PRIM'X TECHNOLOGIES

version 6.2

Cible de Sécurité

Critères Communs niveau EAL3+

Document v1 r7

Sommaire

Liste des figures

Liste des tableaux

1. Introduction de la cible de sécurité

1.1. Identification de la cible de sécurité

Cible de sécurité :	ZoneCentral version 6.2 Cible de sécurité CC niveau EAL3+
Version de la ST :	PX171727 v1r7 - Janvier 2020
Cible d'évaluation (TOE) :	ZoneCentral version 6.2 build 3030 pour les plates-formes PC sous Microsoft Windows 7 et Windows 10 versions 1809 et 1903 (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 :	Aucune.
Référence des CC :	Critères Communs version 3.1 Révision 4, Parties 1 à 3 – Septembre 2012

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

ZoneCentral est un produit de sécurité pour assurer la confidentialité des données des organismes. Le logiciel agit comme une couche de sécurité intégrée au système, transparente pour les utilisateurs et pouvant s'appliquer à tous les systèmes de fichiers qu'ils soient locaux, amovibles ou réseau. En chiffrant les fichiers et les dossiers là où ils résident, il n'y a aucun impact sur l'organisation des données de l'organisme.

ZoneCentral sera évalué pour une plate-forme PC sous les systèmes d'exploitation Microsoft Windows 7 et Windows 10 versions 1809 et 1903 (64 bits).

1.3. Conformité aux Critères Communs

Cette cible de sécurité respecte les exigences des Critères Communs version 3.1 révision 4 de septembre 2012 :

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Révision 4, Septembre 2012. CCMB-2012-09-001.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Révision 4, Septembre 2012. CCMB-2012-09-002.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Révision 4, Septembre 2012. CCMB-2012-09-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Révision 4, Septembre 2012. CCMB-2012-09-004.

Toutes les exigences fonctionnelles décrites dans cette cible de sécurité sont issus de la Partie 2 « stricte » des Critères Communs version 3.1 révision 4 de septembre 2012. Le niveau d'assurance « EAL3 augmenté » retenu est conforme à la Partie 3 « stricte » des Critères Communs version 3.1 révision 4 de septembre 2012. 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 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 de sécurité – niveau standard – version 1.2, DCSSI.

[CRYPTO_STD] RGS version 2.0 – Annexe B1. Mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - Version 2.03 du 21 février 2014, 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.

2. Description de la cible d'évaluation (TOE)

2.1. Présentation de la TOE

2.1.1. Description Générale

ZoneCentral est un **produit de sécurité** pour postes de travail opérant avec des processeurs 32 ou 64 bits sous Windows (à partir de Windows 7). Seul le produit s'exécutant sur les processeurs 64 bits sera évalué. Le rôle de ZoneCentral est de préserver la confidentialité des documents manipulés par les utilisateurs, sur des postes isolés, des ordinateurs portables, ou des postes de travail connectés à un réseau d'un organisme.

Il permet de gérer un stockage chiffré des fichiers, sans modifier leurs caractéristiques (emplacement, nom, dates, tailles) et de façon la plus transparente possible pour les utilisateurs. Le chiffrement des fichiers s'effectue en effet '***in-place***' (là où résident les fichiers) et '***à la volée***' (sans manipulation particulière de l'utilisateur).

Pour simplifier la gestion des fichiers chiffrés, ZoneCentral est basé sur le principe de **zones** : une zone chiffrée est un volume, ou un dossier, avec tout ce qu'il contient (fichiers et sous-dossiers) et à l'intérieur duquel tout fichier existant ou à venir est maintenu chiffré, sans qu'il existe à aucun moment de copie en clair des données.

L'ensemble des zones chiffrées définit un **espace sécurisé** pour les utilisateurs : cela peut comprendre son 'profil utilisateur Windows' (avec son dossier 'Mes Documents', son 'Bureau', son cache de navigation Web, les fichiers temporaires, etc.), son espace de travail habituel (l'endroit où habituellement l'utilisateur gère ses fichiers), les partages réseau auxquels il accède (serveurs de fichiers), ou encore la ou les clés mémoire USB qu'il utilise.

Pour chaque zone chiffrée, 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.

