.

Ces secrets sont eux-mêmes chiffrés avec chacun des mots de passe qui permettent de déverrouiller le disque (utilisateur, recouvrement, invité).

L'algorithme de chiffrement est AES avec une longueur de clé paramétrable : 128, 192, 256 bits.

1.3.3 Déploiement / Administration

1.3.3.1 Infrastructure d'exploitation

L'exploitation de Stormshield Endpoint Security fait intervenir les composants suivants :

- La **console d'administration** permet de définir la politique de sécurité, d'administrer les utilisateurs et de consulter les journaux (logs) remontés par les postes clients.
- La politique de sécurité est déposée sur un **serveur**, à partir duquel elle est régulièrement téléchargée par les postes clients. Ce serveur permet également de déployer une mise à jour du logiciel et réceptionne les journaux générés par les postes clients.
- La politique de sécurité et les journaux sont stockés dans **une base de données** SQL qui peut être hébergée sur une machine dédiée.
- Sur chaque poste client, l'**agent** SES applique la politique de sécurité et remonte sur le serveur les événements qu'il génère.

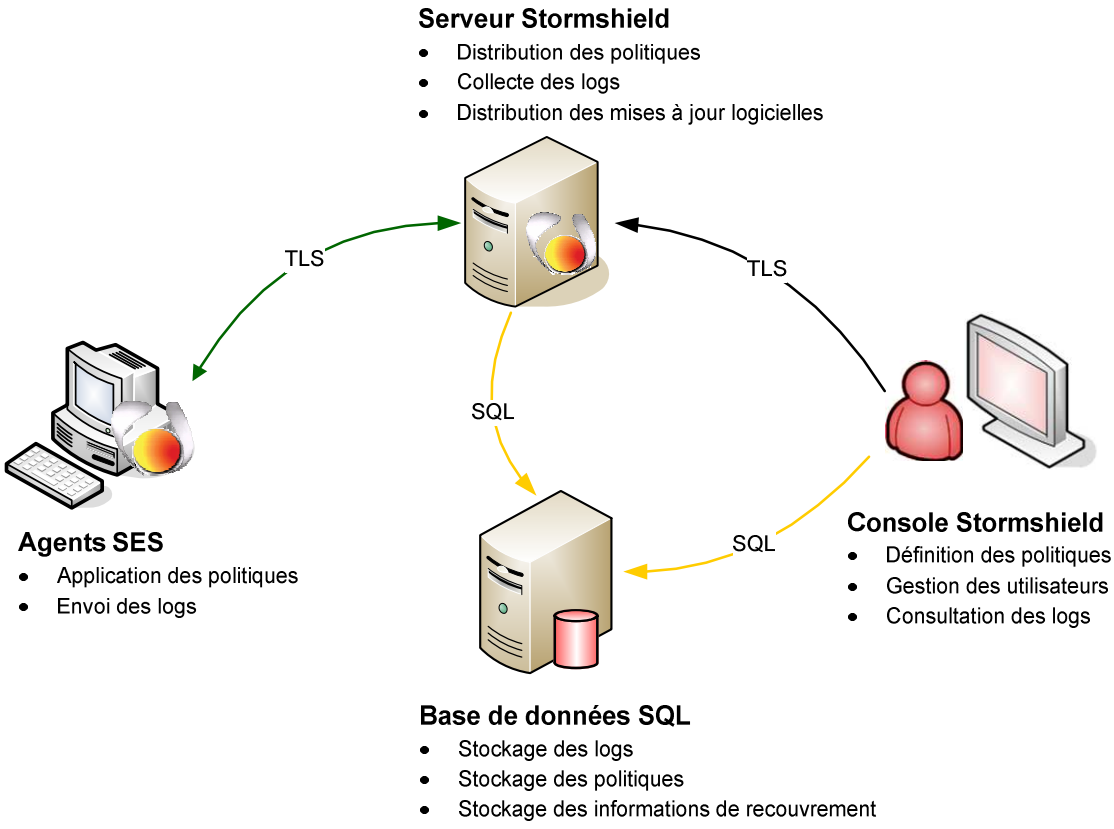

Figure 1 : Infrastructure d'exploitation

Notes :

- La console, le serveur et la base de données peuvent être installés sur la même machine.
- Afin de supporter une grande quantité de postes client, il est possible de définir un serveur principal dit primaire et de le répliquer sur des serveurs dits secondaires afin de répartir la charge de télécollecte de la politique et de dépôt des journaux.
- Les communications avec les serveurs primaires et secondaires sont sécurisées à l'aide du protocole TLS.

1.3.3.2 Déploiement

Une fois le serveur et la console installés, l'agent peut être déployé sur les postes client de plusieurs manières :

- De façon interactive depuis une interface web disponible sur le serveur Stormshield.
- De façon automatique (l'agent est installé à distance de façon transparente pour l'utilisateur) :
    - Soit à l'aide d'un assistant de déploiement Stormshield.
    - Soit à l'aide des outils standards de déploiement logiciel tel que Microsoft SCCM.

Stormshield Endpoint Security intègre également un mécanisme automatique de mise à jour de ses composants et en particulier l'agent :

- Les mises à jour (correctifs) sont mises à disposition sur le serveur.
- Les agents (et les éventuels serveurs secondaires) téléchargent et appliquent automatiquement la mise à jour logicielle.

1.3.3.3 Systèmes supportés

Le tableau suivant indique les systèmes supportés pour chaque élément d'infrastructure présenté à la section 1.3.3.1.

Serveur Stormshield	- Windows Server 2008 SP2, 32 ou 64 bits - Windows Server 2008 R2 64 bits
Base de données	- Microsoft SQL Serveur 2005 et supérieure.
Console d'administration	- Windows XP SP3 32 bits. - Windows Vista SP1, SP2, 32 ou 64 bits. - Windows 7 SP1 32 ou 64 bits. - Windows Server 2008 SP1, SP2, 32 ou 64 bits.
Agent Stormshield Endpoint Security	- Windows XP SP3 32 bits. - Windows Vista SP2 32 bits. - Windows 7 32 ou 64 bits. - Windows Server 2008 R2 64 bits

Tableau 1 : Systèmes supportés

1.3.4 Exemples de déploiement

1.3.4.1 Petite Echelle

Le schéma suivant illustre une infrastructure suffisante pour quelques centaines de postes utilisateur : le serveur Stormshield et la base de données sont hébergés sur le même serveur physique.

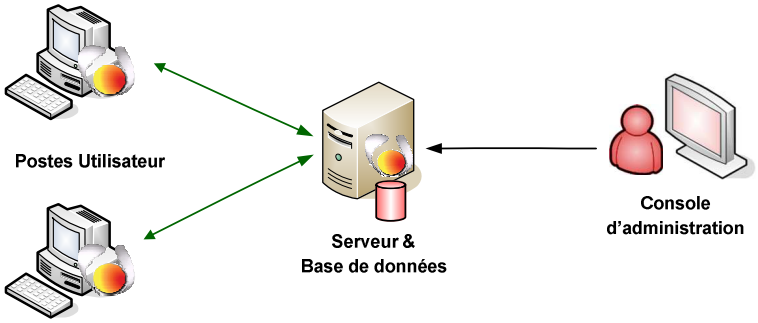

Figure 2 : Infrastructure Minimaliste

1.3.4.2 Grande Echelle

Pour gérer un grand nombre de postes utilisateur, il est nécessaire de mettre en place plusieurs serveurs afin de répartir la charge générée par les postes.

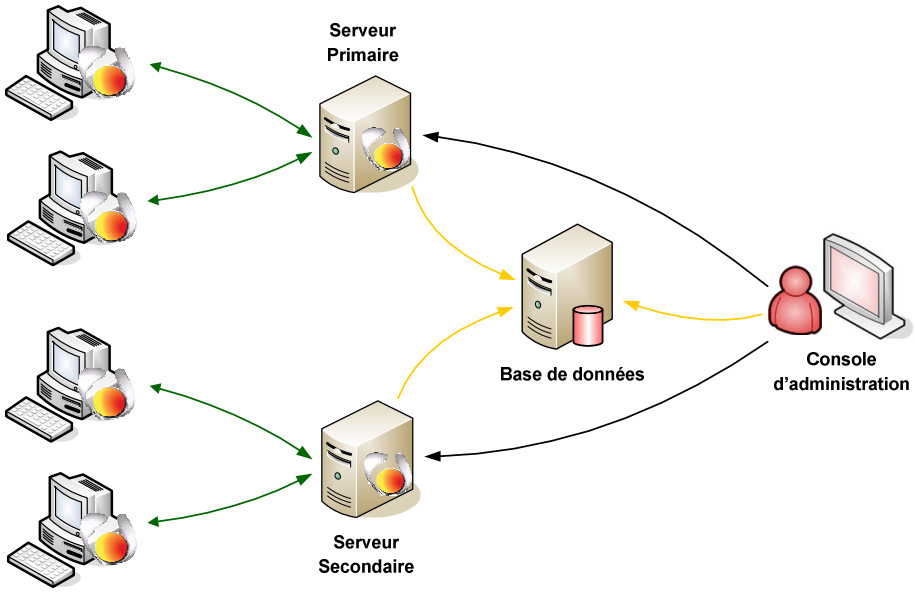

Figure 3 : Infrastructure Multi-serveurs

Les serveurs secondaires :

- reçoivent les politiques de sécurité depuis la console d'administration,
- mettent les différentes politiques à disposition des agents,
- stockent les journaux reçus dans la base de données.

