CRYHOD

FOR DISKS AND LAPTOPS

CIBLE DE SECURITE CRITERES COMMUNS NIVEAU EAL3+

VERSION Q.2021

Réf. : PX2051294r6

PRIMX

MAKE ENCRYPTION HAPPEN

Reproduction et droits

PRIMX

Siège : 18 rue du Général Mouton-Duvernet 69003 LYON – support@primx.eu

Direction commerciale : 21 rue Camille Desmoulins 92100 ISSY-LES-MOULINEAUX – Tél. : +33 (0)1 77 72 64 80 – business@primx.eu

www.primx.eu

Sommaire

Liste des figures

Liste des tableaux

1. INTRODUCTION DE LA CIBLE DE SECURITE

1.1. Identification de la cible de sécurité

Cible de sécurité :	Cryhod version Q.2021.2 Cible de sécurité CC niveau EAL3+
Version de la ST :	PX2051294 – v1r6 - Mai 2022
Cible d'évaluation (TOE) :	Cryhod Q.2021.2 pour les plateformes sous Microsoft Windows 10 versions 1809 LTSC et 20H2 (64 bits).
Niveau EAL :	EAL3 augmenté des composants ALC_FLR.3 et AVA_VAN.3 associé à une expertise de l'implémentation de la cryptographie décrite dans [QUALIF_STD].
Conformité à un PP existant :	Profil de Protection Application de chiffrement de données à la volée sur mémoire de masse [CDISK]
Référence des CC :	Critères Communs version 3.1 Révision 5, Parties 1 à 3 – Avril 2017

1.2. Vue d'ensemble de la cible d'évaluation

Cryhod est un **produit de sécurité logiciel** pour la confidentialité des données des organismes. Le produit permet le chiffrement de toutes les partitions d'un ou de plusieurs disques durs, le chiffrement est effectué au niveau des secteurs de disques. L'authentification des utilisateurs est effectuée avant l'amorçage du système.

Cryhod sera évalué pour une plateforme sous le système d'exploitation Microsoft Windows 10 versions 1809 LTSC et 20H2 (64 bits).

1.3. Conformité aux Critères Communs

Cette cible de sécurité respecte les exigences des Critères Communs version 3.1 d'avril 2017 :

[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Révision 5, Avril 2017. CCMB-2017-04-001.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Révision 5, Avril 2017. CCMB-2017-04-002.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Révision 5, Avril 2017. CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Révision 5, Avril 2017. CCMB-2017-04-004.

Toutes les exigences fonctionnelles décrites dans cette cible de sécurité sont issus de la Partie 2 « étendue » des Critères Communs version 3.1 révision 5 d'avril 2017. Le niveau d'assurance « EAL3 augmenté » retenu est conforme à la Partie 3 « stricte » des Critères Communs version 3.1 révision 5 d'avril 2017. Le niveau d'assurance est un niveau EAL3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

Toutes les interprétations des Critères Communs parues à la date de démarrage de l'évaluation seront retenues.

1.4. Conformité à un profil de protection

Cette cible est conforme (conformité démontrable selon la définition dans la Partie 1 des Critères Communs) au profil de protection suivant (configuration « avec génération de clé ») :

[CDISK] Profil de Protection Application de chiffrement de données à la volée sur mémoire de masse – version 1.4 d'aout 2008, DCSSI

Les parties relatives au profil de protection sont indiquées en caractères rouges.

1.5. Conformité aux référentiels de l'ANSSI

Cette cible de sécurité est conforme aux référentiels de l'ANSSI suivants :

[QUALIF_STD]	Processus de qualification d'un produit – version 1.0 du 12 janvier 2017, ANSSI.
[CRYPTO_STD]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - Version 2.04 du 1er janvier 2020, ANSSI.
[CLES_STD]	RGS version 2.0 – Annexe B2. Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques - version 2.0 du 8 juin 2012, ANSSI
[AUTH_STD]	RGS version 1.0 – Annexe B3. Authentification : Règles et recommandations concernant les mécanismes d'authentification - Version 1.0 du 13 janvier 2010, ANSSI.
[MOTS_DE_PASSE_STD]	Recommandations de sécurité relatives aux mots de passe Version 1.1 du 5 juin 2012, ANSSI

2. DESCRIPTION DE LA CIBLE D'EVALUATION (TOE)

2.1. Présentation de la TOE

2.1.1. Description Générale

Cryhod est un **produit de sécurité** pour postes de travail opérant avec des processeurs 32 ou 64 bits sous Windows (à partir de Windows 7) et Linux (à partir d'Ubuntu 12.04 et CentOS 6.5). Cryhod assure à la fois une authentification avant l'amorçage du poste et un chiffrement complet et transparent des données sur les disques dur internes ou additionnels. Son rôle est de préserver la confidentialité des documents manipulés par les utilisateurs, sur des postes isolés, des ordinateurs portables, ou des postes de travail connectés au réseau d'un organisme.

En effet, tous les fichiers systèmes « invisibles à l'utilisateur » sont susceptibles de contenir des données sensibles (fichiers temporaires, fichier d'échange). Il en va de même des fichiers supprimés par l'utilisateur et dont le contenu peut rester longtemps sur le disque. Le chiffrement complet des partitions du disque assure la protection de ces données au même titre que les autres données utilisateur.

Le logiciel n'a aucun impact sur les habitudes de travail de l'utilisateur ; une fois authentifié celui-ci accède aux données de façon habituelle, le (dé)chiffrement étant effectué '**à la volée**' de façon totalement transparente. Les opérations de chiffrement initial (ainsi que les processus de déchiffrement et de transchiffrement) sont conçues pour résister aux imprévus, notamment aux coupures de courant ou au plantage système. Les mécanismes de récupération interne de Cryhod assurent une récupération sans perte de données et la reprise automatique du processus de chiffrement (déchiffrement, transchiffrement).

L'authentification de l'utilisateur est effectuée dans la phase d'amorçage (pré-boot) du système. Pour s'authentifier, il est possible de définir un certain nombre **d'accès** : l'accès de l'utilisateur principal, d'un collègue ou d'un chef de service éventuel, l'accès réservé du responsable de la sécurité, l'accès de secours de l'organisme (recouvrement), etc. La définition de ces accès est libre, mais le produit est doté de fonctions et de mécanismes d'administration permettant d'imposer certains accès ou certains types d'accès.

Cryhod prend en charge et gère les aspects hibernation (veille prolongée) en assurant le chiffrement des données d'image générées afin de les sauvegarder de façon sécurisée sur le disque dur. Lors du «réveil» du poste de travail, Cryhod demande à l'utilisateur de s'authentifier de nouveau.

Cryhod propose un service de « Single Sign-On (SSO)» évitant à l'utilisateur de de saisir plusieurs fois ses secrets, une première fois pour s'authentifier avant l'amorçage du système (mot de passe ou clé RSA), une seconde fois pour ouvrir une session Windows (mot de passe). L'utilisateur s'authentifie une seule fois (à l'amorçage donc par mot de passe ou clé RSA) pour les deux opérations. En cas de modification du mot de passe Windows par l'utilisateur, Cryhod met à jour automatiquement le mot de passe renseigné dans l'identifiant SSO du pré-boot.

Enfin, Cryhod permet un recouvrement local ou distant (procédure de secours) par un Officier de Sécurité des partitions chiffrées.

2.1.2. Accès

Pour pouvoir accéder aux données chiffrées, un utilisateur doit donc disposer d'une **clé d'accès**. Un accès correspond à une **clé d'accès** (une clé cryptographique) que possède un utilisateur. Cette clé peut être soit une clé dérivée d'un mot de passe (dans ce cas l'utilisateur ne possède pas la clé d'accès elle-même mais le mot de passe permettant à Cryhod de la calculer), soit une clé RSA hébergée dans un porte-clés comme un fichier de clé ou une carte à mémoire, un conteneur CSP ou CNG Microsoft Windows (le porte-clés intégrant la plupart du temps son propre dispositif d'authentification avec un code confidentiel). Une clé d'accès permet de retrouver (en les déchiffrant) les informations de chiffrement des fichiers.

S'il s'agit d'une clé RSA hébergé dans un porte-clés, cette clé lui a été remise par l'Administrateur de la Sécurité (appelé Administrateur de la TOE dans la suite du document). Le mot de passe peut être fourni par l'administrateur de la TOE ou choisi par l'utilisateur en fonction de la politique de sécurité mise en œuvre.

Cryhod propose différents algorithmes et mécanismes de sécurité, tous conformes aux standards en la matière. Il propose deux schémas de gestion de clés d'accès qui peuvent être utilisés en même temps. Un schéma dit « symétrique » basé sur des mots de passe et des clés dérivées de mots de passe (réf. : PKCS#5) et un schéma dit « asymétrique » utilisant des clés RSA (réf. : PKCS#1) embarquées dans des fichiers de clés (réf. : PKCS#12) ou des porte-clés (ref: PKCS#11 et/ou CSP/CNG).

Parmi les accès, il peut y avoir un ou plusieurs accès dits "de recouvrement", de type 'mot de passe' ou de type 'clé RSA' (accès apposé par certificat). Ces recouvrements sont systématiquement appliqués s'ils sont déclarés dans une politique de sécurité dédiée.

2.2. Services d'utilisation et rôles

2.2.1. Définition des rôles

Hormis le responsable de la sécurité de l'organisation qui fixe la politique générale de sécurité à appliquer, on distingue 3 rôles mettant en œuvre (directement ou indirectement) les fonctionnalités de la TOE :

- Un rôle opérant uniquement dans l'environnement de la TOE : L'administrateur de la sécurité de l'environnement Windows des utilisateurs (appelé administrateur Windows dans la suite du document) en charge de définir les règles d'usage et de sécurité (les policies), c'est-à-dire le paramétrage de fonctionnement du produit : cette opération de « haut-niveau » est effectuée sous le contrôle du Responsable de la Sécurité (administrateur de la TOE défini ci-dessous) qui a étudié les différents paramètres et décidé des valeurs à affecter pour obtenir le comportement souhaité du produit dans le cadre d'utilisation et d'environnement prévu. Les policies peuvent être signées par l'administrateur de la TOE et vérifiées par Cryhod avant leur application. Le mécanisme de signature de politiques permet de garantir que seules des politiques validées par l'administrateur puissent être appliquées sur les postes de travail. En environnement Active Directory, un administrateur de domaine, autorisé pourtant à modifier les politiques du domaine, ne pourra pas intervenir sur la configuration du produit : s'il modifie les politiques, la signature deviendra invalide et donc les nouvelles politiques seront refusées sur les postes de travail. Les règles une fois affectées ne changeront ensuite que de façon très exceptionnelle. Il est à noter que ce rôle peut se décliner en plusieurs rôles hiérarchiques correspondant aux différents niveaux des domaines Windows. Dans ce cas les administrateurs Windows des niveaux supérieurs doivent interdire aux administrateurs des sous-niveaux (domaines, contrôleurs de domaines, postes de travail) la modification des « policies » de la TOE qu'ils souhaitent eux-mêmes contrôler.
- Un rôle administrateur de la TOE en charge de définir les emplacements chiffrés du « parc » et effectuer la procédure de migration initiale qui consiste à chiffrer leur contenu actuel. Pour chaque emplacement chiffré, il faut configurer la liste des personnes pouvant y accéder en introduisant leurs clés d'accès (ou en paramétrant des listes d'accès). Par la suite, l'entretien consistera principalement à créer de nouveaux emplacements si besoin est (nouveaux ordinateurs), à gérer les 'mouvements de personnel' (nouvel utilisateur, retrait d'accès pour une personne en partance), et, éventuellement, de transchiffrer les emplacements chiffrés (sur compromission ou régulièrement). L'administrateur de la TOE effectue par ailleurs les opérations de recouvrement local et de secours distant. Sauf mention contraire dans la suite de ce document, toute référence à l'administrateur se rapporte à ce rôle.
- Utilisateur de la machine dont certaines données sont à protéger en confidentialité sur le disque de la machine. L'utilisateur utilise la TOE selon la configuration imposée par l'administrateur Windows et l'administrateur de la TOE.

Il faut noter que, à part la définition des policies, généralement dévolue à un responsable de la sécurité, les autres opérations peuvent être effectuées par différents acteurs en fonction de la confiance, de l'organisation et des moyens de l'organisme.

2.2.2. Administration

Les différentes commandes offertes permettent de réaliser les opérations d'administration suivantes :

- Lire ou modifier les policies, signer les policies ;
- Chiffrer une partition ;

- Déchiffrer une partition ;
- Transchiffrer une partition (renouveler les clés de chiffrement de la partition);
- Ajouter, modifier ou supprimer un accès à une partition ;
- Modifier le rôle d'un accès (utilisateur ou administrateur);
- Consulter les accès d'une partition ;
- Effectuer le recouvrement par l'administrateur de sécurité.
- Effectuer le secours utilisateur par l'administrateur de sécurité.

Certaines opérations (chiffrement, déchiffrement) peuvent être télé-ordonnées via policies et l'utilisateur peut n'avoir aucun droit de gestion. Un centre de chiffrement sur le poste permet de consulter l'état de chiffrement des différentes partitions et de passer des directives de façon complémentaire au paramétrage par policies (si les policies le permettent).

Cryhod met également à disposition ses informations de gestion au travers de l'interface **WMI** (Windows Management Instrumentation). Ce format standard permet de collecter des informations précises sur tous les postes de travail (conformité aux règles de chiffrement, application des accès de recouvrement, inventaire des partitions chiffrées, des accès etc.).

Les commandes d'administration peuvent enregistrer leur déroulement dans des fichiers 'traces' pour analyse ultérieure.

Par ailleurs, Cryhod émet des événements Windows consultables avec **l'Observateur d'Evénements Windows** (Eventvwr). La liste des événements est configurable, et ils peuvent également être envoyés vers un serveur Windows. On y trouve les événements d'authentification (notamment à l'amorçage) et toutes les commandes d'administration, réussies ou non.

Un **outil de collecte d'informations** est disponible (si la politique de sécurité le permet) via le menu de la fenêtre "A propos de…". Cet outil permet de générer un rapport de configuration chiffré à transmettre au support technique Prim'X (en pièce jointe d'un courrier électronique par exemple). Les informations collectées et sélectionnées par l'utilisateur sont la configuration des politiques, les applications installées, les fichiers logs. Le rapport est intégré dans un fichier sécurisé basé sur la même technologie que le carnet de mot de passe (avec le support technique comme accès unique) pour transmission via email par exemple.

2.2.3. Exemple d'utilisation

Il existe différents scénarios de mise en œuvre, mais le principe d'utilisation reste le même pour les utilisateurs.

L'administrateur de la sécurité de l'environnement Windows définit ***les règles d'usage (policies)*** du produit puis l'administrateur de la sécurité les signe avec sa clé de signature privée, ce qui se traduit par une configuration prédéfinie (policy) qui peut être masterisée (personnalisation de l'installation) ou télé-gérée (diffusée, mise à jour) soit par des commandes d'administration fournies par le produit soit par la logistique intégrée des réseaux bureautiques (exemple : contrôleurs de domaines). Ces règles sont généralement établies à « haut niveau » dans l'entreprise par le Responsable de la Sécurité. Parmi ces règles, on trouve, par exemple, l'algorithme de chiffrement à utiliser, le comportement que doit adopter le logiciel dans certains cas, les porte-clés PKCS#11 supportés etc.