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 ZoneCentral de la calculer) soit une clé RSA hébergée dans un porte-clés comme un fichier de clé, une carte à mémoire, un container CSP ou CNG Microsoft Windows (le porte-clés pouvant lui-même être protégé par un code confidentiel). Une clé d'accès permet de retrouver (en les déchiffrant) les informations de chiffrement des zones et des fichiers.

L'objectif de ZoneCentral est de protéger les fichiers stockés [dans des zones chiffrées] et de faire en sorte qu'il n'y ait pas de résidus en clair sur les supports de stockage (si l'espace sécurisé des utilisateurs est correctement défini et chiffré).

Dans le cas d'accès à des serveurs depuis des postes clients, ZoneCentral n'intervient que si ces accès sont effectués sous la forme d'accès à des fichiers (exemple: lecture ou copie d'un fichier se trouvant sur un partage serveur). ZoneCentral n'intervient pas si le mode d'échange entre le poste client et le poste serveur s'effectue de façon applicative (procédé client/serveur quelconque). En effet, dans ce cas, c'est l'application du serveur qui lit les fichiers, retransforme éventuellement le contenu en mémoire (présentation) avant de retourner l'information à l'application cliente par un protocole quelconque. Il ne s'agit plus d'accès fichiers, mais d'accès réseaux. Dans ce cas, si on souhaite protéger le tronçon réseau, il convient de s'équiper de solutions complémentaires, comme du TLS ou du VPN dédiées à ce type de protection.

Par contre, ZoneCentral offre une protection locale si ces échanges réseau entraînent des stockages locaux de données dans des fichiers. Par exemple, une application Intranet (sous forme Web), permettant de consulter des données sensibles sera certainement protégée par TLS qui chiffrera les échanges protocolaires du réseau. Mais TLS ne protège pas les copies des pages lues qui sont conservées dans le cache local du navigateur Internet, elles sont enregistrées en clair, avec toutes leurs informations, sauf si ZoneCentral est actif sur le poste et que l'espace local Internet fait partie d'une zone chiffrée (généralement le profil de l'utilisateur Windows).

Tous les éléments clés de ZoneCentral (zones, accès, listes d'accès) sont manipulables au travers d'une **interface de programmation** (API). Cette API permet de développer ses propres applications dans différents langages et d'intégrer des opérations ZoneCentral dans un workflow interne ou de développer sa propre application de gestion des accès par exemple.

2.1.2. La technologie de ZoneCentral

Sous Windows, un fichier appartient à un ***FileSystem***, qui le stocke et le gère. Par exemple NTFS pour un volume système C:, FAT pour un petit volume D:, CDFS pour un CD-ROM, le Client Réseau Microsoft pour un partage réseau sur un serveur, etc. Tous les FileSystem offrent des méthodes d'accès aux fichiers qu'ils hébergent, sous une forme relativement homogène et universelle, de façon à ce que les applications qui accèdent aux fichiers n'aient normalement pas à se préoccuper de la nature du FileSystem qui héberge leurs fichiers. Bien entendu, tous les FileSystem ne sont pas identiques, puisqu'ils sont conçus pour offrir des services différents (NTFS offre des ACLs de droits d'accès, un client réseau gère l'aspect réseau, etc.).

Toute application, tout composant système sous Windows qui accède à un fichier (ouvrir un fichier, lire une partie de son contenu, écrire, réécrire, ajouter de l'information, etc.) soumet ses requêtes à un mécanisme qui les confie au FileSystem concerné par le fichier en question.

ZoneCentral s'intègre au noyau Windows et se positionne dans les chaînes de FileSystem, selon une technologie de « ***filtre*** » prévue justement dans ces chaînes. Ainsi positionné, il reçoit (et retransmet ensuite à l'élément suivant de la chaîne) toutes les requêtes passées sur tous les fichiers de tous les FileSystem qu'il filtre. Au passage (de ces requêtes), il est en mesure d'effectuer certaines opérations lorsque c'est nécessaire : déchiffrer la portion lue lorsqu'il s'agit d'une lecture d'un fichier chiffré, ou au contraire chiffrer la portion écrite lorsqu'il s'agit d'une écriture d'un fichier chiffré, ou encore effectuer un effacement par surcharge lorsqu'un fichier est supprimé.