Les agents se connecteront à l'un ou l'autre des serveurs selon :

- l'ordre de priorité défini par l'administrateur,
- la disponibilité et le taux d'occupation de chaque serveur.

1.4 Description de la TOE

1.4.1 Périmètre de la TOE

Le périmètre logique d'évaluation est illustré par le schéma ci-dessous.

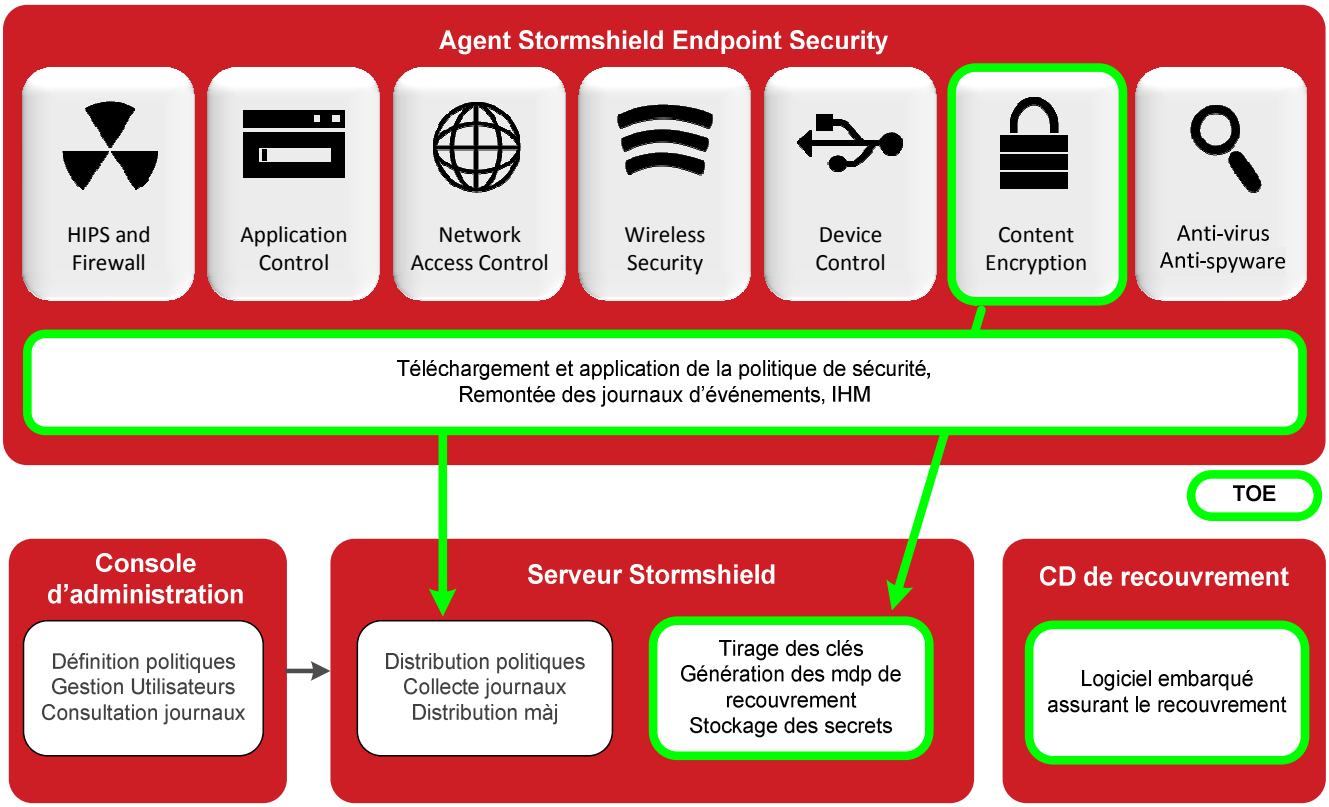

Figure 4 : Périmètre de la TOE

Ce périmètre est plus précisément constitué des composants suivants:

- Côté Client :
  - Un résident BIOS qui gère l'authentification de l'utilisateur et le lancement de Windows.
  - Un driver Windows qui assure le chiffrement/déchiffrement du disque.
  - Des services, communs à tous les modules fonctionnels de Stormshield Endpoint Security, qui assurent sous Windows :
    - L'application de la politique de sécurité et l'enregistrement des journaux.
    - Les communications sécurisées avec le serveur (téléchargement de la politique de sécurité, transmission des journaux).
    - Toutes les fonctions interactives : changement de mot de passe, consultation locale des journaux, etc.
- Coté Serveur :
  - Les modules qui fournissent les clés de chiffrements et les mots de passe de recouvrement, et qui en assurent le stockage sécurisé dans la base de données
- Le logiciel installé sur un CD de recouvrement.

Le périmètre physique est constitué des éléments logiciels correspondant aux modules logiques de la TOE.

Les éléments suivants sont hors évaluation :

- Le BIOS et le système d'exploitation Microsoft Windows.
- La base de données dans laquelle sont stockés les secrets.
- La Console d'administration.

1.4.2 Plate-forme de test pour l'évaluation de la TOE

Pour l'évaluation du produit Stormshield Enpoint Security, la plate-forme réseau minimale suivante devra être mise en place par l'évaluateur :

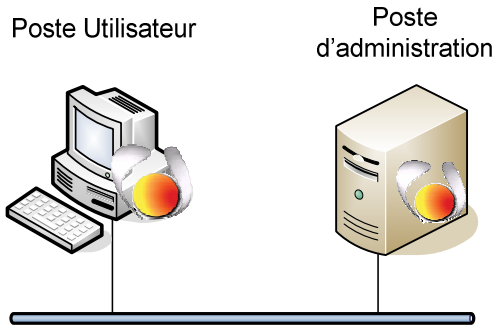

Figure 5 : Plateforme de test pour l'évaluation de la TOE

La plateforme de test utilisée pour l'évaluation est constituée des éléments logiques suivants :

- Un poste utilisateur sous Microsoft Windows XP Professionnel SP3 32 bit ou Seven Enterprise SP1 64 bits. Sur ce poste est installé l'agent Stormshield Enpoint Security version 7.2.06 build 29579.
- Un poste d'administration sous le système d'exploitation Windows Server 2008 SP2. Sur ce poste sont installés :
    - La console Stormshield Enpoint Security version 7.2.06 build 29579.
    - Le serveur Stormshield Enpoint Security version 7.2.06 build 29579.
    - Microsoft SQL Server 2005

2. DECLARATION DE CONFORMITE

2.1 Conformité aux Critères communs

Le présent document est conforme aux exigences des Critères Communs version 3.1 révision 4 [CC] :

- les exigences fonctionnelles sont issues de la partie 2 « stricte » des Critères Communs.
- les exigences d'assurance sont issues de la partie 3 « stricte » des Critères Communs.

2.2 Conformité à un profil de protection

Cette cible de sécurité est conforme au profil de protection "Application de chiffrement de données à la volée sur mémoire de masse" [CDISK].

2.3 Conformité à un paquet d'assurance

Le niveau d'assurance visé correspond au paquet **EAL3 augmenté** des composants ALC_FLR.3 et AVA_VAN.3.

3. DEFINITION DU PROBLEME DE SECURITE

3.1 Biens sensibles

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.

La description de chaque bien fournit les types de protection requis pour chacun d'eux (partie *Protection*).

3.1.1 Données utilisateur protégées par la TOE (User Data)

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).

Stormshield Enpoint Security chiffre :

- soit uniquement la partition système où le système d'exploitation de l'ordinateur est installé
- soit toutes les partitions du disque sur lequel Stormshield Enpoint Security est installé.

Les biens sensibles sont donc ici tous les dossiers et fichiers de l'utilisateur stockés sur le disque.

Stormshield Enpoint Security protège également le fichier d'hibernation du système, lequel peut contenir des données sensibles, tels que par exemple des portions de fichiers confidentiels qui étaient ouvert au moment de l'hibernation.

Protection: confidentialité.

D.CODES_SECRETS

Ces codes sont :

- le code confidentiel de l'utilisateur ;
- le mot de passe de recouvrement (ou mot de passe « administrateur ») ;
- le code confidentiel "invité" provisoire.

Ces codes permettent de récupérer les éléments cryptographiques nécessaires au chiffrement/déchiffrement des partitions.

Protection: confidentialité.

3.1.2 Données sensibles de la TOE (TSF Data)

D.POLITIQUE

Ce bien représente la politique de sécurité, c'est-à-dire les paramètres de configuration des différents composants du logiciel Stormshield Enpoint Security. Cette politique est définie depuis la console par l'administrateur de la sécurité, et est téléchargée par l'agent local Stormshield.

Protection: intégrité.

D.CLES_CHIFFREMENT_DISQUE

Ce bien représente les clés cryptographiques qui permettent de chiffrer et déchiffrer les partitions d'un disque.

Protection: confidentialité.

D.JOURNAL

Ce bien représente les événements et les alertes générés par le logiciel. Ces éléments sont régulièrement transmis et sauvegardés le serveur Stormshield.

Protection: intégrité.

3.1.3 Synthèse des biens sensibles

Le tableau ci-dessous résume la liste des biens sensibles protégés par Stormshield Endpoint Security et rappelle leurs besoins de sécurité.