Le logiciel, masterisé ou non, est ensuite ***installé*** sur un poste de travail, manuellement ou via les logiciels de télé-installation du marché.

Par ailleurs, il est à la charge de l'administrateur de la sécurité de ***définir (fournir) les clés d'accès*** des utilisateurs (issues d'une PKI, par exemple). Cryhod supporte différents scénarios de gestion de clés, mais n'en fournit pas l'infrastructure. Si une PKI est en place, il sait en utiliser les éléments (clés RSA, porte-clés, certificats), si elle n'est que partiellement installée, ou s'il n'y en a pas, il sait également utiliser des accès par mots de passe.

Puis, l'administrateur de la TOE doit définir une politique de chiffrement sur les postes de travail, en fonction de leur contenu et/ou de leur topologie : il s'agit en pratique de définir quels emplacements doivent être chiffrés et d'exécuter la procédure de chiffrement initial. L'exécution de la procédure peut être effectuée par l'administrateur lui-même ou être déléguée à l'utilisateur.

Une fois ces opérations initiales effectuées, les emplacements chiffrés sont définis et chiffrés, et les accès pour les utilisateurs sont définis. Seuls les utilisateurs disposant de clés d'accès valides pour les emplacements chiffrés pourront donc y accéder.

Pour un utilisateur, et, par extension, pour TOUTES les applications (y compris le système lui-même), le fonctionnement est alors très simple et transparent : dès qu'un fichier est ouvert dans un emplacement chiffré, à des fins de lecture ou d'écriture, les portions qui sont lues sont déchiffrées «à la volée» et les portions qui sont écrites sont chiffrées «à la volée». Techniquement, les applications (au sens large) ignorent que le contenu du fichier est chiffré, ou va être chiffré, elles travaillent exactement comme si ce n'était pas le cas. Par exemple, un «double-clic» pour ouvrir un fichier chiffré lance directement l'application concernée, qui accède au contenu.

Avant le démarrage du système (amorçage du système), Cryhod demande à l'utilisateur une clé d'accès permettant de s'authentifier. Cette clé donne l'accès au login Windows (ou permet de lancer directement le système d'exploitation en mode SSO) et de déchiffrer les fichiers dans les emplacements permis à l'utilisateur (en pratique, le schéma est plus complexe, et cette clé d'accès permet de déchiffrer des clés intermédiaires qui elles-mêmes chiffrent les fichiers).

2.3. Périmètre et architecture de la cible d'évaluation

2.3.1. Les composants de Cryhod

Cryhod s'articule autour de 4 composants principaux :

- En mode BIOS ne nécessitant pas le support des périphériques USB pour entrer la clé d'accès (clé d'accès de type mot de passe par exemple), le pré-boot BIOS est en charge de piloter la phase d'amorçage du poste de travail en gérant la phase d'authentification de l'utilisateur ainsi que quelques fonctions de base (langue, gestion par l'utilisateur du mode SSO …). Ce mode n'est pas dans le périmètre de la TOE.
- En mode BIOS nécessitant le support des périphériques USB pour entrer la clé d'accès (utilisation d'une carte à puce par exemple), le pré-boot BIOS charge un Linux propriétaire (construit à partir du noyau Linux 3.7.3) pour gérer la phase d'authentification de l'utilisateur. Ce mode n'est pas dans le périmètre de la TOE.
- En mode EFI, le pré-boot EFI effectue les mêmes fonctions que les 2 composants du mode BIOS.
- Les drivers et services sous Windows qui assurent le fonctionnement du produit dans l'environnement de travail de l'utilisateur : chiffrement (déchiffrement) et transchiffrement du poste, gestion des accès, audit …

2.3.2. Périmètre de la TOE

2.3.2.1. Périmètre logique

Le périmètre d'évaluation est constitué de l'ensemble des composants du logiciel.

Seul le build Q.2021.2 configuré avec les politiques de sécurité activées suivantes est déclaré conforme (toutes les politiques non indiquées sont configurées avec leur valeur par défaut) :

Mode Active directory

- Comme indiqué dans le guide utilisateur, la politique P131 (accès obligatoires) doit être configurée pour pouvoir utiliser le produit. Cette politique doit donc être configurée avec l'accès de recouvrement de l'administrateur.

Note : Au moment d'effectuer le recouvrement, les politiques P269 - Ouverture au moyen de clés de recouvrement, P198 - Affichage des accès de recouvrement et P199 - Affichage des accès obligatoires devront être activées. Ces politiques ne sont normalement pas activées dans un environnement de production (notamment pour masquer les accès de recouvrement) et ne font donc pas partie du périmètre de test de l'évaluation).

- La politique P710 (seuil d'acceptation des mots de passe) doit être configurée à 100% et la politique P712 (longueur des mots de passe) doit être configurée à 12.
- La politique P303 (activer les événements pour toutes les opérations d'administration) doit être configurée à « oui ».

- La politique P339 (options du rapport de configuration) doit être configurée à « 0 » qui permet la collecte, il faut également renseigner le mot NONE dans le nom de la valeur de la politique P137 (accès imposés lors du chiffrement des informations collectées).
- La politique P382 (autoriser l'utilisation du jeu d'instructions AES-NI) doit être configurée à « Non ».
- La politique P383 (mode de chiffrement RSA) doit être configurée à « PKCS#1 v2.2 avec utilisation de SHA-256 ».
- La politique P386 (mécanisme de signature) doit être configurée à « PKCS#1 v2.2 PSS ».
- La politique P387 (mécanisme de dérivation (mot de passe)) doit être configurée à « SHA256-PBKDF2 » ou « SHA512-PBKDF2 ».
- La politique P258 (Action suite au retrait d'accès d'une partition chiffrée) doit être configurée à « Imposer le transchiffrement de la partition » (valeur par défaut)
- La politique P885 (autoriser l'installation du module de démarrage automatique) doit être configurée à « Non installé » (valeur par défaut)

Mode Alternatif :

Toutes les politiques ci-dessus (P131, P710 et P712, P303, P339 et P137, P382, P383, P386, P387, P258 et P885) sont à configurer dans le fichier de configuration des politiques dédié au mode alternatif.

En dehors de ce fichier, il faut configurer la suivante dans les politiques Active Directory:

- La politique P070 (configuration alternative des politiques) doit être configurée en indiquant le chemin du fichier de configuration alternative des politiques

2.3.2.2. Périmètre physique

Cryhod sera évalué sur une plate-forme PC sous deux builds du système d'exploitation Windows 10 (64 bits) de Microsoft. Donc le produit Cryhod Linux n'est pas concerné par l'évaluation.

L'évaluation couvre uniquement l'amorçage des systèmes en mode EFI (l'ancien mode BIOS est donc hors périmètre). Lors de la phase d'amorçage, le mode SSO (permettant de coupler l'entrée de la clé d'accès au pré-boot et l'authentification à la session Windows) sera également analysé.

L'utilisation avec les différentes clés d'accès sera évalué (mot de passe et clé RSA). En particulier, le dialogue PKCS#11 entre la TOE et les porte-clés utilisateurs, le dialogue PKCS#12 entre la TOE et les fichiers de clés seront également évalués.

Les éléments suivants sont hors évaluation :

- Les systèmes d'exploitation Windows ;
- Les portes clés utilisés (comme les porte-clés de type Token USB, les fichiers de clés ou les containers CSP/CNG). Attention la dérivation des mots de passe utilisateur en clé d'accès fait bien partie du périmètre.
- l'outil GPOSign.exe permettant à l'administrateur de sécurité de signer les politiques ainsi que la génération de la clé de signature. Par contre la vérification de la signature des politiques par Cryhod fait bien partie du périmètre de la TOE.
- La mise à jour système automatisée sans utilisateur
- Le pré-chiffrement d'une machine par un opérateur externe

Le logiciel Cryhod utilise des clés utilisateurs (les «clés d'accès») fournies par l'environnement (clés RSA dans des porte-clés ou mots de passe fournis par l'administrateur de la TOE) mais ne procède pas au tirage de clés utilisateurs. Ce tirage est donc hors évaluation.

Cryhod est téléchargée depuis le site Web de l'éditeur à partir d'un compte privé sur le site client (client.primx.eu/Software/Download) ou le site partenaire (partner.primx.eu/Software/Download). Le programme d'installation est signé par Prim'X avec la technologie Authenticode. La valeur de la signature peut être comparé à celle indiquée pour le package à la page « Signature » du site Web. Le programme installe les outils de signature des

politiques (hors périmètre) et de secours utilisateur, ainsi que tous les guides du produit au format pdf à savoir le guide d'installation, les guides d'utilisation et de mise en œuvre rapide, le guide de supervision WMI et le guide de signature des politiques. Les guides sont également téléchargeables à partir du compte client ou partenaire.

2.3.2.3. Plate-forme de tests pour l'évaluation de la TOE

Pour l'évaluation du produit Cryhod, la plate-forme suivante devra être mise en place par l'évaluateur.

- Deux PC ou machines virtuelles équipés des systèmes d'exploitation suivants :
  - Windows 10 version 1809 LTSC 64 bits en modes d'authentification par token USB et fichier de clés ;
  - Windows 10 version 20H2 64 bits en mode d'authentification par CSP et mot de passe ;
- Un contrôleur de domaine (PC ou machine virtuelle) équipé de Windows Serveur 2019.

Le type physique de porte-clés (carte à puce ou clé USB) étant transparent pour Cryhod (seul le dialogue PKCS#11 est important), les tests de l'évaluateur pourront s'effectuer avec un seul type de porte-clés.

On activera les politiques de sécurité conformément au périmètre logique défini ci-dessus. En mode active directory, la fonction de contrôle de signature des politiques nécessite une installation de la TOE avec un package d'installation spécialement préparé en se référant à la documentation de la fonction.

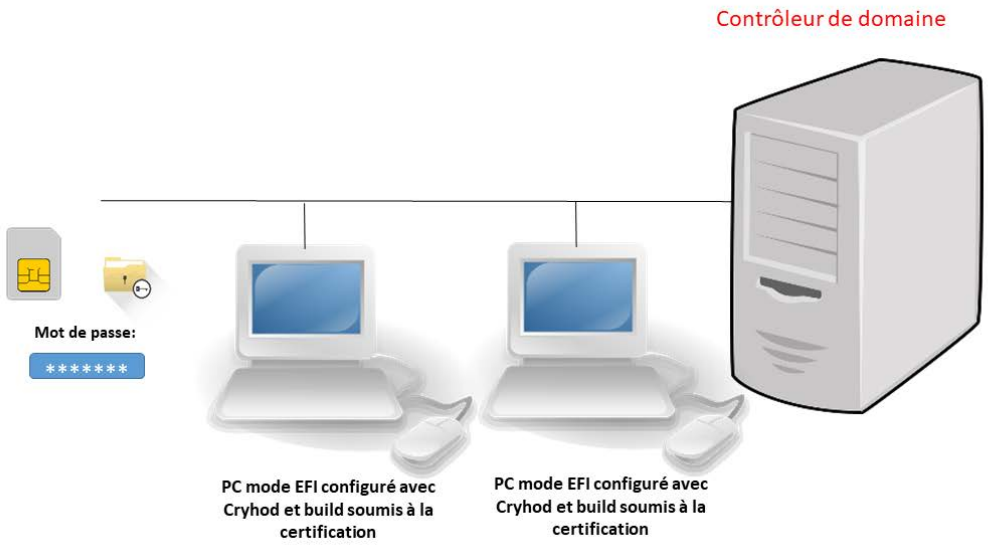

Figure 1 : Plate-forme de tests pour l'évaluation de la TOE

3. DEFINITION DU PROBLEME DE SECURITE

3.1. Les biens sensibles

3.1.1. Biens sensibles de l'utilisateur

3.1.1.1. Clés d'accès : D. CLES_ACCES

Lors de la phase d'authentification, Cryhod met en œuvre les clés d'accès des utilisateurs. En fonction des cas de figure, il peut être amené à manipuler directement soit la clé d'accès elle-même, soit son code confidentiel de protection.

- Accès par mot de passe : Cryhod gère la saisie du mot de passe, sa transformation (dérivation) en clé d'accès puis le déchiffrement de la clé de chiffrement et déchiffrement des fichiers du conteneur par cette clé d'accès. La politique de complexité des mots de passe est configurable par les politiques de sécurité ;
- Accès par clé RSA hébergée dans un fichier de clés en utilisant le mécanisme PKCS#12 : Cryhod gère la saisie du code confidentiel du fichier de clés, lit et déchiffre le fichier de clés avec ce code confidentiel, obtient la clé d'accès RSA et effectue le déchiffrement de la clé de chiffrement et déchiffrement des fichiers du conteneur par cette clé d'accès;
- Accès par clé RSA hébergée dans un token logique accédé au travers d'un composant externe PKCS#11 (ce composant pouvant piloter une carte à mémoire, un token USB ou tout autre dispositif hardware ou software) : Cryhod gère la saisie du code confidentiel du token logique, le remet au composant externe pour le déverrouiller. Cryhod fournit également au composant externe la clé de chiffrement des fichiers chiffrés par sa clé publique. Le composant déchiffre la clé de chiffrement avec sa clé privée puis la transmet à Cryhod qui peut alors effectuer le déchiffrement des fichiers;
- Accès par clé RSA hébergée dans un token logique accédé au travers d'un composant externe CSP ou CNG (ce composant pouvant piloter une carte à mémoire, un token USB ou tout autre dispositif hardware ou software) : Cryhod ne gère pas la saisie du code confidentiel du token logique, c'est le composant externe qui le fait spontanément avec ses propres moyens. Cryhod fournit au composant externe la clé de chiffrement des fichiers chiffrés par sa clé publique. Le composant déchiffre la clé de chiffrement avec sa clé privée puis la transmet à Cryhod qui peut alors effectuer le déchiffrement des fichiers. Ce moyen d'accès n'est disponible que dans l'environnement Windows (accès à une partition pour laquelle on n'a pas fourni de clé lors de l'amorçage du système).

En fonction de ces cas, donc, Cryhod manipule comme biens sensibles un mot de passe ou code confidentiel (en saisie), et une clé d'accès cryptographique. Dans les cas 1 et 2, il manipule les deux éléments, dans le cas 3, il ne manipule que le premier, dans le cas 4, il n'en manipule aucun.

Il faut noter que Cryhod ne génère PAS les clés d'accès des utilisateurs : quand il s'agit de clés RSA, quel que soit le porte-clés qui les héberge et le module qui les traite, elles sont toujours générées par un outil externe à Cryhod (en général une PKI), de même que le porte-clés éventuel et le code confidentiel de protection. Quand il s'agit de mots de passe, c'est l'administrateur de la sécurité ou le premier utilisateur (administrateur des accès) qui le choisissent. L'utilisateur et son environnement (règles et procédures internes, établies par le Responsable de la Sécurité) sont responsables de la qualité de ces clés, de la protection du porte-clés et de leur bonne utilisation.

Plutôt que de définir directement les accès utilisateurs dans une partition, il est possible (c'est même le comportement par défaut) de passer par un maillon intermédiaire, la **liste d'accès**. Une liste d'accès regroupe l'accès utilisateurs, l'accès de secours et les accès de recouvrement et la partition fait ensuite référence à cette liste. Cela permet notamment d'utiliser une même liste d'accès pour toutes les partitions (unicité de gestion), et de regrouper les listes d'accès au même endroit (centralisation).