2.1.3. Les zones et les accès

ZoneCentral gère des **zones chiffrées**. Une zone est un emplacement (un dossier) dans lequel tous les fichiers sont chiffrés, ainsi que tous les sous-dossiers et leur contenu.

Chaque zone chiffrée est définie par son emplacement, certaines caractéristiques de chiffrement (dont font partie les clés de chiffrement des fichiers, les algorithmes, etc.), une liste d'accès utilisateurs et, éventuellement, une liste d'exceptions de fichiers (qui ne sont pas chiffrés bien qu'étant dans la zone).

Pour pouvoir utiliser une zone chiffrée, un utilisateur doit disposer d'une **clé d'accès**. Cette clé d'accès lui a été remise par l'Administrateur de la Sécurité (appelé Administrateur de la TOE dans la suite du document). Il peut s'agir d'une clé RSA hébergée dans un porte-clés comme un fichier de clés, une carte à puce, un container Microsoft CSP ou CNG (le porte-clés intégrant la plupart du temps son propre dispositif d'authentification avec un code confidentiel). Le mot de passe (qui donnera la clé d'accès par dérivation) peut être fourni par l'administrateur ou choisi par l'utilisateur en fonction de la politique de sécurité mise en œuvre.

Lorsque la zone chiffrée a été fabriquée, les fichiers de la zone ont été chiffrés avec des clés dédiées à la zone, et ces clés ont elles mêmes été chiffrées avec les clés d'accès des utilisateurs à qui l'Administrateur de la TOE donne le droit d'accéder au contenu (confidentiel) de la zone. Bien entendu, les clés d'accès elles-mêmes ne figurent pas dans la zone.

ZoneCentral propose différents algorithmes et mécanismes de sécurité, tous conformes à l'état de l'art en la matière. Il propose deux schémas de gestion de clés d'accès qui peuvent être utilisés en même temps sur les mêmes zones. Un schéma dit « symétrique » basé sur des mots de passe et des clés dérivées de mots de passe (réf. : PKCS#12) et un schéma dit « asymétrique » utilisant des clés RSA (réf. : PKCS#1 v2.2) embarquées dans des fichiers de clés (réf. : PKCS#12) ou des porte-clés (ref: PKCS#11 et/ou CSP/CNG).

Quand un utilisateur accède à une zone chiffrée, le moteur temps-réel de ZoneCentral le détecte, s'aperçoit que le fichier demandé est chiffré et qu'il a besoin de le déchiffrer pour restituer les informations qu'il contient à l'application qui le demande.

S'il ne dispose pas d'une clé d'accès valide pour cette zone, il la demande en temps réel à l'utilisateur. Celui-ci la fournit, et ZoneCentral est alors en mesure de 'servir' tous les fichiers de la zone. Quand l'utilisateur accède à une autre zone chiffrée, ZoneCentral regarde si la ou les clés d'accès déjà fournies peuvent convenir avant d'en redemander une à l'utilisateur. Les clés d'accès ainsi fournies restent valides tant qu'elles n'ont pas été explicitement fermées par l'utilisateur (avec l'explorateur de Zones, l'afficheur graphique de ZoneCentral pour l'utilisateur), ou tant qu'un événement système ne s'est pas produit, comme un verrouillage de session Windows, un déclenchement de l'économiseur d'écran ou l'arrêt du système.

Les zones chiffrées peuvent résider sur des disques locaux, des unités amovibles (comme des clés USB) ou des unités partagées sur serveurs.

L'administrateur de la TOE peut également définir des **zones en clair**. Par défaut, toute zone non chiffrée depuis la racine d'un volume est une zone en clair. Mais à l'intérieur d'une zone chiffrée, tous les sous-dossiers sont chiffrés, et il peut être utile,

pour diverses raisons, de disposer de sous-dossiers en clair. Il est possible d'interdire la création de nouveaux fichiers à l'intérieur d'une zone en clair.

De la même manière, l'administrateur de la TOE peut définir **des zones chiffrées à l'intérieur d'autres zones chiffrées** (et ceci autant de fois qu'il le souhaite). La raison la plus courante est qu'il souhaite que les utilisateurs qui y aient accès ne soient pas les mêmes.