Biens sensibles		Confidentialité	Intégrité
Biens sensibles de l'utilisateur	D.DONNEES_UTILISATEUR	Oui	
	D.CODES_SECRETS	Oui	
Biens sensibles de la TOE	D.POLITIQUE		Oui
	D.CLES_CHIFFREMENT_DISQUE	Oui	
	D.JOURNAL		Oui

Tableau 2 : Synthèse des biens sensibles

3.2 Utilisateurs

Les trois rôles gérés par le produit sont (voir section 1.3.2.3.) :

- **L'administrateur de la sécurité,** en charge de définir la politique de sécurité et assurer le recouvrement des disques.
- **L'utilisateur** de la machine dont certaines données sont à protéger en confidentialité sur le disque de la machine.
- L'**invité**, qui utilise la machine de façon temporaire.

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 (lesquels font l'objet de la section 3.4 Politique de sécurité de l'organisation (OSP). 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.

Les agents menaçants pour la TOE sont:

- Un **Voleur** qui subtiliserait le poste sur lequel les données confidentielles à protéger sont stockées,
- Un **Utilisateur non autorisé** qui aurait un accès physique au poste mais qui ne serait pas autorisé à accéder au contenu du disque,

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.

Le vol est perpétré alors que la machine est éteinte ou en veille prolongée (hibernation).

Les biens menacés sont les données de l'utilisateur et les biens sensibles de la TOE.

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.

T.MODIFICATION_POLITIQUE

Une personne malveillante interceptant les communications entre l'agent et le serveur Stormshield modifie la politique téléchargée.

T.MODIFICATION_JOURNAL

Une personne malveillante interceptant les communications entre l'agent et le serveur Stormshield modifie le journal transmis au serveur.

T.INTERCEPTION_CLES

Une personne malveillante interceptant les communications entre l'agent et le serveur Stormshield prend connaissance des secrets intervenant dans le chiffrement du disque.

3.4 Politique de sécurité de l’organisation (OSP)

Les politiques de sécurité organisationnelle présentes dans cette section portent uniquement sur les fonctions attendues de la TOE.

OSP.DISQUE

La TOE doit assurer la protection en confidentialité du disque d'un ordinateur conformément à la politique de sécurité définie par l’administrateur de la sécurité, ce disque ne pouvant être lu ou modifié que par un utilisateur autorisé. Cette protection est assurée lorsque l'ordinateur est éteint ou en veille prolongée.

OSP.RECOUVREMENT

La TOE doit permettre de déverrouiller un poste ou un disque en cas d'oubli du mot de passe, en l'absence de l'utilisateur légitime ou en cas d'impossibilité de démarrer le système.

OSP.REPRISE

En cas d'arrêt inopiné du processus de chiffrement initial du disque, la TOE doit automatiquement reprendre et terminer le chiffrement des données.

OSP.HIBERNATION

La TOE doit assurer la confidentialité des fichiers de mise en veille prolongée et imposer l’authentification de l’utilisateur à la sortie de la mise en veille.

OSP.JOURNALISATION

La TOE doit générer des journaux d'évènements en rapport avec son fonctionnement.

OSP.CRYPTO

Les mécanismes cryptographiques de la TOE doivent être conformes aux exigences pour le niveau de robustesse standard des référentiels cryptographiques [RGS_CRYPTO] et [RGS_CLES] de l'ANSSI.

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

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.

Plus généralement, on considère qu'il existe dans l'organisation une politique de sécurité du système d'information (PSSI) dont les exigences sont respectées par la machine hôte. Cette politique doit notamment prévoir que les logiciels installés soient régulièrement mis à jour et que le système soit protégé contre les virus et autres logiciels espions.

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.

A.ADMIN_SECURITE_CONFIANCE

L'administrateur de sécurité en charge de la définition de la politique de sécurité sur le poste ou via la console Stormshield est considéré de confiance.

A.MACHINES_ADMINSTRATION

Les machines sur lesquelles la console, le serveur Stormshield et la base de données sont installés doivent respecter les exigences suivantes :

- Ces machines sont protégées contre les virus et autres logiciels espions.
- L'accès à ces machines est restreint aux seuls administrateurs de celles-ci (administrateur système ou administrateur base de données).
- L'installation et la mise à jour de logiciels s'effectue sous le contrôle de l'administrateur.
- Les logiciels installés sont régulièrement mis à jour.

A.ADMIN_SYSTEME

Un administrateur chargé de l'environnement dans lequel la TOE est mise en œuvre est considéré de confiance.

Cet administrateur, qui n'a aucun rôle vis-à-vis de la TOE, est typiquement :

- L'administrateur système en charge de l'exploitation des machines d'administration (console, serveur, base de données) et des postes utilisateurs.
- L'administrateur de la base de données.

A.INSTALLATION_AGENT

L'installation de l'agent s'effectue sur un poste sain respectant la PSSI de l'organisme (système protégé contre les virus, logiciels régulièrement mis à jour, etc).

Au moment de l'installation de l'agent, le serveur Stormshield doit être disponible afin que l'agent puisse télécharger la politique de sécurité définie par l'administrateur.

Cette installation s'effectue sur un environnement réseau de confiance, typiquement un réseau local dûment paramétré et protégé par un pare-feu.

A.POLITIQUE

La politique de sécurité générée hors TOE par la console Stormshield est considérée de confiance pour cette évaluation.

Cette politique est déposée par la console sur le Serveur Stormshield via un lien sécurisé (TLS) permettant d'assurer l'authenticité et l'intégrité de cette politique.

4. OBJECTIFS DE SECURITE

Les objectifs de sécurité reflètent l'intention déclarée et sont à même de contrer toutes les menaces identifiées et de couvrir toutes les politiques de sécurité organisationnelles et les hypothèses identifiées.

4.1 Objectifs de sécurité pour la TOE

4.1.1 Protection des données utilisateurs

O.ARRET_UTILISATEUR

La TOE doit rendre inaccessibles les données sensibles, en particulier les clés cryptographiques, lorsque l'utilisateur éteint ou met en veille prolongée son ordinateur.

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.

En outre, en cas d'arrêt inopiné du processus de chiffrement initial du disque, la TOE doit automatiquement reprendre et terminer le chiffrement des données.

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.

O.HIBERNATION

La TOE doit assurer la confidentialité des fichiers de mise en veille prolongée et imposer l'authentification de l'utilisateur à la sortie de la mise en veille.

4.1.2 Administration

O.ROLES

La TOE doit permettre de distinguer les trois rôles administrateur, utilisateur normal et invité.

O.JOURNALISATION

La TOE doit générer des journaux d'évènements en rapport avec son fonctionnement.

O.RECOUVREMENT

La TOE doit permettre de déverrouiller un poste ou un disque en cas d'oubli du mot de passe, en l'absence de l'utilisateur légitime ou en cas d'impossibilité de démarrer le système.

La légitimité d'une demande de recouvrement doit être préalablement vérifiée par des procédures organisationnelles.

O.COMMUNICATIONS

La TOE doit assurer la protection des communications entre l'agent et le Serveur Stormshield.

Cette protection consiste en :

- L'authentification mutuelle entre l'agent et le serveur
- La confidentialité et l'intégrité des biens sensibles échangés.

O.APPLICATION_POLITIQUE

La TOE doit appliquer la politique de sécurité définie par l'administrateur de la sécurité.

Si l'administrateur l'a autorisé, l'utilisateur peut éventuellement reporter le chiffrement de son disque en cas de nécessité opérationnelle, mais il ne peut en aucun cas refuser ou désactiver plus tard ce chiffrement.

4.1.3 Cryptographie

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 [RGS_CRYPTO] et [RGS_CLES] de l'ANSSI.

O.CLES_CHIFFREMENT

La TOE doit générer des clés de chiffrement conformément aux exigences pour le niveau de robustesse standard des référentiels cryptographiques [RGS_CRYPTO] et [RGS_CLES] de l'ANSSI.

4.2 Objectifs de sécurité pour l'environnement opérationnel de la TOE

4.2.1 Environnement physique de la TOE

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 Administration

OE.ADMIN_SECURITE_CONFIANCE

L'administrateur de sécurité en charge de la définition de la politique de sécurité est considéré de confiance.

OE.MACHINES_ADMINSTRATION

Les machines sur lesquelles la console, le serveur Stormshield et la base de données sont installés doivent respecter les exigences suivantes :

- Ces machines sont protégées contre les virus et autres logiciels espions.
- L'accès aux fonctions d'administration de ces machines est restreint aux seuls administrateurs système.
- L'installation et la mise à jour de logiciels s'effectue sous le contrôle de l'administrateur.
- Les logiciels installés sont régulièrement mis à jour.

OE.ADMIN_SYSTEME

Un administrateur chargé de l'environnement dans lequel la TOE est mise en œuvre est considéré de confiance.

Cet administrateur, qui n'a aucun rôle vis-à-vis de la TOE, est typiquement :

- L'administrateur système en charge de l'exploitation des machines d'administration (console, serveur, base de données) et des postes utilisateurs.
- L'administrateur de la base de données est également.

OE.INSTALLATION_AGENT

L'installation de l'agent s'effectue sur un poste sain respectant la PSSI de l'organisme (système protégé contre les virus, logiciels régulièrement mis à jour, etc).

Au moment de l'installation de l'agent, le serveur Stormshield doit être disponible afin que l'agent puisse télécharger la politique de sécurité définie par l'administrateur.

Cette installation s'effectue sur un environnement réseau de confiance, typiquement un réseau local dûment paramétré et protégé par un pare-feu.