Protection: confidentialité.

3.1.1.2. Données utilisateur : 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).

Cryhod permet de conserver sous forme chiffrée les fichiers (et dossiers) stockés sur les partitions du disque dur. Les biens sensibles sont donc les fichiers et dossiers utilisateurs, de tous types, stockés sur le disque.

Protection: confidentialité.

Remarque:

Les fichiers supprimés (quelle que soit la façon dont ils sont supprimés, action utilisateur ou par programme) ainsi que les fichiers temporaires et les fichiers d'échange de la mémoire virtuelle du système (contenant des 'images mémoire instantanées' des applications actives), peuvent contenir des données utilisateur sensibles. Tous ces fichiers sont chiffrés par le chiffrement des partitions du disque et sont donc considérés comme des données utilisateur chiffrées.

3.1.1.1. Bi clé de signature des politiques : D.ID_ADMIN

Les politiques de sécurité sont signées par l'administrateur de la sécurité et vérifiées par Cryhod avant leur application. Le bi-clé de signature dont surtout la clé privée de l'administrateur fait donc partie des biens sensibles de cet utilisateur particulier.

Protection: confidentialité (clé privée) et intégrité (clé publique).

3.1.1.2. Fichiers hibernation:D.HIBER

Cryhod permet d'utiliser le mode hibernation (veille prolongée) tout en assurant le chiffrement des données générées.

Protection: confidentialité

Note: Par sécurité, l'installation de Cryhod désactive la possibilité de mise en veille simple car celle-ci est trompeuse pour l'utilisateur (qui peut croire son poste éteint) et dangereuse car les clés des disques chiffrés sont actives et en mémoire vive qui reste alimentée par définition dans ce mode. Le verrouillage de session est permis car l'utilisateur en a la visibilité.

3.1.2. Biens sensibles de la TOE

3.1.2.1. Les clés symétriques de chiffrement de partitions : D.CLES_PAR

Les partitions sont chiffrées par une clé de chiffrement générée lors du lancement du chiffrement. Les clés sont stockées chiffrées par les clés d'accès des utilisateurs dans un fichier de fonctionnement spécifique voir D.FONC ci-dessous).

Protection: confidentialité

3.1.2.1. Bi clé de signature des fichiers de fonctionnement : D.ID_FONC

Les fichiers de fonctionnement sont signés par Cryhod à chaque modification et vérifiés avant l'amorçage du poste. Le bi-clé de signature dont surtout la clé privée fait donc partie des biens sensibles de la TOE.

Protection: confidentialité (clé privée).

3.1.2.2. Les programmes : D.PROGRAMMES

Pour assurer son fonctionnement, la TOE met en œuvre ses ***programmes*** (exécutables, bibliothèques dynamiques. La sécurité en intégrité des programmes sous Windows est d'abord assurée par l'environnement : il faut être administrateur Windows pour les modifier. Par ailleurs, ces programmes sont également signés par le système authenticode Windows.

Par ailleurs, les programmes du pré-boot ainsi que les drivers sont signés par Microsoft (technologie Secure Boot en mode EFI).

Protection: intégrité.

3.1.2.3. La configuration : D.CONFIGURATION

Pour assurer son fonctionnement, la TOE met en œuvre des ***policies :***

- Soit par l'intermédiaire des « Group Policies » qui sont des fonctions de gestion centralisée de la famille Microsoft Windows permettant la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory.
- Soit en utilisant un «mode alternatif», permettant de définir la configuration désirée au sein d'un ou plusieurs fichiers accessibles sur un simple partage de fichiers.

La sécurité en intégrité de ces policies est assurée :

- Par l'environnement (i.e. le système des policies sous Windows) : il faut être l'administrateur Windows de plus haut niveau pour les modifier (si un domaine Windows définit une valeur pour un paramètre, alors un administrateur local au poste ne pourra pas la modifier).
- Par le produit dans la mesure où les politiques sont signées par l'administrateur de la sécurité et vérifiées par Cryhod avant d'être appliquées.

  Protection: intégrité.

3.1.2.4. Les fichiers techniques de fonctionnement : D.FONC

On ne considère ici que les fichiers sensibles décrivant les accès aux partitions chiffrés ainsi que des données utilisées par le pré-boot. Ils contiennent notamment quelques informations de gestion (politiques, éléments de personnalisation, événements générés par le pré-boot), et les 'wrappings' d'accès, c'est-à-dire les clés de chiffrement des emplacements chiffrés par les clés d'accès des utilisateurs habilités. Un contrôle d'intégrité est effectué sur ces fichiers.

Protection: confidentialité et intégrité

3.1.2.5. Synthèse des biens sensibles

Le tableau ci-dessous résume la liste des biens sensibles protégés par Cryhod et indique la nature de la sensibilité associée. Les qualificatifs « forte » et « faible » de la sensibilité font référence au degré de protection vis-à-vis du potentiel d'attaque visé dans la cible (chapitre 3.4). Une sensibilité forte impose un niveau de protection résistant à l'attaque correspondante pour le niveau visé (divulgation du bien, atteinte à l'intégrité non détectée), une sensibilité faible indique que le bien n'a pas à être protégé au degré visé. Par exemple la divulgation des politiques apporte peu d'information intéressante à un éventuel attaquant (configuration générale du produit) mais la modification des politiques doit être contrôlée sous peine d'atteinte à la sécurité du produit (ajout d'un accès de recouvrement par exemple).

Remarque : de façon générale, l'intégrité n'est pas l'objectif premier de Cryhod. Le rôle du produit est de gérer la confidentialité des biens sensibles qui lui sont confiés, mais ce n'est pas un produit dont le but est de détecter une altération quelconque dans l'environnement (intrusion, virus, etc.). Par contre, Cryhod met en œuvre des dispositifs permettant de détecter des altérations qui seraient nuisibles à son bon fonctionnement, ou qui induiraient un défaut dans son objectif de confidentialité.

Biens sensibles	Confidentialité	Intégrité
Biens sensibles de l'utilisateur		
Eléments des clés d'accès manipulés par Cryhod : cas des mots de passe ou codes confidentiels éventuels. (D.CLES_ACCES)	Forte	NA
Eléments des clés d'accès manipulés par Cryhod : cas des clés d'accès elle-même si elles sont directement utilisées par Cryhod (D.CLES_ACCES)	Forte	Forte
Fichiers et dossiers de l'utilisateur stockés sur le disque (dont les fichiers temporaires et le fichier d'échange) (D.DONNEES_UTILISATEUR)	Forte	*Faible.*
Bi clé de signature (D.ID_ADMIN)	Forte	Forte
Fichier hibernation (D.HIBER)	Forte	*Faible.*

Biens sensibles	Confidentialité	Intégrité
Biens sensibles de la TOE		
Clé de chiffrement des partitions (D.CLE_PAR)	Forte	Forte
Bi clé de signature (D.ID_FONC)	Forte	Forte
Programmes de Cryhod (D.PROGRAMMES)	*Faible*	Forte
Configuration (D.CONFIGURATION)	*Faible*	Forte
Fichiers de fonctionnement (D.FONC)	Forte	Forte

Tableau 1 : Synthèse des biens sensibles

3.2. Utilisateurs

La TOE supporte 2 rôles:

- L'administrateur de la TOE en charge de gérer les accès et assurer le recouvrement (accès particulier) et le secours.
- Utilisateur de la machine dont certaines données sont à protéger en confidentialité sur le disque de la machine.

3.3. Hypothèses

Pour Cryhod, nommée la TOE dans les paragraphes suivants, les hypothèses suivantes sur l'environnement d'utilisation seront prises en compte pour l'évaluation du niveau de confiance offert aux utilisateurs :

A.NON_OBSERV — L'environnement physique de la TOE permet aux utilisateurs d'entrer leur mot de passe ou code PIN sans être observable directement et sans que cela puisse être intercepté par d'autres utilisateurs ou attaquants potentiels.

A.ENV_OPERATIONNEL — L'environnement opérationnel ne permet pas à un attaquant d'accéder au disque (physiquement ou par le réseau) lorsque des données sensibles sont accessibles à un utilisateur légitime sur l'équipement. L'équipement doit donc apporter des protections efficaces contre l'accès illicite distant (pare-feu correctement configuré, antivirus et anti logiciels espions avec bases de données à jour etc.). L'environnement de la TOE fournit un système d'horodatage fiable qui permet à la TOE de dater précisément les événements enregistrés dans son journal.

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.FIRMWARE — L'environnement d'exécution du mode EFI doit contrôler l'intégrité du code de démarrage (pré-boot) de la TOE (technologie Secure Boot). Cette fonction ne doit pas pouvoir être désactivée par un attaquant potentiel et doit donc être protégée de toute manipulation par un mot de passe conforme aux recommandations détaillées dans le document [MOTS_DE_PASSE_STD].

A.PORT_DMA — DMA (Direct Memory Access) est une technologie permettant à des périphériques de lire/écrire directement dans la mémoire sans passer par le micro-processeur. Un attaquant pourrait donc profiter d'une absence de l'utilisateur pour brancher un matériel, à son insu, sur l'un des ports DMA,

	afin de récupérer plus tard certaines informations sensibles stockées en mémoire après que l'utilisateur ait utilisé son poste. L'administrateur doit donc veiller à désactiver l'utilisation des périphériques DMA dans les paramètres de configuration du BIOS de la station de travail.
A.CONFIANCE_ADM_TOE	Les administrateurs de la TOE sont des personnes de confiance. Ils sont formés à l'utilisation de la TOE tout comme les utilisateurs.
A.CONSERVATION_CLES	Les utilisateurs sont chargés de la conservation dans un lieu sûr et de la non divulgation des clés d'accès qui leurs ont été transmises par l'administrateur de la sécurité. L'administrateur de la sécurité est également chargé de conservation dans un lieu sûr et de la non divulgation des clés de recouvrement et de son bi-clé de signature.
A.CERTIFICATS	L'administrateur de la TOE est chargé de mettre en œuvre des procédures organisationnelles assurant la protection des certificats lors de leur remise aux utilisateurs. Il est également chargé, lors de la fourniture des clés d'accès possédant un certificat X509, de vérifier la validité de ces certificats et leur adéquation avec l'usage qui en est fait par la TOE.
A.ADMIN_WINDOWS	Les administrateurs Windows sont des personnes de confiance. Les administrateurs Windows de plus haut niveau du domaine Windows sont chargés d'interdire aux administrateurs Windows des sous-niveaux (domaines, contrôleurs de domaines, postes de travail) la modification des « policies » de la TOE. De même, les administrateurs et utilisateurs de la TOE ne doivent pas pouvoir modifier les « policies ».
A.FIDELE_ENV	L'environnement d'exécution (système d'exploitation du poste de l'utilisateur) fournit à la TOE une date et une heure exacte pour assurer les fonctions d'horodatage.
A.ENV_ALEA	L'environnement d'exécution fournit à la TOE des mécanismes (événements partiellement imprédictible) pour produire les aléas nécessaires à la génération des secrets : clés de chiffrement, mot de passe de secours, sels utilisés dans la dérivation PKCS#5.
A.CRYPTO_EXT	Les clés d'accès générées ou stockées à l'extérieur de la TOE doivent être conformes aux documents [CRYPTO_STD] et [CLES_STD] pour le niveau standard.

3.4. Menaces [contre les biens sensibles de la TOE]

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 (couvertes par les Politiques de Sécurité Organisationnelles, services du produit, décrites plus loin). 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.

L'attaquant considéré est doté d'un potentiel d'attaque « enhanced-basic » au sens des Critères Communs.

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 (éteint ou en hibernation) ou le disque. Les biens impactés sont les données de l'utilisateur, le fichier hibernation ainsi que les fichiers de fonctionnement (en confidentialité).

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. Les biens impactés sont les données de l'utilisateur et les clés cryptographiques (en confidentialité).
T.MODIF_AMORÇAGE	Un attaquant manipule le code de pré-boot de la TOE pour capturer les clés d'accès entrées par l'utilisateur lors de la phase d'amorçage ou bien directement les clés de partition déchiffrées par les clés d'accès. Les biens impactés sont les programmes (en intégrité) et les clés cryptographiques (en confidentialité).
T.MODIF_FIC_FONC	Un attaquant modifie les fichiers de fonctionnement de la TOE pour tenter d'accéder aux informations protégées (par exemple il modifie le fichier de contrôle afin de s'ajouter parmi les accès autorisés). Les biens impactés sont donc les fichiers internes de la TOE (intégrité) et indirectement les données utilisateur (confidentialité).

Biens sensibles	Menaces
D.CLES_ACCES	T.ACCES_MEMOIRES, T.MODIF_AMORÇAGE
D.DONNEES_UTILISATEUR	T.ACCES_DONNEES, T.ACCES_MEMOIRES, T.MODIF_FIC_FONC
D.HIBER	T.ACCES_DONNEES
D.CLES_PAR	T.ACCES_ MEMOIRES, T.MODIF_AMORÇAGE
D.PROGRAMMES	T.MODIF_AMORÇAGE
D.FONC	T.ACCES_DONNEES, T.MODIF_FIC_FONC

Tableau 2 Association biens sensibles vers menaces

Note :

- D.CONFIGURATION est couvert par OSP.VERIF_POLICIES (ci-dessous).
- D.ID_ADMIN est couvert par l'hypothèse A.CONSERVATION_CLES

3.5. Politiques de sécurité organisationnelles

OSP.DISQUE	La TOE doit offrir un service de protection en confidentialité (chiffrement), automatique et systématique, du stockage des fichiers sensibles des utilisateurs, ces fichiers ne pouvant être lus (déchiffrés) ou écrits (chiffrés) que par des utilisateurs disposant de clés d'accès valides pour ces fichiers.
OSP.ADMIN_DISQUES	La TOE doit offrir un service de gestion des partitions des disques (chiffrement, déchiffrement et transchiffrement).
OSP.ACCES	La TOE doit permettre aux utilisateurs de fournir une clé d'accès au démarrage du poste de travail permettant d'accéder aux fichiers sensibles stockés sur le disque. S'ils ne peuvent fournir une clé d'accès valide, l'accès doit être rejeté et l'événement correspondant journalisé.