Une zone chiffrée peut contenir des **exceptions**, c'est-à-dire des fichiers qui ne sont pas chiffrés bien qu'étant physiquement dans la zone. Généralement, ce mécanisme est utilisé pour des fichiers qui ne présentent pas de caractère de confidentialité et qu'il est préférable de laisser en clair pour ne pas perturber une application ou le système lui-même. Par défaut, par exemple, les stratégies de sécurité de ZoneCentral définissent comme des exceptions les exécutables (pour que l'Explorateur puisse afficher leurs icônes sans demander d'accès à l'utilisateur), les liens, et les fichiers de clés utilisateurs (qui sont déjà auto-protégés).

2.1.4. Les listes d'accès

Plutôt que de définir directement les accès utilisateurs dans une zone chiffrée, il est possible de passer par un maillon intermédiaire, la **liste d'accès**. Une liste d'accès regroupe les accès utilisateurs, et la zone fait ensuite référence à cette liste. Cela permet notamment d'utiliser une même liste d'accès pour plusieurs zones (unicité de gestion), et de regrouper les listes d'accès au même endroit (centralisation).

Une zone peut référencer plusieurs listes d'accès, et une liste d'accès peut en référencer une ou plusieurs autres. Noter que deux zones référençant la même liste d'accès conservent des clés de chiffrement différentes. Il est également possible de mixer des accès directs (définition des accès directement dans une zone) et des indirects (via des listes d'accès).

Les listes d'accès sont référencées par leur nom de fichier, mais sans l'emplacement qui, lui, est spécifié dans une stratégie de sécurité («Policy»). Il y a **l'emplacement principal** et un emplacement **secondaire**, pouvant servir de «cache local». Ce mécanisme a été prévu pour que l'emplacement principal soit sur un partage réseau et que l'emplacement secondaire soit local. La copie de secours permet de continuer à fonctionner si le réseau n'est pas disponible (cas des postes nomades)

2.1.5. Autres fonctionnalités

ZoneCentral intègre un service automatique et transparent d'**effacement sécurisé par surcharge.** Pour cela, ZoneCentral détecte en temps réel toutes les suppressions de fichiers sur le système, qu'elles proviennent de l'utilisateur directement, d'une application ou du système lui-même, et applique à ces fichiers un traitement de surcharge de leur contenu avant leur suppression effective. Cela concerne également tous les fichiers temporaires. Cela concerne également les résidus de fichiers qui ne sont pas supprimés mais «retaillés» (diminution de taille). Le type de surcharge (nombre de passes et masque) est configurable par l'administrateur.

ZoneCentral chiffre également le fichier d'échange de la mémoire virtuelle du poste (le **swap**) dans lequel peuvent figurer des informations rémanentes (portions de mémoire des applications utilisées).

ZoneCentral **peut interdire la création de fichiers en clair** (i.e. en dehors de zones chiffrées), sur le poste, sur un périphérique amovible, sur le réseau, ou en fonction de directives indiquées dans les zones en clair explicites. L'objectif est de «contraindre» les utilisateurs à travailler dans des zones chiffrées, et, par exemple, de faire en sorte qu'ils ne puissent pas écrire sur des clés mémoire USB (sauf si elles sont elles-mêmes chiffrées).

Les **envois de fichiers chiffrés dans la Corbeille Windows** sont sécurisés. Ces fichiers, qui sortent d'une zone chiffrée pour aller dans la Corbeille, demeurent chiffrés et conservent les propriétés de zone leur permettant d'être restaurés (à condition de présenter une clé d'accès adéquate bien entendu).

ZoneCentral supporte le **partage de dossiers** sur les postes utilisateurs. Si ce partage porte sur un dossier d'une zone chiffrée, **le partage est effectué en chiffré** : le trafic réseau est donc chiffré et la ou les personnes qui accèdent à ce partage ne peuvent l'utiliser que si elles disposent de ZoneCentral et de clés d'accès valides pour la zone de partage.

Les services et outils des différents types de FileSystems demeurent opérationnels : les droits d'accès, le contrôle d'erreur (scandisk), la défragmentation, etc. Seule la compression intégrée est inefficace, puisque des fichiers chiffrés sont binaires.