OE.POLITIQUE

La politique de sécurité est générée hors TOE par la console Stormshield.

Cette politique est considérée de confiance : elle est définie par un administrateur habilité puis déposée sur le Serveur Stormshield via un lien sécurisé (TLS) permettant d'assurer l'authenticité et l'intégrité de cette politique.

5. EXIGENCES DE SECURITE

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 [CC Part1]) : 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 6.

Sujets

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

Sujet	Attribut de sécurité	Valeurs possibles
S.API	Type d'utilisateur authentifié (AT.ROLE)	USER / ADMIN / GUEST
S.DISK	Statut du disque (AT.STATUS)	ACTIVATED / DEACTIVATED
S.DISK	Identifiant Disque (AT.ID)	Identification propriétaire

Tableau 3 : Liste des sujets

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 de la cible de sécurité, 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)	Identification propriétaire
Données utilisateur chiffrées (OB.UD)	Identifiant disque associé (AT.ID)	Identification propriétaire
Données d'Authentification (OB.AD)	Identifiant disque associé (AT.ID)	Identification propriétaire

Données d'Authentification (OB.AD)	Rôle associé (AT.ROLE)	USER / ADMIN / GUEST
Données d'Authentification (OB.AD)	Mot de passe (AT.PASSWORD)	Mot de passe
Politique de Sécurité (Policy)		

Tableau 4 : Liste des objets

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.

La politique de sécurité (Policy) contient tous les paramètres de fonctionnement de la TOE.

Opérations

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

Opération	Sujet	Valeurs possibles
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
Renouvellement du mot de passe de recouvrement (CHANGE_PASSWORD_SO)	TSF	OB.AD
Invitation (INVITE)	S.API	OB.AD
Changement du mot de passe (CHANGE_PASSWORD)	S.API	OB.AD

Tableau 5 : Liste des opérations

CREATE correspond intuitivement à la création d'un disque: une clé de chiffrement y est implicitement associée.

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 déverrouillant le disque et permettant toute opération sur les données de l'utilisateur (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 œuvre 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 œuvre 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.

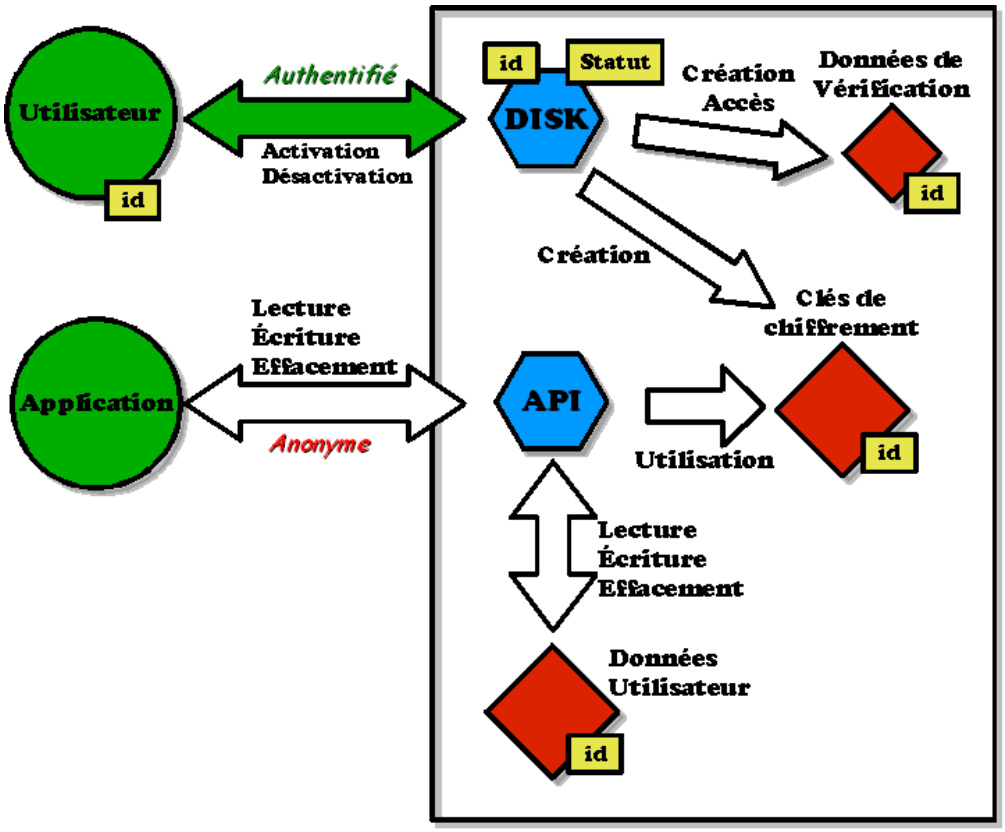

Figure 6 : Résumé de la TSP

Utilisateurs

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

U.Admin représente un administrateur du produit

U.Guest représente un invité susceptible de travailler sur le poste de l'utilisateur.

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 Synthèse des exigences fonctionnelles

Authentification des utilisateurs

FIA_UID.1 Timing of identification

FIA_UAU.1 Timing of authentication

Journalisation

FAU_GEN.1 Audit data generation

FAU_GEN.2 User identity association

Robustesse

FPT_FLS.1 Failure with preservation of secure state

Administration

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security management roles

FMT_SAE.1 Time-limited authorisation

FPT_ITT.1 Basic internal TSF data transfer protection

FDP_ACC.1/Policy Subset access control

FDP_ACF.1/Policy Security attribute based access control

Contrôle d'accès

FMT_MSA.3 Static attribute initialization

FMT_MSA.1/Disk_Status Management of security attributes

FMT_MSA.1/ID Management of security attributes

FMT_MSA.1/Password_SO Management of security attributes

FMT_MSA.1/Password_User Management of security attributes

FMT_MSA.1/New_Password_Guest Management of security attributes

FMT_MSA.1/Del_Password_Guest Management of security attributes

FDP_ACC.1/Disk Subset access control

FDP_ACF.1/Disk Security attribute based access control

Cryptographie

FCS_COP.1 Cryptographic operation

FDP_RIP.1 Subset residual information protection

FCS_CKM.1 Cryptographic key generation

5.1.2 Détail des exigences fonctionnelles

5.1.2.1 Exigences liées à l'authentification des utilisateurs

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- **CREATE**

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**, **DISMOUNT, USE, DECIPHER, CIPHER, ERASE, CHANGE_PASSWORD, CHANGE_PASSWORD_SO, INVITE,** and **ACCESS**.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

- **CREATE**

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, **DISMOUNT, USE, DECIPHER, CIPHER, ERASE, CHANGE_PASSWORD, CHANGE_PASSWORD_SO, INVITE** and ACCESS.

The authentication mechanism must meet the ANSSI's requirements [RGS_AUTH].

Note d'application

L'authentification des utilisateurs se fait par une phrase de passe.

5.1.2.2 Exigences liées à la journalisation

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events for the **not specified** level of audit; and

c)
- **New policy download**
- **Disk encryption and decryption**
- **Authentication: user / recovery / guest , success / failure**
- **Guest management: invitation, cancellation**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **none**.

FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.2.3 Exigence liée à la robustesse

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)**
- **when the disk encryption or decryption operation is interrupted, whatever the reason (power cut, system or application crash**).

5.1.2.4 Exigence liée à l'administration

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1 The TSF shall be capable of performing the following management functions:

- **Application of security policy downloaded from Stormshield Server**
- **password management**
- **recovery function**

FMT_SMR.1 Security management roles

FMT_SMR.1.1 The TSF shall maintain the roles **U.USER, U.ADMIN, U.GUEST**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

FMT_SAE.1 Time-limited autorisation

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [**OB.AD with OB.AD.ROLE=GUEST**] to **U.Admin**.

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to **disable the OB.AD concerned** after the expiration time for the indicated security attribute has passed.

Raffinement non éditorial : concerne le mot de passe « invité ».

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from **disclosure, modification** when it is transmitted between separate parts of the TOE.

Raffinement non editorial : concerne la protection en confidentialité et intégrité des communications entre l'agent et le serveur.

FDP_ACC.1/Policy Subset access control

FDP_ACC.1.1/Policy The TSF shall enforce the **access control** on **TOE access control policy**.

Raffinement non éditorial : concerne la protection locale de la politique de sécurité téléchargée.

FDP_ACF.1/Policy Security attribute based access control

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

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

- **The TOE access control policy can only be updated by the TSF.**
- **The update comes from a policy securely downloaded from Stormshield Server.**

FDP_ACF.1.3/Policy The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/Policy The TSF shall explicitly deny access of subjects to objects based on: **none**.

Raffinement non éditorial : concerne la mise à jour et la protection locale de la politique de sécurité téléchargée.

5.1.2.5 Exigences liées au contrôle d'accès

FMT_MSA.3 Static attribute initialization

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 est déterminée par une méthode propriétaire.

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.

FMT_MSA.1/Password_SO Management of security attributes

FMT_MSA.1.1/Password_SO The TSF shall enforce the **TOE access control policy** to restrict the ability to **modify** the security attributes **OB.AD.PASSWORD where OB.AD.ROLE=Admin** to **the TSF itself**.

Note d'application

Seule la TSF peut modifier le mot de passe de recouvrement.

FMT_MSA.1/Password_User Management of security attributes

FMT_MSA.1.1/Password_User The TSF shall enforce the **TOE access control policy** to restrict the ability to **modify** the security attributes **OB.AD.PASSWORD where OB.AD.ROLE=User** to **U.USER and U.ADMIN**.