OSP.ADMIN_ACCES	La TOE doit offrir un service de gestion des accès.
OSP.RECOUVREMENT	La TOE doit offrir un service de recouvrement des partitions chiffrées des utilisateurs par l'emploi de clés d'accès de recouvrement gérées par l'administrateur de la TOE. Ces clés sont systématiquement et automatiquement affectées lors du primo chiffrement. La TOE doit également permettre un recouvrement distant (secours utilisateur) si l'utilisateur a oublié son mot de passe ou perdu/cassé son token. Ce secours s'effectue par l'intermédiaire d'une clé systématiquement et automatiquement affectées lors de la création de la liste d'accès de l'utilisateur. Toute opération de recouvrement doit être journalisée.
OSP.COLLECTE	La TOE doit offrir un service de collecte d'information dans un fichier protégé pour les opérations de support. Les informations collectées sont sélectionnables parmi les logs, la configuration, les applications installées etc.
OSP.HIBERNATION	La TOE doit assurer la confidentialité du fichier hibernation ainsi que l'authentification de l'utilisateur à la sortie de la veille prolongée.
OSP.REPRISE	La TOE doit assurer une reprise du processus de chiffrement/déchiffrement/transchiffrement (dont le chiffrement initial du poste) après la survenue d'une coupure de courant ou un plantage système. Cette reprise doit assurer l'intégrité des données et la finalisation correcte du chiffrement.
OSP.AUDIT	La TOE doit permettre la journalisation des événements de sécurité dès la phase d'authentification.
OSP.VERIF_POLICIES	La TOE doit offrir un service (transparent pour l'utilisateur) de vérification de la signature des politiques de sécurité par la clé privée de l'administrateur de sécurité. L'application de toute nouvelle politique est conditionnée par le succès de cette vérification.
OSP.CRYPTO	Les mécanismes cryptographiques de la TOE doivent être conformes aux exigences pour le niveau de robustesse standard des référentiels cryptographiques [CRYPTO_STD] et [CLES_STD] de l'ANSSI. Les mécanismes d'authentification doivent être conformes aux exigences définies dans le document [AUTH_STD].
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.

4. OBJECTIFS DE SÉCURITÉ

4.1. Objectifs de sécurité pour la TOE

4.1.1. Contrôle d'accès

O.ACCES	La TOE doit permettre de visualiser les accès et gérer les clés d'accès.
O.PROTECTION_DES_ DONNEES_ENREGISTREES	La TOE doit s'assurer que l'utilisateur a été authentifié avant de rendre accessibles les données enregistrées. Pour cela, la TOE ne doit autoriser l'accès à l'environnement de travail chiffré qu'après présentation d'une clé d'accès valide au démarrage du poste de travail.
O.ROLES	La TOE doit gérer deux rôles d'utilisateurs : un rôle 'utilisateur normal' ou plus simplement 'utilisateur' (utilisation du poste de travail sous condition de présentation d'une clé d'accès valide) et un rôle 'administrateur' (utilisation, recouvrement, plus possibilité d'administrer le poste, c'est-à-dire gérer ses accès).

4.1.2. 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 [CRYPTO_STD] et [CLES_STD] de l'ANSSI. La TOE doit implémenter les fonctions d'authentification conformément aux exigences définies dans le document [AUTH_STD].
O.CLES_CHIFFREMENT	La TOE doit générer des clés de chiffrement conformément aux exigences pour le niveau de robustesse standard des référentiels cryptographiques [CRYPTO_STD] et [CLES_STD] de l'ANSSI.

4.1.3. Gestion

O.RECOUVREMENT	La TOE doit permettre d'affecter des clés d'accès de recouvrement et de secours.
O.COLLECTE	La TOE doit permettre de collecter de manière sécurisée des informations utiles aux opérations de support.
O.AUDIT	La TOE doit générer des événements en rapport avec son fonctionnement dès la phase de contrôle d'accès.
O.ADM_DISQUES	La TOE doit offrir une interface à l'administrateur, lui permettant de gérer l'état de chiffrement des disques et de leurs partitions.

4.1.4. Protections lors de l'exécution

O.AMORÇAGE	La TOE doit vérifier l'intégrité des fichiers de fonctionnement avant l'amorçage du poste. En cas d'échec lors de la vérification, l'accès aux données ne doit être autorisé qu'à l'administrateur.
O.HIBERNATION	La TOE doit chiffrer le fichier hibernation et imposer l'authentification de l'utilisateur à la sortie de la veille prolongée.
O.INT_POLICIES	La TOE doit vérifier la signature de toutes nouvelles politiques de sécurité à appliquer. En cas d'échec lors de la vérification, les politiques appliquées restent inchangées.
O.ARRET_UTILISATEUR	La TOE doit rendre inaccessibles les données sensibles, en particulier les clés cryptographiques, lorsque l'utilisateur arrête le poste de travail.

O.ROBUSTESSE	L'arrêt subit (intempestif) de la TOE (de l'équipement, du disque) ne doit pas permettre d'accéder aux données sensibles. Par ailleurs toute opération de chiffrement, déchiffrement ou transchiffrement en cours doit être reprise après l'authentification utilisateur puis finalisée sans perte de donnée. *Note d'application* Cet objectif assure que, hors du cadre de fonctionnement nominal, la TOE n'enregistre pas en clair de façon persistante des données qui sont censées être chiffrées. En effet, un arrêt brutal de la TOE peut survenir avant le vol ou la copie de l'image. Dans ce cas, le support serait susceptible de contenir des données utilisateur non chiffrées.

4.2. Objectifs de sécurité pour l'environnement

4.2.1. Pendant l'utilisation

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. L'environnement doit fournir un système d'horodatage fiable qui permettant de dater précisément les événements enregistrés dans le journal.
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.SO_CONF	Les administrateurs de la TOE doivent être des personnes de confiance.
OE.CONSERV_CLES	Les utilisateurs doivent conserver, dans un lieu sûr, les clés d'accès qui leur ont été transmises par un administrateur de la TOE et empêcher leur divulgation. L'administrateur de la TOE doit conserver ses clés de recouvrement dans un lieu sûr et empêcher leur divulgation.
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.
OE.ENV_FIRMWARE	L'environnement d'exploitation en mode EFI contrôle l'intégrité du code

	de démarrage (pré-boot) de la TOE (technologie Secure Boot de Microsoft Windows). La désactivation de cette protection est protégée par l'entrée un mot de passe fort entrée par un administrateur et conforme aux recommandations détaillées dans le document [MOTS_DE_PASSE_STD].
OE.PORT_DMA	Un attaquant pourrait profiter d'une absence de l'utilisateur pour brancher un matériel sur un des ports DMA (Direct Memory Access) afin de récupérer, plus tard, certaines informations sensibles stockées en mémoire après que l'utilisateur ait utilisé son poste. L'administrateur doit donc désactiver l'utilisation des périphériques DMA dans les paramètres de configuration du BIOS de la station de travail.
OE.HORODATAGE	L'environnement d'exploitation fournit à la TOE un horodatage de qualité pour lui permettre d'assurer correctement les fonctions nécessitant une date et une heure exacte (traçage des événements de sécurité notamment).
OE.ENV_ALEA	L'environnement d'exploitation fournit à la TOE des données lui permettant de mettre en œuvre des mécanismes pour fournir les aléas nécessaires à la génération des secrets.

4.2.2. Formation des utilisateurs et des administrateurs

OE.FORMATION	L'administrateur des accès et les utilisateurs de la TOE doivent être formés à l'utilisation de la TOE et sensibilisés à la sécurité informatique (ceci prend en compte la sensibilisation sur la qualité des clés d'accès et de leur support lorsqu'elles sont hébergées par un porte-clés). Les administrateurs de la TOE doivent recevoir une formation adaptée à cette fonction.
OE.CRYPTO_EXT	L'administrateur de la sécurité doit être sensibilisé sur la qualité des clés d'accès qu'il apporte à la TOE afin que ces clés soient conformes à l'état de l'art dans leur implémentation. Il doit également être sensibilisé à la qualité du support de ces clés lorsqu'elles sont hébergées par un porte-clés externe.

4.2.3. Administration

OE.CERTIFICATS	L'administrateur de la TOE est chargé de mettre en œuvre des procédures organisationnelles assurant la protection des certificats lors de leur remise aux utilisateurs. Il est également chargé, lors de la fourniture des clés d'accès possédant un certificat X509, vérifier la validité de ces certificats et leur adéquation avec l'usage qui en est fait par la TOE. Cette exigence s'applique en particulier aux certificats racines dits «authenticode» à partir desquels la vérification d'intégrité de la TOE peut être effectuée.
OE.ADM_ROOT_WINDOWS	Les administrateurs Windows sont des personnes de confiance. Les administrateurs de plus haut niveau du domaine Windows doivent interdire aux administrateurs des sous-niveaux (domaines, contrôleurs de domaines, postes de travail) la modification des « policies » de la TOE. De même, les administrateurs de la TOE ne peuvent modifier les « policies ». En conséquence, ces administrateurs de plus haut niveau doivent eux-mêmes être des personnes de confiance.

5. EXIGENCES DE SÉCURITÉ

5.1. Exigences fonctionnelles de sécurité de la TOE

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

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

Le modèle des exigences fonctionnelles de sécurité (SFR) est résumé dans la figure 2.

Sujets

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

Sujet	Attribut de sécurité	Valeurs possibles
S.API	AT.ROLE	U.USER, U.ADMIN
S.DISK	Etat du disque (AT.STATE)	ENCRYPTED/DECRYPTED
S.DISK	Statut du disque (*AT.STATUS*)	ACTIVATED/DEACTIVATED
S.DISK	Identifiant Disque (*AT.ID*)	Méthode d'identification propriétaire

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

Les termes « DISK » et « disque » sont utilisées pour conserver le vocabulaire du profil de protection [CDISK] mais ces termes génériques désignent en fait un ensemble disque + partition (et pour les systèmes mono disque, qui constituent la plupart des cas d'utilisation, simplement la partition du disque).

Chaque disque géré par la TOE est représenté par un sujet *S.DISK* maintenant un attribut de sécurité AT.STATE indiquant si le disque est chiffré et si c'est le cas 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 (avec le rôle utilisateur ou le rôle administrateur défini lors de la phase d'authentification).

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*)	Méthode d'identification propriétaire
Données utilisateur chiffrées (*OB.UD*)	Identifiant disque associé (*AT.ID*)	Méthode d'identification propriétaire

Objet	Attribut de sécurité	Valeurs possibles
Données d'Authentification (*OB.AD*)	Identifiant disque associé (*AT.ID*)	Méthode d'identification propriétaire
Données d'Authentification (OB.AD)	Identifiant utilisateur (AT.LOGIN)	Nom de login
Données d'Authentification (OB.AD)	Secret utilisateur (AT.SECRET)	Secret utilisateur (mot de passe ou clé privée)

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

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

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

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

Opérations

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

Opération	Sujet	Objet
Création (CREATE)	TSF	S.DISK, OB.AD, OB.KEY
Annulation (CANCEL)	TSF	S.DISK, 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
Gestion des accès (MANAGE)	S.API	OB.AD
Lecture/Écriture/Effacement (DECIPHER/CIPHER/ERASE)	S.API	OB.UD

L'opération *CREATE* correspond intuitivement à la création d'un disque: une clé de chiffrement y est implicitement associée. L'état du disque devient ENCRYPTED.

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. L'administrateur a également la possibilité d'ajouter et de supprimer des objets OB.AD relatifs à un disque (MANAGE). La création d'un disque crée automatiquement un objet OB.AD particulier correspondant à l'accès de recouvrement (configuré dans les politiques de sécurité) ainsi qu'un objet OB.AD relatif à l'accès de secours. Une fois créées, ces données ne sont manipulables (*ACCESS*) que par leur créateur, l'opération *ACCESS* donnant droit à toutes les opérations sur les données appartenant à l'utilisateur (effacement, modification, lecture...).

L'opération CANCEL correspond au déchiffrement d'un disque (on rappelle que ce terme général désigne dans la plupart des cas une partition), la clé de chiffrement est supprimée (mais pas les données d'authentification qui peuvent servir à plusieurs disques), l'état du disque devient DECRYPTED.

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 oeuvre de cette opération entraîne une modification de l'attribut de sécurité S.DISK.STATUS qui prend la valeur DEACTIVATED.

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

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

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

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

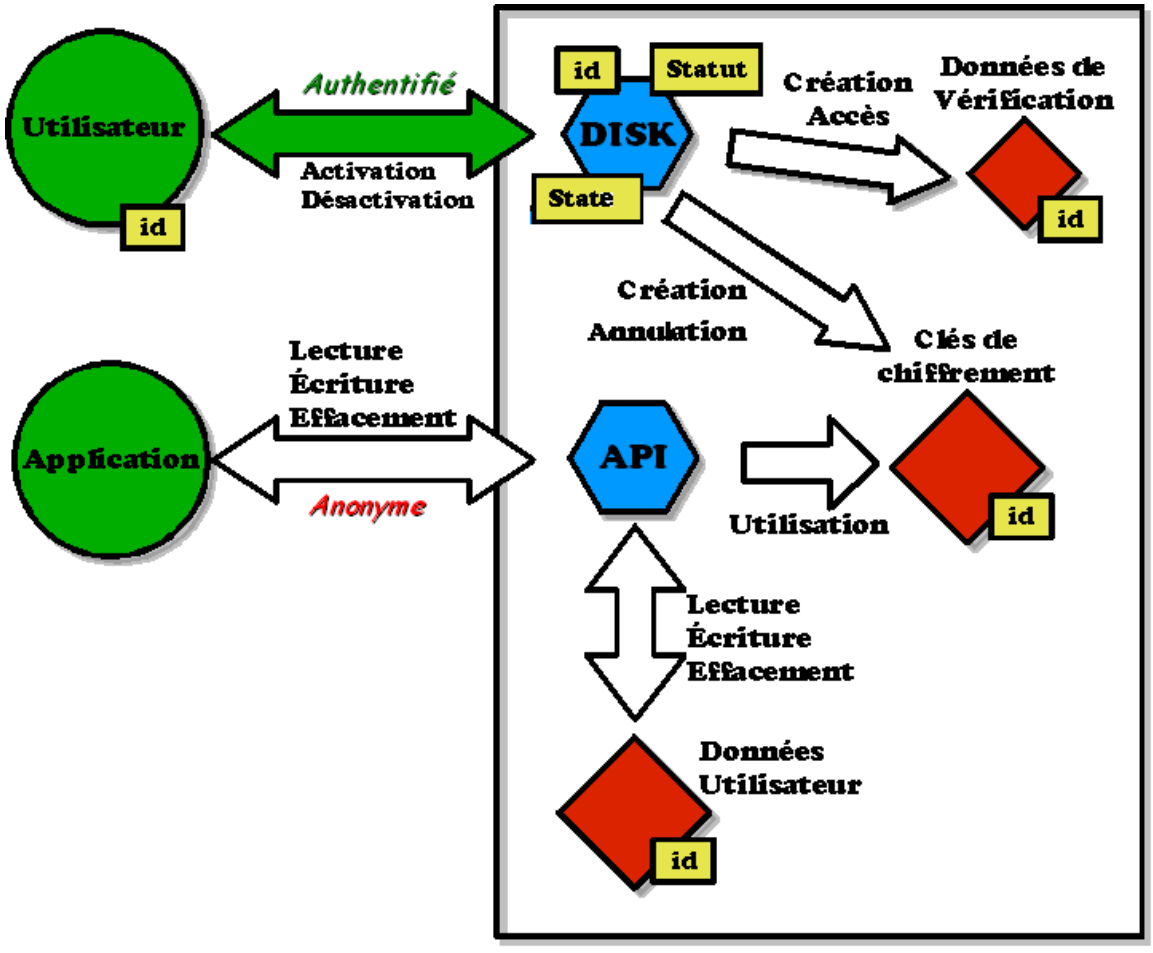

Figure 2 : Résumé de la TSP (l'utilisateur s'authentifie en tant qu'utilisateur ou administrateur)

Utilisateurs

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

U.Admin représente l'administrateur de la TOE.

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

5.1.1. Exigences 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 **minimum** level of audit; and

c)

- **Boot process (including verification of technical files integrity);**
- **Partition encryption and decryption ;**
- **Access management (creation, destruction, modification, recovery, SOS);**
- **Authentication;**
- **Policies and technical files verification.**

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 ST, **no other audit relevant information.**

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. Exigences liées à l'authentification des utilisateurs

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **three** unsuccessful authentication attempts occur related to **pre-boot authentication**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met** or surpassed, the TSF shall **force Windows boot**.

Note d'application :

Le boot forcé va forcément échouer (clé incorrecte) imposant un redémarrage du poste. Le nombre d'échec consécutifs est fixé à 3 par défaut mais est configurable par politiques.

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, MANAGE, USE, DECIPHER, CIPHER, ERASE 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, MANAGE, USE, DECIPHER, CIPHER, ERASE and ACCESS.

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

Note d'application :

L'authentification des utilisateurs peut se faire par une phrase de passe, une clé RSA hébergée dans un porte-clés comme un fichier de clé, une carte à puce, un token USB etc.

5.1.3. Exigences liées à la robustesse de la TOE

FPT_FLS.1 Failure with preservation of secure state

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

- **hot/warm/cold reset of the host machine**
- **when the host machine is switched off (power shortage or power cut)**
- **When the system hibernates**
- **When the operating system crashes during a partition encryption (decryption, encryption, key renewal).**

FPT_SDI_EXT.2 TSF data integrity monitoring and action

FPT_SDI_EXT.2.1 The TSF shall be able to detect [**modification of data, substitution of data, deletion of data**] of [**the TSF technical files**].

FPT_SDI_EXT.2.2 Upon detection of a data integrity error, the TSF shall take the following actions: [**boot authorized to the administrator role only**].

FPT_TST.1 TSF self test

FPT_TST.1.1 The TSF shall run a suite of self tests [**during initial start-up, periodically during normal operation**] to demonstrate the correct operation of [the TSF].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **[no parts of TSF data].**

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **[no parts of TSF].**

5.1.4. Divers

FMT_MSA.3 Static attribute initialisation

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

Raffinement non éditorial:

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

- Rule STATUS: The TSF shall assign the value DEACTIVATED to the security attribute AT.STATUS whenever a S.DISK is created.
- Rule STATE: The TSF shall assign the value DECRYPTED to the security attribute AT.STATE 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 des mécanismes internes propriétaires.

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/Access_Admin Management of security attributes

FMT_MSA.1.1/Access_Admin The TSF shall enforce the **TOE access control policy** to restrict the ability to **add, modify, delete** the security attributes **AT.LOGIN and AT.SECRET** to **U.ADMIN**.

FMT_MSA.1/Disk_Admin Management of security attributes

FMT_MSA.1.1/Disk_Admin The TSF shall enforce the **TOE access control policy** to restrict the ability to **set to decrypted** the security attributes **AT.STATE** to **U.ADMIN**.

FMT_MSA.1/Role_Admin Management of security attributes

FMT_MSA.1.1/Role_Admin The TSF shall enforce the **TOE access control policy** to restrict the ability to **modify** the security attributes **AT.ROLE** to **U.ADMIN**.

FMT_MSA.1/User Management of security attributes

FMT_MSA.1.1/User The TSF shall enforce the **TOE access control policy** to restrict the ability to **change_default, modify** the security attributes **AT.SECRET** to **U.USER**.

FMT_SMR.1 Security management roles

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

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

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **disable, enable** the functions **information gathering, recovery and SOS function** to **U.ADMIN**.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **change_default, modify or, delete** the **policy** to **U.ADMIN**.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **Access management**
- **Disk management**
- **Recovery and SOS functions**
- **Information gathering for Prim'X support**

FDP_ACC.1 Subset access control

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

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

FDP_ACF.1 Security attribute based access control

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

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

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

Rule	Operation	Condition
Rule1	The TSF is allowed to CREATE a S.DISK and the associated OB.KEY and OB.AD	no 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
Rule 7	a subject S.API is allowed to MANAGE an object OB.AD (access management)	The user is authenticated by the TSF based on OB.AD and the value of the security attributes AT.ROLE is U.ADMIN (AT.LOGIN and AT.SECRET management) or the user is authenticated by the TSF based on OB.AD and the value of the security attributes AT.ROLE is U.USER (AT.SECRET change only).
Rule 8	a subject S.DISK is allowed to CANCEL a S.DISK	The user is authenticated by the TSF based on OB.AD, the value of the security attributes AT.ROLE is U.ADMIN (AT.STATE modification) and the value of the security attribute S.DISK.STATE is ENCRYPTED

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

- **Rule9: The TSF shall perform DISMOUNT operation on S.DISK after reboot, power off or hibernation provided the value of the security attribute S.DISK.STATUS is ACTIVATED.**
- **None.**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **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.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **Hash, encryption, decryption, key wrapping and unwrapping, key derivation** in accordance with a specified cryptographic algorithm **SHA-256 and SHA-512, RSA PKCS#1 v2.2, AES modes CBC et XTS** and cryptographic key sizes **128, 192 and 256 bits symmetric keys, 2048, 3072 and 4096 bits asymmetric keys** that meet the following: **ANSSI's cryptographic requirements ([CRYPTO_STD] and [CLES_STD])**.

FDP_RIP.1 Subset residual information protection

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

Raffinement non éditorial:

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

5.1.5. Exigences liées à la génération de clé

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm

- **génération de nombres pseudo-aléatoires utilisés pour la génération des clé de chiffrement et des clés RSA de listes d'accès en utilisant les générateurs Hash_DRBG, HMAC_DRBG ou CTR_DRBG décrit dans la publication « Recommendation for Random Number Generation Using Deterministic Random Bit Generators » (référence SP 800-90A révision 1) du NIST ;**
- **diversification de clés PKCS#5 à partir des mots de passe**

and specified cryptographic key sizes **128, 192 and 256 bits (AES keys), 2048, 3072 and 4096 bits (RSA keys)** that meet the following: **ANSSI's cryptographic requirements ([CRYPTO_STD] and [CLES_STD]).**

Note d'application

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

5.2. Exigences d'assurance de sécurité de la TOE

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 [QUALIF_STD].

Ce qui correspond à la sélection des composants d'assurance suivants :

Composant		Commentaire
ADV_ARC.1	Security architecture description	EAL3
ADV_FSP.3	Functional specification with complete summary	EAL3
ADV_TDS.2	Architectural design	EAL3
AGD_OPE.1	Operational user guidance	EAL3
AGD_PRE.1	Preparative procedures	EAL3
ALC_CMC.3	Authorisation controls	EAL3
ALC_CMS.3	Implementation representation CM coverage	EAL3
ALC_DEL.1	Delivery procedures	EAL3
ALC_DVS.1	Identification of security measures	EAL3
ALC_FLR.3	Systematic flaw remediation	+
ALC_LCD.1	Developer defined life-cycle model	EAL3
ASE_CCL.1	Conformance claims	EAL3
ASE_ECD.1	Extended components definition	EAL3
ASE_INT.1	ST introduction	EAL3
ASE_OBJ.2	Security objectives	EAL3
ASE_REQ.2	Security requirements	EAL3
ASE_SPD.1	Security problem definition	EAL3
ASE_TSS.1	TOE summary specification	EAL3
ATE_COV.2	Analysis of coverage	EAL3
ATE_DPT.1	Testing: basic design	EAL3
ATE_FUN.1	Functional testing	EAL3
ATE_IND.2	Independent testing - sample	EAL3
AVA_VAN.3	Focused vulnerability analysis	+

Tableau 3 : Composants d'assurance de sécurité

6. SPECIFICATIONS GLOBALES DE LA TOE

Les fonctions de sécurité réalisées par la TOE sont décrites dans ce chapitre.

F.CONFIGURATION_TOE **Modification de la configuration de la TOE**

Cette fonction de sécurité couvre l'ensemble des opérations de configuration de la TOE (initialisation et modification) et assure que seules des valeurs sûres de paramètres de configuration peuvent être utilisées. Les données de configuration concernent les «« policies »» de Windows (Group Policies ou mode alternatif) qui sont signées par l'administrateur de sécurité et exploitées par la TOE après vérification de leur signature. Ces données définissent notamment les disques à chiffrer selon des règles, les types d'accès supportés, les algorithmes utilisés, la force des mots de passe, le contrôle des certificats. Si la vérification est correcte, le poste est mis en conformité avec les nouvelles politiques.

F.AUDIT **Audit**

Cette fonction de sécurité assure l'enregistrement des événements liés aux opérations réalisées par la TOE. La journalisation inclut les événements liés à l'authentification (notamment à l'amorçage) et toutes les commandes d'administration, réussies ou non. La journalisation indique l'utilisateur associé à chaque événement.

F.OPERATIONS_CRYPTO **Implémentation des opérations cryptographiques**

Cette fonction de sécurité couvre l'ensemble des opérations cryptographiques mises au service des autres fonctions de sécurité et assure que ces opérations sont réalisées conformément aux exigences de l'ANSSI.

La fonction effectue des tests au démarrage des programmes et de manière périodique pour vérifier le bon fonctionnement des algorithmes et du générateur aléatoire.

F.GESTION_ACCES **Gestion des accès**

Cette fonction de sécurité gère les utilisateurs, leurs accès et les droits qui leur sont associés (on y distingue les rôles utilisateur et administrateur). Un accès correspond à une clé d'accès (une clé cryptographique) que possède un utilisateur et permet d'obtenir les éléments de chiffrement/déchiffrement de la partition. L'administrateur peut ajouter, modifier ou détruire des accès, l'utilisateur ne peut que modifier sa clé d'accès. Cette fonction gère également l'accès de recouvrement qui est un accès particulier ainsi que l'accès de secours permettant de dépanner un utilisateur distant.

F.CONTROLE_ACCES **Contrôle d'accès**

Cette fonction de sécurité constitue l'interface obligatoire pour accéder aux partitions contrôlées par la TOE. La TSF autorise ou refuse l'accès à une partition chiffrée sur la base de la vérification d'un couple identifiant/authentifiant fourni par l'utilisateur de la TOE. Concrètement, la clé d'accès utilisateur (clé RSA ou clé dérivée à partir du mot de passe) permet de déchiffrer les clés de chiffrement des partitions, ce qui implique que l'accès aux données en claires des partitions est cryptographiquement impossible en l'absence des données d'authentification. Par ailleurs c'est l'identifiant qui permet à la TOE de déterminer le rôle associé et de permettre ou interdire certaines actions (gestion des accès par exemple). A noter que plusieurs échecs d'authentification au pré-boot (3 par défaut) conduisent à un échec du boot obligeant l'utilisateur à redémarrer la machine.

F.GESTION_PARTITION **Gestion des partitions**

Cette fonction de sécurité constitue le point d'entrée des opérations sur les partitions conformément au plan de chiffrement défini par l'administrateur sécurité dans les politiques de sécurité (chiffrement, déchiffrement et transchiffrement avec reprise des opérations de manière sûre en cas de problème, affichage des informations sur les partitions). Seules les opérations de déchiffrement et transchiffrement (qui implique un déchiffrement) sont soumises à l'entrée d'une clé d'accès administrateur. Dans la pratique l'opération de primo chiffrement est effectuée par l'utilisateur.

Cette fonction a par ailleurs en charge l'initialisation et la gestion des attributs de sécurité relatifs aux disques/partitions ainsi que l'association entre une partition d'un disque, une clé de chiffrement, les données d'authentification et les données utilisateurs.

F.GESTION_AMORÇAGE_ET_ARRET **Boot et arrêt du système**

Cette fonction prend en charge la vérification de l'intégrité des fichiers techniques de fonctionnement et du code d'amorçage.

Cette fonction assure également le nettoyage des traces de données sensibles dans la mémoire (RAM) ou sur le disque dur dès la fin des opérations réalisées et assure qu'aucune donnée sensible n'est disponible après un arrêt brutal. Cette gestion prend également en compte la protection des données lors du processus d'hibernation.

7. ANNONCES DE CONFORMITE A UN PP

Cette cible est conforme (conformité démontrable selon la définition dans la Partie 1 des Critères Communs) au profil de protection [CDISK] (configuration « avec génération de clé »).

La conformité au profil de protection est discutée en annexe.

8. ARGUMENTAIRE

8.1. Argumentaire pour les objectifs de sécurité

8.1.1. 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 et par O.HIBERNATION qui assure le chiffrement du fichier hibernation.

O.ROBUSTESSE contribue également à contrer cette menace en garantissant qu'aucune donnée utilisateur n'est enregistrée, même temporairement, en clair sur le disque.

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

Enfin, O.CRYPTO garantit que les fonctions de cryptographie mises en 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 la 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.MODIF_AMORÇAGE:

Cette menace est couverte par OE.ENV_FIRMWARE qui vérifie la signature du code de pré-boot EFI dès le chargement.

T.MODIF_FIC_FONC

Cette menace est couverte par O.AMORÇAGE qui assure la vérification de l'intégrité des fichiers techniques de fonctionnement avant l'amorçage.

8.1.2. Politiques de sécurité de l'organisation

OSP.DISQUE:

Cette OSP est couverte par O.PROTECTION_DES_DONNEES_ENREGISTREES qui assure l'authentification utilisateur pour l'accès aux données sensibles, O.CRYPTO et O.CLES_CHIFFREMENT qui garantissent l'utilisation de fonctions cryptographiques conforme au niveau de robustesse visé.

OSP.ADMIN_DISQUES:

Cette OSP est couverte par O.ADM_DISQUES qui offre une interface permettant de gérer les disques et leurs partitions. La gestion des disques est assujettie à une authentification réussie (O.PROTECTION_DES_DONNEES_ENREGISTREES) avec le rôle administrateur (O.ROLES) et est tracée dans le journal des événements (O.AUDIT).

OSP.ACCES:

Cette OSP est couverte par O.PROTECTION_DES_DONNEES_ENREGISTREES qui fait en sorte que seule une clé d'accès valide puisse permettre de retrouver les clés de chiffrement des partitions permettant l'accès à l'environnement de travail chiffré et par O.AUDIT qui trace tous les échecs d'authentification dans le journal des événements.

OSP.ADMIN_ACCES:

Cette OSP est couverte par O.ACCES qui offre une interface permettant de visualiser et gérer les accès. La gestion des accès est assujettie à une authentification réussie (O.PROTECTION_DES_DONNEES_ENREGISTREES) avec le rôle administrateur (O.ROLES) et tracés dans le journal des événements (O.AUDIT).

OSP.RECOUVREMENT:

Cette OSP est couverte par O.RECOUVREMENT qui assure l'affectation de clés de recouvrement et de secours. Le recouvrement et le secours sont uniquement réservés au rôle Administrateur de la TOE (géré par O.ROLES) et assujettie à une authentification réussie de celui-ci (O.PROTECTION_DES_DONNEES_ENREGISTREES). L'opération est tracée dans le journal des événements (O.AUDIT).

OSP.COLLECTE :

Cette OSP est couvert par O.COLLECTE qui offre une interface à l'administrateur lui permettant de collecter les informations avec O.PROTECTION_DES_DONNEES_ENREGISTREES pour le contrôle d'accès à ces données.

OSP.HIBERNATION:

Cette OSP est couverte par O.HIBERNATION qui garantit la confidentialité du fichier d'hibernation (chiffrement assuré par O.CRYPTO) et impose l'authentification utilisateur pour y accéder (gérée par O.PROTECTION_DES_DONNEES_ENREGISTREES).