Note d'application

Seuls l'utilisateur du poste et l'administrateur peuvent modifier le mot de passe utilisateur.

FMT_MSA.1/New_Password_Guest Management of security attributes

FMT_MSA.1.1/New_Password_Guest The TSF shall enforce the **TOE access control policy** to restrict the ability to **create** the security attributes **OB.AD.PASSWORD with OB.AD.ROLE=GUEST** to **U.USER and U.ADMIN**.

Note d'application

Seuls l'utilisateur du poste et l'administrateur peuvent créer un mot de passe invité.

FMT_MSA.1/Del_Password_Guest Management of security attributes

FMT_MSA.1.1/Del_Password_Guest The TSF shall enforce the **TOE access control policy** to restrict the ability to **delete** the security attributes **OB.AD.PASSWORD with OB.AD.ROLE=GUEST** to **U.USER, U.ADMIN and the TSF itself**.

Note d'application

Seuls l'utilisateur du poste, l'administrateur et la TSF peuvent supprimer un mot de passe invité.

FDP_ACC.1/Disk Subset access control

FDP_ACC.1.1/Disk 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, CHANGE_PASSWORD, CHANGE_PASSWORD_SO, INVITE**

FDP_ACF.1/Disk Security attribute based access control

FDP_ACF.1.1/Disk 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)** **AT.ROLE (for S.API)**
Objects	**S.DISK, OB.KEY, OB.UD, OB.AD**	**AT.ID, AT.ROLE and AT.PASSWORD**

FDP_ACF.1.2/Disk 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 condition**
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**
Rule7	**The TSF is allowed to change the recovery password**	**The user is authenticated by the TSF based on OB.AD and the values of the security attributes AT.ROLE is ADMIN**
Rule8	**a subject S.API is allowed to INVITE a guest, which consists in creating an associated OB.AD**	**The user is authenticated by the TSF based on OB.AD and the values of the security attribute AT.ROLE is USER or ADMIN**
Rule9	**a subject S.API is allowed to CHANGE_PASSWORD, which consists in changing the attribute AD.PASSWORD of the object OD.AD where AD.ROLE=USER**	**The user is authenticated by the TSF based on OB.AD and the values of the security attribute AT.ROLE is USER or ADMIN**

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

- **Rule10: The TSF shall perform DISMOUNT operation on S.DISK after shut down, restart, hibernate, provided the value of the security attribute S.DISK.STATUS is ACTIVATED.**
- **None.**

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

- **None.**

Note d'application

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

5.1.2.6 Exigences liées à la cryptographie

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **hash, key derivation, key wrapping and unwrapping, encryption and decryption** in accordance with a specified cryptographic algorithm **SHA-256 and AES** and cryptographic key sizes **128, 192, 256 bits** that meet the following: **ANSSI's cryptographic requirements ([RGS_CRYPTO] and [RGS_CLES]).**

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.

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 **based on SHA-256 and AES** and specified cryptographic key sizes **128, 192, 256 bits** that meet the following: **ANSSI's cryptographic requirements ([RGS_CRYPTO] and [RGS_CLES])**.

5.2 Exigences d'assurance pour la TOE

Le niveau visé est **EAL3 augmenté** des composants ALC_FLR.3 et AVA_VAN.3

ADV : Development

ADV_ARC.1: Security architecture description

ADV_FSP.3: Functional specification with complete summary

ADV_TDS.2: Architectural design

AGD : Guidance documents

AGD_OPE.1: Operational user guidance

AGD_PRE.1: Preparative procedures

ALC : Life-cycle support

ALC_CMC.3: Authorisation controls

ALC_CMS.3: Implementation representation CM coverage

ALC_DEL.1: Delivery procedures

ALC_DVS.1: Identification of security measures

ALC_FLR.3: Systematic flaw remediation

ALC_LCD.1: Developer defined life-cycle model

ASE : Security Target evaluation

ASE_CCL.1 Conformance claims

ASE_ECD.1 Extended components definition

ASE_INT.1 ST introduction

ASE_OBJ.2 Security objectives

ASE_REQ.2 Derived security requirements

ASE_SPD.1 Security problem definition

ASE_TSS.1 TOE summary specification

ATE : Tests

ATE_COV.2: Analysis of coverage

ATE_DPT.1: Testing: basic design

ATE_FUN.1: Functional testing

ATE_IND.2: Independent testing - sample

AVA : Vulnerability assessment

AVA_VAN.3: Focused vulnerability analysis

6. RESUME DES SPECIFICATIONS DE LA TOE

6.1 Authentification des utilisateurs

FIA_UID.1 Timing of identification

Le chiffrement initial du disque est déclenché après que l'utilisateur ait lui-même choisit le mot de passe qui protège le disque.

Une fois le disque chiffré, pour démarrer le système, l'opérateur doit sélectionner le rôle sous lequel il va s'authentifier : utilisateur, administrateur, ou invité.

FIA_UAU.1 Timing of authentication

Pour chaque rôle, l'opérateur doit s'authentifier à l'aide d'un mot de passe.

Une fois l'utilisateur authentifié, la TOE contrôle l'accès à ses fonctions selon les principes spécifiés ci-après à la fonction **FDP_ACF.1/Disk**.

6.2 Journalisation

FAU_GEN.1 Audit data generation

La TOE enregistre les événements suivants :

- Lancement et arrêt de l'agent.
- Téléchargement / Application d'une nouvelle politique.
- Chiffrement / Déchiffrement d'un disque.
- Authentification réussie ou en échec, en mode utilisateur, administrateur ou invité.
- Création / Annulation d'un mot de passe invité.

Les événements sont enregistrés dans un journal local et sont transmis au serveur Stormshield.

FAU_GEN.2 User identity association

Les événements de la TOE relatifs à une action d'un utilisateur authentifié sont enregistrés avec le rôle de l'utilisateur (utilisateur, administrateur, invité).

6.3 Robustesse

FPT_FLS.1 Failure with preservation of secure state

Après l'arrêt intempestif (coupure de courant) ou volontaire du poste (y compris l'hibernation), les données sensibles stockées en mémoire ou sur le disque sont inaccessibles.

En outre, si l'arrêt intervient lors d'une opération de chiffrement ou du déchiffrement du disque, alors l'opération reprend automatiquement et se termine au redémarrage suivant, sans perte de données.

6.4 Administration

FMT_SMF.1 Specification of Management Functions

La TOE applique la politique de sécurité téléchargée depuis le serveur Stormshield.

La TOE offre également une IHM permettant de définir et de changer les mots de passe de l'utilisateur standard et de l'invité, et gère de façon transparente et automatique la définition et le renouvellement du mot de passe administrateur.

La TOE offre enfin une fonction de recouvrement permettant à un administrateur de déverrouiller et monter un disque soit à l'aide d'un mot de passe dédié, soit à l'aide d'un CD d'amorçage.

FMT_SMR.1 Security management roles

La TOE supporte les trois rôles : utilisateur du poste, administrateur de la sécurité et invité, gère leurs actions et permissions respectives.

FMT_SAE.1 Time-limited authorisation

Une durée de validité du mot de passe invité peut être définie par l'administrateur de la sécurité via la politique de sécurité.

Quand un utilisateur crée un mot de passe invité, ce mot de passe est automatiquement invalidé une fois passée cette durée de validité.

FDP_ITT.1 Basic internal TSF data transfer protection

La TOE assure la protection des communications entre l'agent et le Serveur Stormshield (authentification mutuelle, intégrité et confidentialité des biens sensibles transmis).

FDP_ACC.1/Policy Subset information flow control

La TOE protège contre toute modification illicite la politique stockée en local.

FDP_ACF.1/Policy Subset information flow control

La politique de sécurité appliquée ne peut être modifiée que via le serveur StomShield.

6.5 Contrôle d'accès

FMT_MSA.3 Static attribute initialization

La TOE assure :

- l'initialisation des secrets intervenant dans le schéma de chiffrement des partitions,
- l'association et la protection de ces secrets avec les données d'authentification des différents rôles (utilisateur, administrateur, invité).

FMT_MSA.1/Disk_Status Management of security attributes

Seule la TSF peut déverrouiller un disque et monter les partitions qu'il héberge.

FMT_MSA.1/ID Management of security attributes

Seule la TSF manipule les attributs de sécurité d'un disque (secrets et données d'authentification).

FMT_MSA.1/Password_SO Management of security attributes

Seule la TSF peut modifier le mot de passe de recouvrement.

FMT_MSA.1/Password_User Management of security attributes

Seuls l'utilisateur du poste et l'administrateur peuvent modifier le mot de passe utilisateur.

FMT_MSA.1/New_Password_Guest Management of security attributes

Seuls l'utilisateur du poste et l'administrateur peuvent créer un mot de passe invité.

FMT_MSA.1/Del_Password_Guest Management of security attributes

Seuls l'utilisateur du poste, l'administrateur et la TSF peuvent supprimer un mot de passe invité.

FDP_ACC.1/Disk Subset access control

La TOE met en œuvre un système de contrôle d'accès aux objets et aux opérations qu'elle gère.

FDP_ACF.1/Disk Security attribute based access control

La TSF interdit l'accès aux données d'un disque chiffré tant que ce disque n'a pas été déverrouillé par l'authentification d'un opérateur autorisé.

Une fois l'opérateur authentifié, le disque est déverrouillé et peut être utilisé en lecture/écriture sans distinction entre les différents rôles.

La TOE contrôle l'accès aux fonctions gérant les attributs de sécurité selon les autorisations spécifiées dans le tableau suivant :

Fonction	Rôle		
	Utilisateur	Admin.	Invité
Changement du mot de passe utilisateur	●	●	
Changement du mot de passe administrateur		●	
Création/Annulation d'un mot de passe invité	●	●	
Changement du mot de passe invité	●	●	●

En outre, en cas d'arrêt, de redémarrage ou de mise en veille prolongée, le TSF démonte automatiquement le disque et rend ainsi impossible l'accès aux données qu'il contient.

6.6 Cryptographie

FCS_COP.1 Cryptographic operation

La TOE implémente les opérations cryptographiques nécessaires à son fonctionnement :

- Chiffrement et déchiffrement des partitions.
- Chiffrement et déchiffrement des secrets intervenant dans le chiffrement des partitions.
- Dérivation de clé à partir d'un mot de passe.

FDP_RIP.1 Subset residual information protection

Lors du démontage d'un disque (suite à l'arrêt, au redémarrage ou à une mise en veille prolongée du poste), les données sensibles de la TOE et de l'utilisateur sont irrémédiablement effacées de la mémoire de la machine.

FCS_CKM.1 Cryptographic key generation

Lors du chiffrement initial d'un disque, la TOE génère (sur le serveur Stormshield) un ensemble de secrets à partir desquels la clé de chiffrement du disque est déterminée.

Pour chaque rôle, ces secrets sont eux-mêmes chiffrés à l'aide d'une clé dérivée à partir du mot de passe associé au rôle.

7. ARGUMENTAIRES

7.1 Objectifs de sécurité / problème de sécurité

7.1.1 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.

Aussi, O.HIBERNATION garantit que les données sauvegardées dans le fichier d'hibernation sont chiffrées.

Enfin, O.CRYPTO garantit que les fonctions de cryptographie mises en œuvre 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.

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 l'ANSSI, 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.

La qualité de la gestion des clés est garantie par **O.CRYPTO**.

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.

T.MODIFICATION_POLITIQUE

Cette menace est couverte par les objectifs

- O.COMMUNICATIONS qui garantit l'intégrité des biens échangés entre l'agent et le serveur Stormshield.
- O.JOURNALISATION qui enregistre toute opération.

T.MODIFICATION_JOURNAL

Cette menace est couverte par les objectifs

- O.COMMUNICATIONS qui garantit l'intégrité des biens échangés entre l'agent et le serveur Stormshield.
- O.JOURNALISATION qui enregistre toute opération.

T.INTERCEPTION_CLES

Cette menace est couverte par les objectifs

- O.COMMUNICATIONS qui garantit l'intégrité et la confidentialité des biens échangés entre l'agent et le serveur Stormshield.
- O.JOURNALISATION qui enregistre toute opération.

7.1.2 Politiques de sécurité organisationnelles (OSP)

OSP.DISQUE

Cette OSP est couverte par les objectifs :

- O.APPLICATION_POLITIQUE qui assure l'application de la politique de sécurité définie par l'administrateur de la sécurité
- O.PROTECTION_DES_DONNEES_ENREGISTREES qui assure que l'utilisateur a bien été authentifié avant de rendre accessibles les données enregistrées
- O.CRYPTO et O.CLES_CHIFFREMENT qui garantissent l'utilisation de clés et d'algorithmes conformes au niveau de qualification visé.

OSP.RECOUVREMENT

Cette OSP est couverte par les objectifs :

- O.PROTECTION_DES_DONNEES_ENREGISTREES qui assure que l'utilisateur a bien été authentifié avant de rendre accessibles les données enregistrées.
- O.ROLES qui permet de différencier le rôle Administrateur.
- O.RECOUVREMENT qui gère le déverrouillage du disque par l'administrateur dûment authentifié.
- O.JOURNALISATION qui enregistre l'opération.

OSP.HIBERNATION

Cette OSP est couverte par les objectifs :

- O.HIBERNATION qui assure la confidentialité des fichiers de mise en veille prolongée et impose l'authentification de l'utilisateur à la sortie de la mise en veille.
- O.CRYPTO qui implémente les fonctions de cryptographie.

OSP.REPRISE

Cette OSP est couverte par les objectifs :

- O.ROBUSTESSE qui assure la reprise d'une opération de chiffrement en cas d'arrêt inopiné.
- O.JOURNALISATION qui enregistre la reprise.

OSP.JOURNALISATION

Cette OSP est directement couverte par l'objectif O.JOURNALISATION qui assure l'enregistrement et la centralisation de tous les événements générés par la TOE.

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 ».

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.

7.1.3 Hypothèses

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. Ils 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.

A.ADMIN_SECURITE_CONFIANCE

Cette hypothèse est directement couverte par OE.ADMIN_SECURITE_CONFIANCE qui garantit que l'administrateur en charge de la définition de la politique de sécurité est de confiance.

A.MACHINES_ADMINSTRATION

Cette hypothèse est directement couverte par OE.MACHINES_ADMINSTRATION qui définit les exigences applicables aux machines d'administration.

A.ADMIN_SYSTEME

Cette hypothèse est directement couverte par OE.ADMIN_SYSTEME qui stipule qu'un administrateur chargé de l'environnement dans lequel la TOE est mise en œuvre est de confiance.

A.INSTALLATION_AGENT

Cette hypothèse est directement couverte par OE.INSTALLATION_AGENT qui définit l'environnement dans lequel l'installation de l'agent doit s'effectuer.

A.POLITIQUE

Cette hypothèse est directement couverte par OE.POLITIQUE qui garantit l'intégrité et l'authenticité de la politique de sécurité générée hors TOE.

7.1.4 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.HIBERNATION, O.CRYPTO, O.CLES_CHIFFREMENT, O.ARRET_UTILISATEUR	Section 7.1.1
T.ACCES_MEMOIRES	O.ARRET_UTILISATEUR	Section 7.1.1
T.MODIFICATION_POLITIQUE	O.COMMUNICATIONS O.JOURNALISATION	Section 7.1.1
T.MODIFICATION_JOURNAL	O.COMMUNICATIONS O.JOURNALISATION	Section 7.1.1
T.INTERCEPTION_CLES	O.COMMUNICATIONS O.JOURNALISATION	Section 7.1.1

Tableau 6 : Association menaces vers objectifs de sécurité

Objectifs de sécurité	Menaces
O.ARRET_UTILISATEUR	T.ACCES_DONNEES, T.ACCES_MEMOIRES
O.PROTECTION_DES_DONNEES_ENREGISTREES	T.ACCES_DONNEES
O.ROBUSTESSE	T.ACCES_DONNEES
O.HIBERNATION	T.ACCES_DONNEES
O.ROLES	
O.JOURNALISATION	
O.RECOUVREMENT	
O.COMMUNICATIONS	T.MODIFICATION_POLITIQUE T.MODIFICATION_JOURNAL T.INTERCEPTION_CLES
O.APPLICATION_POLITIQUE	
O.CRYPTO	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	
OE.ADMIN_SECURITE_CONFIANCE	
OE.MACHINES_ADMINSTRATION	
OE.ADMIN_SYSTEME	
OE.INSTALLATION_AGENT	
OE.POLITIQUE	

Tableau 7 : Association objectifs de sécurité vers menaces

Politiques de sécurité organisationnelles (OSP)	Objectifs de sécurité	Argumentaire
OSP.DISQUE	O.APPLICATION_POLITIQUE O.PROTECTION_DES_DONNEES_ENREGISTREES O.CRYPTO, O.CLES_CHIFFREMENT	Section 7.1.2
OSP.RECOUVREMENT	O.PROTECTION_DES_DONNEES_ENREGISTREES O.ROLES, O.JOURNALISATION O.RECOUVREMENT	Section 7.1.2
OSP.REPRISE	O.ROBUSTESSE, O.JOURNALISATION	Section 7.1.2
OSP.HIBERNATION	O.HIBERNATION, O.CRYPTO	Section 7.1.2
OSP.JOURNALISATION	O.JOURNALISATION	Section 7.1.2
OSP.CRYPTO	O.CRYPTO, O.CLES_CHIFFREMENT	Section 7.1.2
OSP.NON_REMANENCE_2	OE.NON_REMANENCE_2	Section 7.1.2

Tableau 8 : Association politiques de sécurité organisationnelles vers objectifs de sécurité

Objectifs de sécurité	Politiques de sécurité organisationnelles (OSP)
O.ARRET_UTILISATEUR	
O.PROTECTION_DES_DONNEES_ENREGISTREES	OSP.DISQUE OSP.RECOUVREMENT
O.ROBUSTESSE	OSP.REPRISE
O.ROLES	OSP.RECOUVREMENT
O.JOURNALISATION	OSP.RECOUVREMENT OSP.REPRISE OSP.JOURNALISATION
O.RECOUVREMENT	OSP.RECOUVREMENT
O.HIBERNATION	OSP.HIBERNATION
O.COMMUNICATIONS	
O.APPLICATION_POLITIQUE	OSP.DISQUE
O.CRYPTO	OSP.DISQUE OSP.HIBERNATION OSP.CRYPTO
O.CLES_CHIFFREMENT	OSP.DISQUE OSP.CRYPTO
OE.ENV_OPERATIONNEL.1	
OE.ENV_OPERATIONNEL.2	
OE.NON_REMANENCE_1	
OE.NON_REMANENCE_2	OSP.NON_REMANENCE_2
OE.ADMIN_SECURITE_CONFIANCE	
OE.MACHINES_ADMINSTRATION	
OE.ADMIN_SYSTEME	
OE.INSTALLATION_AGENT	
OE.POLITIQUE	