OSP.REPRISE:

Cette OSP est directement couverte par O.ROBUSTESSE qui assure la finalisation correcte des opérations de chiffrement (déchiffrement, transchiffrement) après une coupure brutale.

OSP.VERIF_POLICIES:

Cette OSP est directement couverte par O.INT_POLICIES qui vérifie la signature des nouvelles politiques de sécurité appliquées et refuse leur application si la signature est incorrecte.

OSP.AUDIT:

Cette OSP est directement couverte par O.AUDIT qui garantit la journalisation de tous les événements de sécurité. OE.ENV_OPERATIONNEL.1 fournit l'horodatage appliqué aux enregistrements.

OSP.CRYPTO:

Cette OSP est directement couverte par les objectifs O.CRYPTO et O.CLES_CHIFFREMENT.

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.

8.1.3. Hypothèses

A.NON_OBSERV:

Cette hypothèse est directement couverte par OE.ENV_OPERATIONNEL.2 qui garantit la prise de précaution lors de la saisie des secrets utilisateur.

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. Par ailleurs OE.ENV_OPERATIONNEL.1 apporte l'horodatage nécessaire à la journalisation des événements.

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.FIRMWARE :

L'objectif OE.ENV_FIRMWARE couvre directement cette hypothèse par la vérification de la signature du code de pré-boot EFI dès le chargement et par l'impossibilité de désactiver cette protection.

A.PORT_DMA :

L'objectif OE.PORT_DMA couvre directement cette hypothèse en imposant à l'administrateur de désactiver l'utilisation des ports DMA.

A.CONFIANCE_ADM_TOE:

Les objectifs OE.SO_CONF et OE.FORMATION couvrent directement cette hypothèse en employant des personnes de confiance et en leur apportant la formation nécessaire.

A.CONSERVATION_CLES:

Les objectifs OE.CONSERV_CLES et OE.FORMATION couvrent cette hypothèse en responsabilisant et en sensibilisant les utilisateurs et les administrateurs.

A.CERTIFICATS:

L'objectif OE.CERTIFICATS couvre directement cette hypothèse en assurant que l'administrateur utilise des procédures organisationnelles adaptées pour la gestion des certificats.

A.ADMIN_WINDOWS:

L'objectif OE.ADM_ROOT_WINDOWS couvre directement cette hypothèse en séparant les rôles des administrateurs Windows des différents niveaux et en s'assurant de leur confiance.

A.FIDELE_ENV:

L'objectif OE.HORODATAGE couvre directement cette hypothèse en assurant que l'utilisateur vérifie régulièrement le bon fonctionnement de l'horloge du poste de travail fournie par le système d'exploitation.

A.ENV_ALEA:

L'objectif OE.ENV_ALEA couvre directement cette hypothèse en fournissant les données permettant à la TOE de mettre en œuvre des mécanismes pour générer les aléas.

A.CRYPTO_EXT:

L'objectif OE.CRYPTO_EXT couvre directement cette hypothèse en garantissant la qualité des clés d'authentification RSA générées et gérées à l'extérieur de la TOE.

8.1.4. Tables de couverture entre définition du problème et objectifs de sécurité

Menaces	Objectifs de sécurité	Argumentaire
T.ACCES_DONNEES	O.ROBUSTESSE, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.CRYPTO, O.CLES_CHIFFREMENT, O.ARRET_UTILISATEUR, O.HIBERNATION	Section 8.1.1
T.ACCES_MEMOIRES	O.ARRET_UTILISATEUR	Section 8.1.1
T.MODIF_AMORÇAGE	OE.ENV_FIRMWARE	Section 8.1.2
T.MODIF_FIC_FONC	O.AMORÇAGE	Section 8.1.2

Tableau 4 Association menaces vers objectifs de sécurité

Objectifs de sécurité	Menaces
O.ACCES	-
O.PROTECTION_DES_DONNEES_ENREGISTREES	T.ACCES_DONNEES
O.ROLES	-
O.CRYPTO	T.ACCES_DONNEES
O.CLES_CHIFFREMENT	T.ACCES_DONNEES
O.RECOUVREMENT	-
O.AUDIT	-
O.ADM_DISQUES	-
O.AMORÇAGE	T.MODIF_FIC_FONC
O.HIBERNATION	T.ACCES_DONNEES
O.INT_POLICIES	
O.ARRET_UTILISATEUR	T.ACCES_DONNEES, T.ACCES_MEMOIRES
O.ROBUSTESSE	T.ACCES_DONNEES
OE.ENV_OPERATIONNEL.1	-
OE.ENV_OPERATIONNEL.2	-
OE.SO_CONF	-
OE.CONSERV_CLES	-
OE.NON_REMANENCE_1	-

Objectifs de sécurité	Menaces
OE.NON_REMANENCE_2	-
OE.HORODATAGE	-
OE.ENV_ALEA	-
OE.ENV_FIRMWARE	T.MODIF_AMORÇAGE
OE.PORT_DMA	-
OE.FORMATION	-
OE.CRYPTO_EXT	-
OE.CERTIFICATS	-
OE.ADM_ROOT_WINDOWS	-

Tableau 5 Association objectifs de sécurité vers menaces

Politiques de sécurité organisationnelles (OSP)	Objectifs de sécurité	Argumentaire
OSP.DISQUE	O.PROTECTION_DES_DONNEES_ENREGISTREES, O.CRYPTO, O.CLES_CHIFFREMENT	Section 8.1.2
OSP.ADMIN_DISQUES	O.ADM_DISQUES, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.ROLES, O.AUDIT	Section 8.1.2
OSP.ACCES	O.PROTECTION_DES_DONNEES_ENREGISTREES, O.AUDIT	Section 8.1.2
OSP.ADMIN_ACCES	O.ACCES, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.ROLES, O.AUDIT	Section 8.1.2
OSP.RECOUVREMENT	O.RECOUVREMENT, O.ROLES, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.AUDIT	Section 8.1.2
OSP.COLLECTE	O.COLLECTE, O.PROTECTION_DES_DONNEES_ENREGISTREES	Section 8.1.2
OSP.HIBERNATION	O.HIBERNATION, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.CRYPTO	Section 8.1.2
OSP.REPRISE	O.ROBUSTESSE	Section 8.1.2
OSP.AUDIT	O.AUDIT, OE.ENV_OPERATIONNEL.1	Section 8.1.2
OSP.VERIF_POLICIES	O.INT_POLICIES	Section 8.1.2

Politiques de sécurité organisationnelles (OSP)	Objectifs de sécurité	Argumentaire
OSP.CRYPTO	O.CRYPTO, O.CLES_CHIFFREMENT	Section 8.1.2
OSP.NON_REMANENCE_2	OE.NON_REMANENCE_2	Section 8.1.2

Tableau 6 Association politiques de sécurité organisationnelles vers objectifs de sécurité

Objectifs de sécurité	Politiques de sécurité organisationnelles (OSP)
O.ACCES	OSP.ADMIN_ACCES
O.PROTECTION_DES_DONNEES_ENREGISTREES	OSP.DISQUE, OSP.ADMIN_DISQUES, OSP.ACCES, OSP.ADMIN_ACCES, OSP.RECOUVREMENT, OSP.HIBERNATION, OSP.COLLECTE
O.ROLES	OSP.ADMIN_DISQUES, OSP.ADMIN_ACCES, OSP.RECOUVREMENT
O.CRYPTO	OSP.CRYPTO, OSP.DISQUE, OSP.HIBERNATION
O.CLES_CHIFFREMENT	OSP.CRYPTO, OSP.DISQUE
O.RECOUVREMENT	OSP.RECOUVREMENT
O.COLLECTE	OSP.COLLECTE
O.AUDIT	OSP.ADMIN_DISQUES, OSP.ACCES, OSP.AUDIT OSP.ADMIN_ACCES, OSP.RECOUVREMENT
O.ADM_DISQUES	OSP.ADMIN_DISQUES
O.AMORÇAGE	-
O.HIBERNATION	OSP.HIBERNATION
O.INT_POLICIES	OSP.VERIF_POLICIES
O.ARRET_UTILISATEUR	-
O.ROBUSTESSE	OSP.REPRISE
OE.ENV_OPERATIONNEL.1	OSP.AUDIT
OE.ENV_OPERATIONNEL.2	-
OE.HORODATAGE	-
OE.ENV_ALEA	-
OE.ENV_FIRMWARE	-
OE.SO_CONF	-
OE.CONSERV_CLES	-
OE.NON_REMANENCE_1	-
OE.NON_REMANENCE_2	OSP.NON_REMANENCE_2
OE.FORMATION	-

Objectifs de sécurité	Politiques de sécurité organisationnelles (OSP)
OE.CRYPTO_EXT	-
OE.CERTIFICATS	-
OE.ADM_ROOT_WINDOWS	-

Tableau 7 Association objectifs de sécurité vers politiques de sécurité organisationnelles

Hypothèses	Objectifs de sécurité pour l'environnement opérationnel	Argumentaire
A.NON_OBSERV	OE.ENV_OPERATIONNEL.2	Section 8.1.3
A.ENV_OPERATIONNEL	OE.ENV_OPERATIONNEL.1, OE.ENV_OPERATIONNEL.2	Section 8.1.3
A.NON_REMANENCE_1	OE.NON_REMANENCE_1	Section 8.1.3
A.FIRMWARE	OE.ENV_FIRMWARE	Section 8.1.3
A.PORT_DMA	OE.PORT_DMA	Section 8.1.3
A.CONFIANCE_ADM_TOE	OE.SO_CONF, OE.FORMATION	Section 8.1.3
A.CONSERVATION_CLES	OE.CONSERV_CLES, OE.FORMATION	Section 8.1.3
A.CERTIFICATS	OE.CERTIFICATS	Section 8.1.3
A.ADMIN_WINDOWS	OE.ADM_ROOT_WINDOWS	Section 8.1.3
A.FIDELE_ENV	OE.HORODATAGE	Section 8.1.3
A.ENV_ALEA	OE.ENV_ALEA	Section 8.1.3
A.CRYPTO_EXT	OE.CRYPTO_EXT	Section 8.1.3

Tableau 8 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, A.NON_OBSERV
OE.SO_CONF	A.CONFIANCE_ADM_TOE
OE.CONSERV_CLES	A.CONSERVATION_CLES
OE.NON_REMANENCE_1	A.NON_REMANENCE_1
OE.NON_REMANENCE_2	-
OE.HORODATAGE	A.FIDELE_ENV

Objectifs de sécurité pour l'environnement opérationnel	Hypothèses
OE.ENV_ALEA	A.ENV_ALEA
OE.ENV_FIRMWARE	A.FIRMWARE
OE.PORT_DMA	A.PORT_DMA
OE.FORMATION	A.CONFIANCE_ADM_TOE, A.CONSERVATION_CLES
OE.CERTIFICATS	A.CERTIFICATS
OE.ADM_ROOT_WINDOWS	A.ADMIN_WINDOWS
OE.CRYPTO_EXT	A.CRYPTO_EXT

Tableau 9 Association objectifs de sécurité pour l'environnement opérationnel vers hypothèses

8.2. Argumentaire pour les exigences de sécurité

8.2.1. Objectifs

O.ACCES:

La TOE offre des fonctions de gestions des accès (FMT_SMF.1) basée sur des attributs de sécurité gérés conformément à FMT_MSA.1/Access_Admin, FMT_MSA.1/Role_Admin et FMT_MSA.1/User.

La TOE limite l'accès à ces fonctions de gestion des accès en fonction du rôle associé aux utilisateurs (FMT_SMR.1) et de la politique d'accès (FDP_ACC.1 et FDP_ACF.1).

Toutes les opérations sur les accès sont journalisées (FAU_GEN.1 et FAU_GEN.2).

O.ROLES:

La TOE doit gérer et distinguer les rôles d'administrateur de la TOE et d'utilisateur de la TOE (FMT_SMR.1) et restreindre aux administrateurs certaines fonctions d'administration de la sécurité (FMT_SMF.1) et la gestion des « policies » (FMT_MTD.1) ainsi que la possibilité de pouvoir utiliser ou non l'accès de recouvrement (FMT_MOF.1).

Le rôle est déterminé par la TOE lors de la phase de contrôle d'accès (FDP_ACC.1 et FDP_ACF.1) en fonction de l'identification de la personne s'authentifiant (FIA_UID.1).

O.ARRET_UTILISATEUR:

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

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

O.CRYPTO:

Cet objectif est couvert par FCS_COP.1, qui assure que toutes les opérations cryptographiques doivent obéir aux exigences des référentiels cryptographiques de l'ANSSI pour le niveau de robustesse standard ([CRYPTO_STD] et [CLES_STD]). La TOE doit exécuter des auto tests pour vérifier le bon fonctionnement des algorithmes cryptographiques (FPT_TST_TST.1). Les opérations de chiffrement, déchiffrement et transchiffrement sont journalisées (FAU_GEN.1 et FAU_GEN.2).

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.

Les données utilisateurs sont chiffrées conformément au référentiel de l'ANSSI (FCS_COP.1) évitant les attaques par force brute sur tout ou partie des disques.

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

D'autre part, les exigences liées à l'authentification obligatoire d'un utilisateur avant l'activation d'un disque (FIA_UID.1 et FIA_UAU.1) assurent que seul l'utilisateur légitime contrôle l'accès aux données qui y sont enregistrées. La TOE assure une règle de ralentissement forte lors de l'entrée de la clé d'accès, en effet 3 échecs d'authentification (valeur par défaut) imposent un redémarrage complet du poste (FIA_AFL.1). Toute tentative d'authentification (succès ou 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 et FMT_MSA.1/ID).

O.ROBUSTESSE:

Cet objectif est couvert par les exigences qui assurent que toute interruption de la TOE, fortuite (FPT_FLS.1), automatique ou délibérée (FDP_ACF.1), laissent la TOE, et surtout les données qu'elle protège, dans un état robuste, à savoir un état où les disques concernés sont désactivés ; autrement dit, les clés de chiffrement ne sont plus accessibles hors-fonctionnement. Dans le cas d'un arrêt brusque lors du chiffrement (déchiffrement/transchiffrement) en cours d'une partition (chiffrement initial notamment), FPT_FLS.1 assure également que l'état permettra de reprendre l'opération sans perte de données utilisateur.

O.RECOUVREMENT:

La TOE doit permettre de restreindre aux administrateurs (FMT_MOF.1 associé au rôle défini dans FMT_SMR.1) les fonctions de recouvrement et de secours spécifiées dans (FMT_SMF.1). Cette opération quand elle a lieu est journalisée (FAU_GEN.1 et FAU_GEN.2).

O.COLLECTE :

La TOE doit permettre de restreindre aux administrateurs (FMT_MOF.1 associé au rôle défini dans FMT_SMR.1) l'activation ou la désactivation de la fonction de collecte d'information (FMT_SMF.1).

O.AUDIT:

La TOE, lors des opérations de gestion et d'utilisation du produit, doit générer des événements dans le journal d'audit du système d'exploitation (FAU_GEN.1) et associer l'identité de l'utilisateur à chaque événement inscrit dans ce journal (FAU_GEN.2).

O.ADM_DISQUES:

La TOE offre des fonctions de gestions des disques (FMT_SMF.1) basée sur des attributs de sécurité gérés conformément à FMT_MSA.1/Disk_Admin qui permet à l'administrateur de déchiffrer ou transchiffrer (déchiffrement suivi d'un chiffrement) un disque.