Tableau 9 : Association objectifs de sécurité vers politiques de sécurité organisationnelles

Hypothèses	Objectifs de sécurité pour l'environnement opérationnel	Argumentaire
A.ENV_OPERATIONNEL	OE.ENV_OPERATIONNEL.1, OE.ENV_OPERATIONNEL.2	Section 7.1.3
A.NON_REMANENCE_1	OE.NON_REMANENCE_1	Section 7.1.3
A.ADMIN_SECURITE_CONFIANCE	OE.ADMIN_SECURITE_CONFIANCE	Section 7.1.3
A.MACHINES_ADMINSTRATION	OE.MACHINES_ADMINSTRATION	Section 7.1.3
A.ADMIN_SYSTEME	OE.ADMIN_SYSTEME	Section 7.1.3
A.INSTALLATION_AGENT	OE.INSTALLATION_AGENT	Section 7.1.3
A.POLITIQUE	OE.POLITIQUE	Section 7.1.3

Tableau 10 : Association hypothèses vers objectifs de sécurité pour l'environnement opérationnel

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.ADMIN_SECURITE_CONFIANCE	A.ADMIN_SECURITE_CONFIANCE
OE.POLITIQUE	A.POLITIQUE

Tableau 11 : Association objectifs de sécurité pour l'environnement opérationnel vers hypothèses

7.2 Exigences de sécurité / objectifs de sécurité

7.2.1 Objectifs

O.ARRET_UTILISATEUR

Cet objectif est couvert par les exigences définissant la politique de contrôle d'accès FDP_ACC.1/Disk, FDP_ACF.1/Disk 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.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/Disk et FDP_ACF.1/Disk) 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). L'éventuel accès autorisé à un invité peut-être limité dans le temps (FMT_SAE.1).

Toute authentification réussie ou en échec est journalisée (FAU_GEN.1 et FAU_GEN.2).

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, FMT_MSA.1/ID, FMT_MSA.1/Password_SO, FMT_MSA.1/Password_User, FMT_MSA.1/New_Password_Guest, FMT_MSA.1/Del_Password_Guest).

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/Disk), 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.

Toute reprise suite à l'arrêt intempestif d'une opération de chiffrement ou de déchiffrement est journalisée.

O.HIBERNATION

Cet objectif est couvert par FCS_COP.1 qui implémente le chiffrement du fichier hibernation.

Au réveil, l'accès aux données est protégé par le contrôle d'accès implémenté par FDP_ACC.1/Disk et FDP_ACF.1/Disk.

O.ROLES

La TOE distingue et gère trois rôles différents (FMT_SMR.1) : utilisateur, administrateur, invité.

Le rôle est déterminé lors de l'identification de l'opérateur (FIA_UID.1). Il est ensuite contrôlé lors de l'accès aux objets protégés par la TOE (FDP_ACC.1/Disk et FDP_ACF.1/Disk).

La TOE permet de modifier les mots de passe associés à chaque rôle (FMT_SMF.1).

O.JOURNALISATION

Cet objectif est couvert par (FAU_GEN.1) qui assure la journalisation des évènements et par (FAU_GEN.2) qui associe le type d'utilisateur (son rôle) à chaque évènement inscrit dans le journal.

O.RECOUVREMENT

La TOE offre une fonction de recouvrement (FMT_SMF.1) accessible uniquement à l'administrateur (FMT_SMR.1).

Toute opération de recouvrement est journalisée (FAU_GEN.1 et FAU_GEN.2)

O.COMMUNICATIONS

La TOE protège en intégrité et confidentialité les échanges entre l'agent et le serveur Stormshield (FPT_ITT.1).

Toute communication réussie ou en échec est journalisée (FAU_GEN.1 et FAU_GEN.2).

O.APPLICATION_POLITIQUE

La TOE applique la politique de sécurité téléchargée sur le serveur Stormshield (FMT_SMF.1).

La politique sauvegardée sur le poste client est protégée de toute modification illicite (FDP_ACC.1/Policy et FDP_ACF.1/Policy**.**

Toute application d'une nouvelle politique est journalisée (FAU_GEN.1 et FAU_GEN.2).

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.CLES_CHIFFREMENT

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

7.2.2 Tables de couverture entre objectifs et exigences de sécurité

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.ARRET_UTILISATEUR	FDP_ACC.1/Disk, FDP_ACF.1/Disk, FDP_RIP.1	Section 7.2.1
O.PROTECTION_DES_DONNEES_ENREGISTREES	FDP_ACF.1/Disk, FIA_UID.1, FIA_UAU.1, FMT_MSA.3, FMT_MSA.1/Disk_Status, FMT_MSA.1/ID, FDP_ACC.1 FAU_GEN.1, FAU_GEN.2 FMT_SAE.1 FMT_MSA.1/Password_SO, FMT_MSA.1/Password_User, FMT_MSA.1/New_Password_ Guest, FMT_MSA.1/Del_Password_ Guest	Section 7.2.1
O.ROBUSTESSE	FPT_FLS.1, FDP_ACF.1/Disk FAU_GEN.1, FAU_GEN.2	Section 7.2.1
O.HIBERNATION	FCS-COP.1 FDP_ACC.1/Disk FDP_ACF.1/Disk	Section 7.2.1
O.ROLE	FMT_SMR.1, FIA_UID.1, FDP_ACC.1/Disk , FDP_ACF.1/Disk, FMT_SMF.1	Section 7.2.1
O.JOURNALISATION	FAU_GEN.1, FAU_GEN.2	Section 7.2.1
O.RECOUVREMENT	FMT_SMF.1, FMT_SMR.1, FAU_GEN.1, FAU_GEN.2	Section 7.2.1
O.COMMUNICATIONS	FPT_ITT.1 FAU_GEN.1, FAU_GEN.2	Section 7.2.1
O.APLLICATION_POLITIQUE	FMT_SMF.1 FDP_ACC.1/Policy FDP_ACF.1/Policy FAU_GEN.1, FAU_GEN.2	
O.CRYPTO	FCS_COP.1	Section 7.2.1
O.CLES_CHIFFREMENT	FCS_CKM.1	Section 7.2.1

Tableau 12 : Association objectifs de sécurité de la TOE vers les exigences fonctionnelles

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FIA_UID.1	O.PROTECTION_DES_DONNEES_ENREGISTREES O.ROLE
FIA_UAU.1	O.PROTECTION_DES_DONNEES_ENREGISTREES
FAU_GEN.1	O.PROTECTION_DES_DONNEES_ENREGISTREES O.ROBUSTESSE O.COMMUNICATIONSO.JOURNALISATION O.RECOUVREMENT, O.APPLICATION_POLITIQUE

FAU_GEN.2	O.PROTECTION_DES_DONNEES_ENREGISTREES O.ROBUSTESSE O.COMMUNICATIONSO.JOURNALISATION O.RECOUVREMENT, O.APPLICATION_POLITIQUE
FPT_FLS.1	O.ROBUSTESSE
FMT_SMF.1	O.ROLE, O.RECOUVREMENT, O.APPLICATION_POLITIQUE
FMT_SMR.1	O.RECOUVREMENT O.ROLE
FMT_SAE.1	O.PROTECTION_DES_DONNEES_ENREGISTREES
FPT_ITT.1	O.COMMUNICATIONS
FDP_ACC.1/Policy:	O.APPLICATION_POLITIQUE
FDP_ACF.1/Policy:	O.APPLICATION_POLITIQUE
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
FMT_MSA.1/Password_SO	O.PROTECTION_DES_DONNEES_ENREGISTREES
FMT_MSA.1/Password_User	O.PROTECTION_DES_DONNEES_ENREGISTREES
FMT_MSA.1/New_Password_Guest	O.PROTECTION_DES_DONNEES_ENREGISTREES
FMT_MSA.1/Del_Password_Guest	O.PROTECTION_DES_DONNEES_ENREGISTREES
FDP_ACC.1/Disk	O.ARRET_UTILISATEUR, O.PROTECTION_DES_DONNEES_ENREGISTREES O.ROLE O.HIBERNATION
FDP_ACF.1/Disk	O.ARRET_UTILISATEUR, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.ROBUSTESSE O.ROLE O.HIBERNATION
FCS_COP.1	O.CRYPTO O.HIBERNATION
FDP_RIP.1	O.ARRET_UTILISATEUR
FCS_CKM.1	O.CLES_CHIFFREMENT

Tableau 13 : Association exigences fonctionnelles vers objectifs de sécurité de la TOE

7.3 Dépendances

7.3.1 Dépendances des exigences de sécurité fonctionnelles

Exigences	Dépendances CC	Dépendances Satisfaites
FIA_UID.1	Pas de dépendance	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FAU_GEN.1	(FPT_STM.1)	
FAU_GEN.2	(FAU_GEN.1) et (FIA_UID.1)	FAU_GEN.1, FIA_UID.1

FPT_FLS.1	Pas de dépendance	
FMT_SMF.1	Pas de dépendance	
FMT_SMR.1	FIA_UID.1	
FMT_SAE.1	(FMT_SMR.1) et (FPT_STM.1)	FMT_SMR.1
FPT_ITT.1	Pas de dépendance	
FDP_ACC.1/Policy	(FDP_ACF.1)	FDP_ACF.1/Policy
FDP_ACF.1/Policy	(FDP_ACC.1) et (FMT_MSA.3)	FDP_ACC.1/Policy
FMT_MSA.3	(FMT_MSA.1) et (FMT_SMR.1)	FMT_MSA.1/Disk_Status, FMT_MSA.1/ID, FMT_SMR.1, FMT_MSA.1/Password_SO, FMT_MSA.1/Password_User, FMT_MSA.1/New_Password_ Guest, FMT_MSA.1/Del_Password_ Guest
FMT_MSA.1/Disk_Status	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1/Disk, FMT_SMF.1, FMT.SMR1
FMT_MSA.1/ID	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1/Disk, FMT_SMF.1, FMT.SMR1
FMT_MSA.1/Password_SO	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1/Disk, FMT_SMF.1, FMT.SMR1
FMT_MSA.1/Password_User	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1/Disk, FMT_SMF.1, FMT.SMR1
FMT_MSA.1/New_Password_ Guest	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1/Disk, FMT_SMF.1, FMT.SMR1
FMT_MSA.1/Del_Password_ Guest	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1/Disk, FMT_SMF.1, FMT.SMR1
FDP_ACC.1/Disk	(FDP_ACF.1)	FDP_ACF.1/Disk
FDP_ACF.1/Disk	(FDP_ACC.1) et (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/Disk
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	
FCS_CKM.1	(FCS_CKM.2 ou FCS_COP.1) et (FCS_CKM.4)	FCS_COP.1

Tableau 14 : Dépendances des exigences fonctionnelles

7.3.1.1 Argumentaire pour les dépendances non satisfaites

Les dépendances **FPT_STM.1** de **FAU_GEN.1** et **FMT_SAE.1** ne sont pas supportées. L'horodate est fourni par l'environnement de la TOE.

La dépendance **FMT_MSA.3** de **FDP_ACF.1/Policy** n'est pas supportée. Le chiffrement du disque (objet de l'évaluation) ne peut être mis en œuvre que via une politique de sécurité.

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.

7.3.2 Dépendances des exigences de sécurité d'assurance

Exigence	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	
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 15 : Dépendances des exigences d'assurance

7.3.2.1 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 [QUALIF_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 [QUALIF_STD].

7.4 Argumentaire pour l'EAL

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

7.5 Argumentaire pour les augmentations à l'EAL

7.5.1 AVA_VAN.3 Focused vulnerability analysis

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

7.5.2 ALC_FLR.3 Systematic flaw remediation

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

8. CONFORMITE AU PROFIL DE PROTECTION [CDISK]

Dans ce document, tout le texte repris du profil de protection (PP) apparaît en police bleu.

Tout ajout par rapport au PP dans la définition du problème de sécurité, dans les objectifs et les exigences de sécurité reste en police noire et apparait donc clairement par rapport au texte de référence du PP.

C'est la raison pour laquelle ce chapitre se concentre sur les éléments supprimés du PP puisqu'ils n'apparaissent pas dans les chapitres précédents. Ces éléments apparaissent ~~en police bleu barrée~~.

Il faut également noter que dans l'ensemble de cette cible, les paragraphes relatifs à la configuration « sans génération de clé » et les mentions à la configuration « avec génération de clé » ont été supprimés.

Enfin, ont également été mis à jour :

- les références à l'ANSSI (DCSSI) et à ses documents de référence.
- Les numéros de tableaux.
- Les numéros de règles (Rule) utilisés dans les exigences.

8.1 Chapitre 3 – Définition du problème de sécurité

8.1.1 Section 3.1 – Biens

Des précisions sont apportées aux biens sensibles de l'utilisateur.

Suppression de la note ci-dessous qui est une suggestion d'expliciter d'autres biens.

~~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.~~

Comme cela est suggéré par cette note, d'autres biens sont ajoutés.

8.1.2 Section 3.2 – Utilisateurs

Ajout des rôles administrateur de la sécurité et invité.

Suppression de la note ci-dessous qui ne s'applique pas, la TOE prévoyant un rôle administrateur :

~~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.~~

8.1.3 Section 3.3 – Menaces

Suppression de la note au profit d'une précision que les biens menacés inclus les biens sensibles de la TOE (en particulier les clés de chiffrements du disque).

~~Note d'application~~

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

8.1.4 Section 3.4 – Politique de sécurité de l'organisation (OSP)

Aucune suppression.

8.1.5 Section 3.4 – Hypothèses

Suppression de l'hypothèse suivante relative 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.~~

8.2 Chapitre 4 – Objectifs de sécurité

8.2.1 Section 4.1 – Objectifs de sécurité pour la TOE

O.ARRET_UTILISATEUR

La TOE n'offrant pas de fonction de démontage, l'objectif est modifié ainsi :

La TOE doit rendre inaccessibles les données sensibles, en particulier les clés cryptographiques, lorsque ~~le disque est démonté par l'utilisateur~~ l'utilisateur éteint ou met en veille prolongée son ordinateur.

~~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.~~

8.2.2 Section 4.2 – Objectifs de sécurité pour l'environnement opérationnel

Suppression des objectifs suivants applicable à la configuration sans génération de clé.

~~**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.~~

8.3 Chapitre 5 – Exigences de sécurité

8.3.1 Chapitre 5.1 – Exigences de sécurité fonctionnelles

8.3.1.1 Opération CREATE

L'opération CREATE est ainsi simplifiée et complétée :

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~~ déverrouillant le disque et permettant toute opération sur les données de l'utilisateur (effacement, modification, lecture...).

8.3.1.2 Exigences FIA_UID.1 et FIA_UAU.1

Une fois un disque chiffré, l'utilisateur doit obligatoirement s'identifier et s'authentifier au démarrage du système. Mise à part l'opération de chiffrement du disque '(CREATE), toutes les autres opérations nécessite donc l'identification et l'authentification de l'utilisateur.

Les exigences FIA_UID.1 et FIA_UAU.1 sont modifiées ainsi :

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_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.

Outre l'ajout des opérations nécessitant une identification/authentification, la note concernant l'authentification est modifiée ainsi :

Note d'application

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

8.3.1.3 Exigence FPT_FLS.1

Les cas d'erreur que la TOE sait reprendre sont précisés dans l'exigence :

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].**~~
- **when the disk encryption or decryption operation is interrupted, whatever the reason (power cut, system or application crash**).

8.3.1.4 Exigence FMT_MSA.3

La note d'application précise la méthode de détermination de l'attribut de sécurité AT.ID :

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.~~

La valeur de l'attribut de sécurité AT.ID est déterminée par une méthode propriétaire.

8.3.1.5 Exigence FDP_ACC.1

L'exigence **FDP_ACC.1** du PP est instanciée en **FDP_ACC.1/Disk.**

8.3.1.6 Exigence FDP_ACF.1

L'exigence **FDP_ACF.1** du PP est instanciée en **FDP_ACF.1/Disk.**

Les événements provoquant le démontage d'un disque sont précisés dans les exigences :

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

- **Rule10: The TSF shall perform DISMOUNT operation on S.DISK after ~~[selection: completion of [assignment: operation], [assignement: time interval of user inactivity], [assignement: other condition]]~~ shut down, restart, hibernate, provided the value of the security attribute S.DISK.STATUS is ACTIVATED.**
- **None.**

FDP_ACF.1.4/Disk 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]~~ None.**

~~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).~~

8.3.1.7 Exigences liées à la cryptographie

Les mécanismes et algorithmes sont précisés dans les exigences FCS_COP.1.1 et FCS_CKM.1.1 :

FCS_COP.1.1 The TSF shall perform **~~[assignment: list of cryptographic operations]~~ hash, key derivation, key wrapping and unwrapping, encryption and decryption** in accordance with a specified cryptographic algorithm **~~[assignment: cryptographic algorithm]~~ SHA-256 and AES** and cryptographic key sizes **~~[assignment: cryptographic key sizes]~~ 128, 192, 256 bits** that meet the following: **ANSSI's cryptographic requirements (**[RGS_CRYPTO] **and** [RGS_CLES]**).**

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **~~[assignment: cryptographic key generation algorithm]~~ based on SHA-256 and AES** and specified cryptographic key sizes **~~[assignment: cryptographic key sizes]~~ 128, 192, 256 bits** that meet the following: **ANSSI's cryptographic requirements (**[RGS_CRYPTO] **and** [RGS_CLES]**)**.

8.3.2 Section 5.2 – Exigences de sécurité d'assurance

Les exigences visées sont celle d'une qualification au niveau standard, comme le demande le profil de protection.

8.4 Chapitre 6 – Argumentaires

Le chapitre « 6 – Argumentaires » du profil de protection correspond au chapitre 7 de la présente cible de sécurité.

Dans l'ensemble de ce chapitre, ont été supprimés :

- Les paragraphes et les lignes de tableaux relatifs à la configuration « sans génération de clé »
- Les portions de texte faisant référence à la configuration « avec génération de clé » ou au deux cas de configuration.

Les tableaux ont été mis en forme sur la base de la configuration « avec génération de clé ».

Dans la section des dépendances, dans la mesure où la TOE gère une notion de rôle (FMT_SMR.1) et offre des fonctions d'administration (FMT_SMF.1), les dépendances non satisfaites dans le PP suivantes sont supprimées :

~~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.~~