La TOE limite l'accès à ces fonctions de gestion des disques en fonction du rôle associé aux utilisateurs (FMT_SMR.1) et de la politique d'accès (FDP_ACC.1 et FDP_ACF.1).

Toutes les opérations sur les accès sont journalisées (FAU_GEN.1 et FAU_GEN.2).

O.AMORÇAGE:

La TOE vérifie (avant l'amorçage) l'intégrité des fichiers techniques de fonctionnement (FPT_SDI_EXT.2) conformément aux algorithmes et tailles de clés cryptographique spécifiés (FCS_COP.1).

Les opérations d'amorçage sont journalisées (FAU_GEN.1 et FAU_GEN.2).

O.HIBERNATION:

Pendant la phase d'hibernation proprement dite, cet objectif est couvert par FCS_COP.1 qui réalise le chiffrement du fichier hibernation et par FDP_RIP.1 qui assure la destruction des données résiduelles. Au réveil, l'accès aux données est conditionné par l'authentification utilisateur assurée par Le contrôle d'accès (FDP_ACC.1 et FDP_ACF.1)

O.INT_POLICIES :

La TOE doit vérifier que la signature utilisée a bien été effectuée par l'administrateur de la sécurité qui est seul autorisé à modifier les politiques de sécurité (FMT_MTD.1). Les opérations de vérification de signature sont effectuées conformément aux algorithmes et tailles de clés cryptographique spécifiés (FCS_COP.1).

O.CLES_CHIFFREMENT:

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

8.2.2. Tables de couverture entre objectifs et exigences de sécurité

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.ACCES	FMT_SMR.1, FMT_SMF.1, FAU_GEN.1, FAU_GEN.2, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1/Access_Admin, FMT_MSA.1/Role_Admin, FMT_MSA.1/User	Section 8.2.1
O.ROLES	FMT_SMR.1, FMT_MTD.1, FMT_SMF.1, FMT_MOF.1, FDP_ACC.1, FDP_ACF.1, FIA_UID.1	Section 8.2.1
O.ARRET_UTILISATEUR	FDP_ACC.1, FDP_ACF.1, FDP_RIP.1	Section 8.2.1
O.CRYPTO	FCS_COP.1, FAU_GEN.1, FAU_GEN.2, FPT_TST.1	Section 8.2.1
O.PROTECTION_DES_DONNEES_ENREGISTREES	FDP_ACF.1, FIA_AFL.1, 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, FCS_COP.1	Section 8.2.1
O.ROBUSTESSE	FPT_FLS.1, FDP_ACF.1	Section 8.2.1
O.RECOUVREMENT	FMT_MOF.1, FMT_SMR.1, FMT_SMF1, FAU_GEN.1, FAU_GEN.2	Section 8.2.1
O.COLLECTE	FMT_MOF.1, FMT_SMR.1, FMT_SMF1	Section 8.2.1
O.AUDIT	FAU_GEN.1, FAU_GEN.2	Section 8.2.1
O.ADM_DISQUES	FMT_SMR.1, FMT_SMF.1, FAU_GEN.1, FAU_GEN.2, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1/Disk_Admin	Section 8.2.1
O.AMORÇAGE	FCS_COP.1, FPT_SDI_EXT.2, FAU_GEN.1, FAU_GEN.2,	Section 8.2.1
O.HIBERNATION	FCS_COP.1, FDP_RIP.1, FDP_ACC.1, FDP_ACF.1	Section 8.2.1
O.INT_POLICIES	FMT_MTD.1, FCS_COP.1	Section 8.2.1
O.CLES_CHIFFREMENT	FCS_CKM.1	Section 8.2.1

Tableau 10 Association objectifs de sécurité de la TOE vers les exigences fonctionnelles

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FAU_GEN.1	O.ACCES, O.CRYPTO, O.AUDIT, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.RECOUVREMENT, O.AMORÇAGE, O.ADM_DISQUES
FAU_GEN.2	O.ACCES, O.CRYPTO, O.AUDIT, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.RECOUVREMENT, O.AMORÇAGE, O.ADM_DISQUES
FIA_AFL.1	O.PROTECTION_DES_DONNEES_ENREGISTREES
FIA_UID.1	O.PROTECTION_DES_DONNEES_ENREGISTREES, O.ROLES
FIA_UAU.1	O.PROTECTION_DES_DONNEES_ENREGISTREES
FPT_FLS.1	O.ROBUSTESSE
FPT_SDI_EXT.2,	O.AMORÇAGE
FPT_TST.1	O.CRYPTO
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/Access_Admin	O.ACCES
FMT_MSA.1/Role_Admin	O.ACCES
FMT_MSA.1/Disk_Admin	O.ADM_DISQUES
FMT_MSA.1/User	O.ACCES
FMT_SMR.1	O.ACCES, O.ROLES, O.RECOUVREMENT, O.COLLECTE, O.ADM_DISQUES
FMT_MOF.1	O.RECOUVREMENT, O.COLLECTE, O.ROLES
FMT_MTD.1	O.INT_POLICIE, O.ROLES
FMT_SMF.1	O.ACCES, O.RECOUVREMENT, O.COLLECTE, O.ROLES, O.ADM_DISQUES
FDP_ACC.1	O.ARRET_UTILISATEUR, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.HIBERNATION, O.ROLES, O.ACCES, O.ADM_DISQUES
FDP_ACF.1	O.ARRET_UTILISATEUR, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.ROBUSTESSE, O.HIBERNATION, O.ROLES, O.ACCES, O.ADM_DISQUES
FCS_COP.1	O.CRYPTO, O.HIBERNATION, O.INT_POLICIES, O.PROTECTION_DES_DONNEES_ENREGISTREES, O.AMORÇAGE
FDP_RIP.1	O.ARRET_UTILISATEUR, O.HIBERNATION
FCS_CKM.1	O.CLES_CHIFFREMENT

Tableau 11 Association exigences fonctionnelles vers objectifs de sécurité de la TOE

8.3. Spécifications globales / Exigences de sécurité

8.3.1. Exigences de sécurité

FAU_GEN.1 :

La TOE permet de générer des données d'audit à partir des événements suivants:

- Le rapport d'audit de la fonction d'amorçage (F.GESTION_AMORÇAGE_ET_ARRET)
- Les opérations diverses sur les partitions : chiffrement, déchiffrement, transchiffrement, reprise après coupure brutale (F.GESTION_PARTITION),
- Les opérations relatives aux accès : succès et échec d'authentification (F.CONTROLE_ACCESS), modification des accès (F.GESTION_ACCES).
- La vérification de la signature des politiques de sécurité (F. CONFIGURATION_TOE)

Ces données sont ensuite enregistrées dans le journal d'audit du système (F.AUDIT).

FAU_GEN.2 :

Outre les paramètres (ex : date et heure) gérés par les fonctions de sécurité traçant des évènements (FAU_GEN.1), c'est F.AUDIT qui gère l'association entre l'événement et l'utilisateur associé. Pour cela la TOE s'appuie sur F.CONTROLE_ACCES qui collecte l'identifiant de l'utilisateur lors de la phase d'authentification.

FIA_AFL.1:

Le nombre maximum d'essai de mots de passe ou de code confidentiel autorisés lors de l'entrée de la clé d'accès au pré-boot est fixé à trois par défaut. Une fois atteint ce nombre, le boot Windows est quand même forcé et échoue. L'utilisateur doit recommencer sa demande d'authentification après avoir redémarré le poste (ce qui le ralenti fortement entre ses différentes séquences d'essais).

La fonction de sécurité F.CONTROLE_ACCES couvre cette fonctionnalité.

FIA_UID.1 :

Cette exigence fonctionnelle est implémentée par F.CONTROLE_ACCES qui contrôle l'accès aux partitions permises et affecte le rôle en fonction de l'identifiant utilisateur. F.GESTION_ACCES intervient également en implémentant la fonction de gestion des utilisateurs et de leurs droits associés et donc en particulier des identifiants (création, suppression). Enfin F.CONFIGURATION_TOE permet la configuration des accès autorisés aux partitions (type d'accès, force des mots de passe, type de certificat …).

FIA_UAU.1 :

Cette exigence fonctionnelle est implémentée par F.CONTROLE_ACCES qui contrôle l'accès aux partitions permises à partir du secret fourni par l'utilisateur. F.GESTION_ACCES intervient également en implémentant la fonction de gestion des utilisateurs (création, suppression, changement du secret). Enfin F.CONFIGURATION_TOE permet la configuration des accès autorisés aux partitions (type d'accès, force des mots de passe, type de certificat …).

FPT_FLS.1 :

La non accessibilité des données sensibles en mémoire ou sur le disque après une interruption brutale (coupure de courant par exemple) ou volontaire (hibernation ou arrêt par l'utilisateur) est entièrement contrôlé par F.GESTION_AMORÇAGE_ET_ARRET qui assure la protection des données sensibles de la TOE et de l'utilisateur après l'arrêt du système hôte. Cette fonction assure également la reprise sans perte de données des opérations cryptographiques de chiffrement (déchiffrement/transchiffrement) d'une partition, notamment le chiffrement initial, survenant après une coupure.

FPT_SDI_EXT.2 :

Cette exigence fonctionnelle est mise en œuvre par la fonction de sécurité F.OPERATIONS_CRYPTO qui implémentent toutes les fonctions nécessaires au contrôle de l'intégrité des fichiers de fonctionnement (calcul de la clé de scellement, calcul de HMAC).

FPT_TST.1:

Les tests cryptographiques réalisés au démarrage de la TOE ou périodiquement pour vérifier le bon fonctionnement du générateur aléatoire et la conformité des algorithmes est assuré par F.OPERATIONS_CRYPTO.

FMT_MSA.3 :

L'initialisation des attributs de sécurité relatifs aux partitions des disques ainsi que l'association entre la partition d'un disque, une clé de chiffrement, les données d'authentification et les données utilisateurs est entièrement assuré par F.GESTION_PARTITION. La fonction F.GESTION_ACCES assure que la force des clés ou mots de passe entrés satisfont à des valeurs minimales imposées.

FMT_MSA.1/Disk_status :

Le statut du disque est modifié lors de la phase de contrôle de la clé d'accès (ouverture des partitions si la clé est valide), cette fonction est donc entièrement assuré par F.CONTROLE_ACCES qui garantit que seul la TSF peut manipuler cette attribut.

FMT_MSA.1/ID :

L'association entre une partition d'un disque, une clé de chiffrement, les données d'authentification et les données utilisateurs est entièrement assuré par F.GESTION_ACCES et F.GESTION_PARTITION qui garantit que seul la TSF peut manipuler ces attributs.

FMT_MSA.1/Access_Admin :

La gestion des accès par l'administrateur est assurée par F.GESTION_ACCES qui lui permet de créer, de supprimer voire de modifier les accès des utilisateurs.

FMT_MSA.1/Disk_Admin :

La gestion des disques par l'administrateur est assuré par F.GESTION_PARTITION qui lui permet de déchiffrer ou transchiffrer (déchiffrement puis chiffrement) les disques.

FMT_MSA.1/Role_Admin :

La gestion des accès par l'administrateur est assurée par F.GESTION_ACCES qui lui permet de modifier le rôle d'un accès.

FMT_MSA.1/User :

La gestion de son propre accès par l'utilisateur est assurée par F.GESTION_ACCES qui lui permet de modifier son secret.

FMT_SMR.1:

La TOE supporte les rôles utilisateur et administrateur (ainsi que la TSF pour la gestion des attributs associés aux partitions).

Cette exigence est entièrement implémentée par F.GESTION_ACCES qui gère les utilisateurs et de leurs droits associés ainsi que par F.GESTION_PARTITION qui détermine les actions de la TSF sur les partitions.

FMT_MOF.1:

Seul l'administrateur de la TOE peut activer ou désactiver la fonction de collecte d'information, de recouvrement et de secours.

La fonction de sécurité F.CONFIGURATION_TOE implémente cette exigence. Une politique de sécurité spécifique (signée par l'administrateur de la sécurité) permet d'activer et désactiver la possibilité d'utiliser l'accès de recouvrement et de secours (indépendamment).

FMT_MTD.1:

Seuls l'administrateur de la sécurité a la possibilité de gérer les stratégies de sécurité (ou « policies).

Cette exigence est implémentée par la fonction de sécurité F.CONFIGURATION_TOE qui vérifie la signature des politiques à appliquer.

FMT_SMF.1:

La TOE permet de réaliser:

- Les fonctions de gestion des disques
- Les fonctions de gestion des accès
- Les fonctions de recouvrement et de secours
- La fonction de collecte d'information

Cette exigence fonctionnelle est implémentée par la fonction de sécurité F.CONTROLE_ACCES et F.GESTION_ACCES (le recouvrement et le mot de passe de secours sont des accès particuliers), F.GESTION_PARTITION et F.CONFIGURATION_TOE (activation ou non des fonctions de recouvrement et de secours), F.OPERATIONS_CRYPTO (collecte d'information).

FDP_ACC.1:

La politique de contrôle d'accès (rôles et opérations permises) est définie par F.GESTION_ACCES et implémentée par F.CONTROLE_ACCES.

FDP_ACF.1:

Les règles régissant la politique de contrôle d'accès sont entièrement définies par F.GESTION_ACCES et implémentées par F.CONTROLE_ACCES. Les actions permises en fonction du rôle sont décrites dans F.GESTION_PARTITION.

FCS_COP.1:

La fonction de sécurité F.OPERATIONS_CRYPTO implémente les opérations cryptographiques mises au service des autres fonctions :

- Chiffrement, déchiffrement et transchiffrement des partitions
- Enveloppement (wrapping) et désenveloppement (unwrapping) des clés de chiffrement par des clés AES
- Enveloppement (wrapping) des clés de chiffrement par des clés publiques RSA et désenveloppement (unwrapping) par des clés privées RSA.
- Dérivation de clé (accès par mot de passe)
- Vérification de la signature des politiques et des fichiers de fonctionnement

FDP_RIP.1:

Le démontage du disque (au sens de [CDISK], en fait l'arrêt, le reboot ou la mise en hibernation) s'accompagne d'un effacement des données sensibles en mémoire.

La fonction de sécurité F.GESTION_AMORÇAGE_ET_ARRET assure la destruction des données sensibles de la TOE et de l'utilisateur en mémoire RAM lors du démontage du ou des disques.

FCS_CKM.1:

A chaque partition chiffrée est associée une clé de chiffrement (AES). Cette clé est tirée lors de la création du premier accès utilisateur.

Lors de l'entrée d'un mot de passe par l'utilisateur (y compris le mot de passe de secours), une clé d'accès est générée (dérivée) par la TOE à partir de ce mot de passe conformément au standard PKCS#5.

La fonction de sécurité F.OPERATIONS_CRYPTO implémente cette exigence fonctionnelle.

8.3.2. Tables de couverture entre exigences fonctionnelles de sécurité et spécifications globales

Exigences fonctionnelles de sécurité	Spécifications globales	Argumentaire
FAU_GEN.1	F.GESTION_PARTITION, F.CONTROLE_ACCES, F.GESTION_ACCES, F.CONFIGURATION_TOE, F.AUDIT, F.GESTION_AMORÇAGE_ET_ARRET	Section 8.3.1
FAU_GEN.2	F.CONTROLE_ACCES, F.AUDIT	Section 8.3.1

Exigences fonctionnelles de sécurité	Spécifications globales	Argumentaire
FIA_AFL.1	F.CONTROLE_ACCES	Section 8.3.1
FIA_UID.1	F.CONTROLE_ACCES, F.GESTION_ACCES, F.CONFIGURATION_TOE	Section 8.3.1
FIA_UAU.1	F.CONTROLE_ACCES, F.GESTION_ACCES, F.CONFIGURATION_TOE	Section 8.3.1
FPT_FLS.1	F.GESTION_AMORÇAGE_ET_ARRET	Section 8.3.1
FPT_SDI_EXT.2	F.OPERATIONS_CRYPTO, F.GESTION_AMORÇAGE_ET_ARRET	Section 8.3.1
FPT_TST.1	F.OPERATIONS_CRYPTO	Section 8.3.1
FMT_MSA.3	F.GESTION_PARTITION, F.GESTION_ACCES	Section 8.3.1
FMT_MSA.1/Disk_Status	F.CONTROLE_ACCES	Section 8.3.1
FMT_MSA.1/ID	F.GESTION_PARTITION, F.GESTION_ACCES	Section 8.3.1
FMT_MSA.1/Access_Admin	F.GESTION_ACCES	Section 8.3.1
FMT_MSA.1/Role_Admin	F.GESTION_ACCES	Section 8.3.1
FMT_MSA.1/Disk_Admin	F.GESTION_PARTITION	Section 8.3.1
FMT_MSA.1/User	F.GESTION_ACCES	Section 8.3.1
FMT_SMR.1	F.GESTION_ACCES, F.GESTION_PARTITION	Section 8.3.1
FMT_MOF.1	F.CONFIGURATION_TOE	Section 8.3.1
FMT_MTD.1	F.CONFIGURATION_TOE	Section 8.3.1
FMT_SMF.1	F.GESTION_ACCES, F.CONTROLE_ACCES, F.GESTION_PARTITION, F.CONFIGURATION_TOE, F.OPERATIONS_CRYPTO	Section 8.3.1
FDP_ACC.1	F.CONTROLE_ACCES, F.GESTION_ACCES	Section 8.3.1
FDP_ACF.1	F.CONTROLE_ACCES, F.GESTION_ACCES, F.GESTION_PARTITION	Section 8.3.1
FCS_COP.1	F.OPERATIONS_CRYPTO	Section 8.3.1
FDP_RIP.1	F.GESTION_AMORÇAGE_ET_ARRET	Section 8.3.1
FCS_CKM.1	F.OPERATIONS_CRYPTO	Section 8.3.1

Tableau 12 Association exigences fonctionnelles vers les spécifications globales

Spécifications globales	Exigences fonctionnelles de sécurité
F.CONFIGURATION_TOE	FAU_GEN.1, FMT_MTD.1, FIA_UID.1, FIA_UAU.1, FMT_SMF.1, FMT_MOF.1
F.AUDIT	FAU_GEN.1, FAU_GEN.2
F.OPERATIONS_CRYPTO	FCS_COP.1, FPT_SDI_EXT.2, FPT_TST.1, FMT_SMF.1, FCS_CKM.1
F.GESTION_ACCES	FAU_GEN.1, FIA_UID.1, FIA_UAU.1, FMT_SMR.1, FMT_SMF.1, FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1/ID, FMT_MSA.1/Access_Admin, FMT_MSA.1/Role_Admin, FMT_MSA.1/User
F.CONTROLE_ACCES	FAU_GEN.1, FAU_GEN.2, FIA_AFL.1, FIA_UID.1, FIA_UAU.1, FMT_MSA.1/Disk_Status, FMT_SMF.1, FDP_ACC.1, FDP_ACF.1
F.GESTION_PARTITION	FAU_GEN.1, FMT_MSA.3,FMT_MSA.1/Disk_Admin, FMT_MSA.1/ID, FDP_ACF.1, FMT_SMR.1
F.GESTION_AMORÇAGE_ET_ARRET	FPT_FLS.1, FPT_SDI_EXT.2, FDP_RIP.1,FAU_GEN.1

Tableau 13 Association spécifications globales vers exigences fonctionnelles

8.4. Dépendances

8.4.1. Dépendances des exigences de sécurité fonctionnelles

Exigences	Dépendances CC	Dépendances Satisfaites
FAU_GEN.1	FPT_STM.1	
FAU_GEN.2	FAU_GEN.1 et FIA_UID.1	FAU_GEN.1, FIA_UID.1
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/Disk_Status	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/ID	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/Access_Admin	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/Disk_Admin	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/Role_Admin	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/User	(FDP_ACC.1 ou FDP_IFC.1) et (FMT_SMF.1) et (FMT_SMR.1)	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
FMT_MOF.1	FMT_SMF.1 et FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_SMF.1	Pas de dépendance	Pas de dépendance
FDP_ACC.1	(FDP_ACF.1)	FDP_ACF.1

Exigences	Dépendances CC	Dépendances Satisfaites
FAU_GEN.1	FPT_STM.1	
FAU_GEN.2	FAU_GEN.1 et FIA_UID.1	FAU_GEN.1, FIA_UID.1
FDP_ACF.1	(FDP_ACC.1) et (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1
FCS_COP.1	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FCS_CKM.1
FDP_RIP.1	Pas de dépendance	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	Pas de dépendance	
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FPT_FLS.1	Pas de dépendance	
FPT_SDI_EXT.2	Pas de dépendance	
FPT_TST.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

Argumentaire pour les dépendances non satisfaites

La dépendance FPT_STM.1 de FAU_GEN.1 n'est pas supportée. Le système d'horodatage est fourni par l'environnement de la TOE.

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.

8.4.2. Dépendances des exigences de sécurité d'assurance

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

Exigences	Dépendances CC	Dépendances Satisfaites
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.4) et (ADV_IMP.1) et (ADV_TDS.3) et (AGD_OPE.1) et (AGD_PRE.1) et (ATE_DPT.1)	ADV_ARC.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Tableau 15 Dépendances des exigences d'assurance

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].

La dépendance ADV_FSP.4 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].

8.5. 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 [QUALIF_STD]. Ce niveau d'assurance impose:

- Des tests indépendants effectués par l'évaluateur (l'utilisateur final est alors assuré que les fonctions de sécurité de la TOE sont implémentées comme spécifié)

- Une analyse de vulnérabilité indépendante effectuée par l'évaluateur qui considèrera un niveau d'attaquant correspondant au niveau élémentaire renforcé ou inférieur (l'utilisateur final est alors assuré que la TOE est

résistante à des attaques de pénétration effectuées par des attaquants possédant un faible potentiel d'attaque).

- L'évaluation de l'architecture de sécurité et de l'architecture logiciel incluant l'analyse de l'implémentation (fonctions cryptographiques seulement) pour vérifier qu'il n'y a pas de défaut de sécurité

- De bonnes pratiques en matière de développement de la partie cryptographique (l'utilisateur final est alors assuré que le produit a été correctement et sécuritairement conçu et développé).

- De bonnes pratiques en matière de maintenance et support aux utilisateurs assurant que toutes les anomalies identifiées seront corrigées et rapportées aux utilisateurs du produit considéré qui pourraient être affectés par cette anomalie.

8.6. Argumentaire pour les augmentations à l'EAL

8.6.1. AVA_VAN.3 Focused vulnerability analysis

Augmentation requise par le processus de qualification standard [QUALIF_STD].

8.6.2. ALC_FLR.3 Systematic flaw remediation

Augmentation requise par le proc

8.7. Argumentaire pour les annonces de conformité à un PP

Cette cible de sécurité est conforme au profil de protection [CDISK] conformément aux recommandations de l'ANSSI pour le niveau standard sur cette classe de produit.

9. ANNEXE A: DEFINITION DE COMPOSANTS ETENDUS

9.1. TSF data integrity (FPT_SDI_EXT)

Family Behavior

This family provides requirements that address protection of TSF data while it is stored within containers controlled by the TSF. Integrity errors may affect technical files stored on the disk.

Component leveling

FPT_SDI_EXT.2: TSF data integrity monitoring and action, requires that the TSF monitor TSF data stored within containers controlled by the TSF for identified integrity errors and take action as a result of an error detection.

Management: FPT_SDI_EXT.2

The following actions could be considered for the management functions in FPT:

a) The actions to be taken upon the detection of an integrity error could be configurable.

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: detection of modification of TSF data;

FPT_SDI_EXT.2: TSF data integrity monitoring and action

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SDI_EXT.2.1 The TSF shall be able to detect [selection: *modification of data, substitution of data, deletion of data, [assignment: other integrity errors*]] of [selection: [assignment: *parts of the TSF data*], *TSF data*].

FPT_SDI_EXT.2.2 Upon detection of a data integrity error, the TSF shall take the following actions: [assignment: *action to be taken*].

10. ANNEXE B: CONFORMITE AU PROFIL DE PROTECTION [CDISK]

L'objectif cette annexe est de détailler, par chapitre, les adaptations effectuées dans la cible de sécurité par rapport au profil de protection [CDISK]. Pour ne pas surcharger inutilement la discussion, nous n'indiquerons pas les mises à jour nécessaires qui ont dues être faites (remplacement du terme DCSSI par ANSSI, mise à jour des versions de certains documents ANSSI par exemple).

Nous n'indiquerons que les modifications apportées, les ajouts (et les assignations) se traduisent par une police différente aisément identifiable (les éléments du profil de protection sont en caractères rouges, les ajouts en caractère bleu).

10.1. Chapitre 3 : Définition du problème de sécurité

10.1.1. Chapitre 3.1 : Biens

D'autres biens ont été explicités (données d'authentifications, clés de chiffrement dans fichier de fonctionnement …).

10.1.2. Utilisateurs

Suppression de la note d'application (ci-dessous) qui ne s'applique pas dans la mesure où la TOE considère 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.

10.1.3. Chapitre 3.3 : Menaces

T.ACCES_DONNEES : Suppression de la *Note d'application* :

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

En effet, l'image du disque ne contient pas de clé de chiffrement en clair. Il a été cependant précisé que les fichiers de fonctionnement (clés de chiffrement chiffrées) sont impactés.

10.1.4. Chapitre 3.4 : Politiques de sécurité organisationnelles (OSP)

Néant

10.1.5. Chapitre 3.5 (PP)/Chapitre 3.3 (cible) : Hypothèses

Suppression du paragraphe 3.5.2 car non applicable dans cette cible. En effet les clés de chiffrement AES sont générées par la TOE (par contre l'hypothèse A.CRYPTO_EXT a été ajoutée pour les clés d'accès RSA).

10.2. Chapitre 4 : Objectifs de sécurité

10.2.1. Chapitre 4.1 : Objectifs de sécurité pour la TOE

1) Suppression de la sous division du paragraphe (« Objectifs applicables aux deux configurations », « Objectifs applicables à la configuration avec génération de clé ») et des mentions relatives aux configurations «sans génération de clé» et «avec génération de clé».

2) Modification de O.ARRET_UTILISATEUR :

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

Note d'application

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

Comme ceci :

La TOE doit rendre inaccessibles les données sensibles, en particulier les clés cryptographiques, lorsque l'utilisateur arrête le poste de travail.

L'objectif se ramène à l'effacement des données sensibles à la fermeture du poste. En effet la notion de démontage de disque n'est pas applicable à Cryhod, l'utilisateur a la possibilité d'éteindre son poste.

10.2.2. Chapitre 4.2 : Objectifs de sécurité pour l'environnement opérationnel de la TOE

Suppression de la sous division du paragraphe (« Objectifs applicables aux deux configurations », « Objectifs applicables à la configuration avec génération de clé ») et des mentions relatives aux configurations «sans génération de clé» et «avec génération de clé». Suppression de OE.ENV_OPERATIONNEL.3 et OE.ENV_OPERATIONNEL.4 (et des mentions qui s'y rapportent) qui ne sont pas applicables.

10.3. Chapitre 5 : Exigences de sécurité

10.3.1. Chapitre 5.1 : Exigences de sécurité fonctionnelles

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

2) L'authentification utilisateur s'effectuant à l'amorçage du système, aucune opération (autre que CREATE lorsque les partitions ne sont pas encore chiffrées) n'est possible. En conséquence les modifications suivantes ont été apportées :

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.

Les opérations supprimées ci-dessus ont été reportées dans les raffinements éditoriaux.

1) Mise en forme de la note d'application de FMT_MSA.3 comme demandée dans le profil de protection.

2) Deux règles ayant été ajoutées dans FDP_ACF.1.2, « Rule 7 » a été incrémentée en « Rule 9 » dans FDP_ACF.1.3.

3) Prise en compte de la génération de clé

10.3.2. Chapitre 5.2 : Exigences de sécurité d'assurance

Néant

10.4. Chapitre 6 (PP)/Chapitre 8 (cible) :Argumentaire

10.4.1. Chapitre 6.1.1 (PP)/Chapitre 8.1.1 (cible) : Menaces

Suppression des paragraphes relatifs à OE.ENV_OPERATIONNEL.3 et OE.ENV_OPERATIONNEL.4 qui ne sont pas applicables dans cette cible.

10.4.2. Chapitre 6.1.2 (PP)/Chapitre 8.1.2 (cible) : OSP

La mention concernant la configuration « avec génération de clé » a été supprimée dans OSP.CRYPTO.

10.4.3. Chapitre 6.1.3 (PP)/Chapitre 8.1.3 (cible) : Hypothèses

Suppression du chapitre relatif à la configuration sans génération de clé.

10.4.4. Chapitre 6.1.4 (PP)/Chapitre 8.1.4 (cible) : Tables de couverture

Mise en forme des tableaux selon la configuration « avec génération de clé »

10.4.5. Chapitre 6.2.1 (PP)/Chapitre 8.2.1 (cible) :Objectifs

Suppression de « L'accès lui-même ne demande aucune authentification (FIA_UID.1). » dans O.PROTECTION_DES_DONNEES_ENREGISTREES.

10.4.6. Chapitre 6.2.2 (PP)/Chapitre 8.2.2 (cible) : Tables de couverture

Mise en forme des tableaux selon la configuration « avec génération de clé »

10.4.7. Chapitre 6.3.1 (PP)/Chapitre 8.4.1 (cible) : Dépendances des exigences de sécurité fonctionnelles

1) Mise en forme du tableau selon la configuration « avec génération de clé »

2) Suppression de certaines dépendances non satisfaites dans le profil de protection (la notion de rôle et par conséquent FMT_SMR.1 est définie dans la TOE ainsi que la fonction de gestion des accès dans FMT_SMF.1 qui induit les manipulations d'attributs dans les différents composants FMT_MSA.1 et FMT_MSA.3) :

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.

10.4.8. Chapitre 6.3.3 (PP)/Chapitre 8.4.2 (cible) : Dépendances des exigences de sécurité d'assurance

Mise à jour des dépendances et de l'argumentaire en accord avec les Critères Communs version 3.1 révision 3

10.4.9. Chapitre 6.4 (PP)/Chapitre 8.5 (cible) : Argumentaire pour l'EAL

Néant

10.4.10. Chapitre 6.4 (PP)/Chapitre 8.6 (cible) : Argumentaire pour les augmentations à l'EAL

Néant