ZoneCentral supporte le **chiffrement de profils utilisateurs Windows**, ce qui permet notamment de chiffrer le Bureau, Mes Documents, l'espace «temporaire», ou encore le cache des navigateurs Internet, ce qui peut être très important en cas d'utilisation d'applications Web Intranet affichant des pages sensibles.

ZoneCentral supporte également les **profils itinérants** (« roaming ») chiffrés, les **dossiers redirigés** du profil (« redirected folders »), ainsi que les **dossiers synchronisés disponibles hors connexion** (« offline folders »), qui peuvent à la fois être chiffrés sur l'image serveur et sur la copie local (« CSC »).

2.2. Services d'administration, 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 4 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 de la TOE 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 sont signées par l'administrateur de la sécurité de la TOE et vérifiées par ZoneCentral 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. 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 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 sécurité) de la TOE** en charge de définir les zones chiffrées du « parc » et effectuer la procédure de migration initiale qui consiste à chiffrer leur contenu actuel, sur les serveurs (partages) et sur les postes de travail. Pour chaque zone chiffrée, 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 nouvelles zones si besoin est (nouveaux ordinateurs, nouveaux partages), à gérer les 'mouvements de personnel' (nouvel utilisateur pour une zone, retrait d'accès pour une personne en partance), et, éventuellement, de transchiffrer les zones chiffrées (sur compromission ou régulièrement). L'administrateur de la TOE a par ailleurs en charge les opérations de signature des politiques et de recouvrement local. Sauf mention contraire dans la suite de ce document, toute référence à l'administrateur se rapporte à ce rôle.
- Un rôle **opérateur de secours** de la TOE en charge des opérations de secours des utilisateurs distant ayant oublié leur mot de passe ou perdu/cassé/bloqué leur porte-clés physique. Contrairement à l'administrateur de le TOE, l'accès de l'opérateur de secours n'est pas déclaré dans les zones des autres utilisateurs.
- Un rôle **utilisateur** qui utilise la TOE selon la configuration imposée par 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.

Note concernant l'utilisation des API :

Les API permettent d'effectuer un nombre limités d'actions relatives aux rôles utilisateur ou Administrateur de la TOE. D'un point de vue utilisateur, elles permettent par exemple d'ouvrir et de fermer des zones, et elles donnent à l'Administrateur la possibilité de gérer les accès ou de remonter des informations sur les zones (mais pas d'effectuer des opérations de chiffrement/déchiffrement). Les 2 rôles peuvent donc utiliser ces API (dans un script) pour faciliter ou automatiser certaines tâches. Par exemple un administrateur peut utiliser les API pour ajouter un accès à toutes les zones d'un poste plutôt que de le faire 'à la main'. Dans tous les cas, c'est la clé d'accès qui fixe le rôle alloué et donc les opérations permises, un utilisateur voulant exécuter une API de gestion des accès se verra demander une clé de niveau administrateur au début de l'opération et la commande sera refusée s'il ne peut la présenter.

ZoneCentral fournit différents outils permettant d'effectuer ces opérations, sous différentes formes techniques et ergonomiques pour s'adapter aux différentes

méthodes de gestion : lignes de commandes scriptables, interfaces graphiques de préparation en 'amont', interfaces simplifiées et conviviales pour une utilisation par les utilisateurs eux-mêmes, etc. En particulier, **ZoneBoard**, outil intégré dans ZoneCentral, permet à l'administrateur de la TOE de créer et supprimer des zones chiffrées, de visualiser et de gérer l'ensemble des accès cryptographique sur les zones chiffrées partagées.

2.2.2. Services d'administration

Les différentes « commandes » (graphiques ou en ligne de commande) offertes permettent de réaliser les opérations d'administration suivantes :

- Lire ou modifier les policies, signer les policies. Attention par défaut les politiques ne sont pas signées, l'opération préalable de signature des politiques et leur intégration dans le package d'installation sont nécessaires pour bénéficier de la fonction de contrôle de signature des politiques ;
- Créer une zone chiffrée (i.e. chiffrement initial d'un emplacement) ;
- Déchiffrer une zone chiffrée ;
- Transchiffrer (renouveler les clés de chiffrement) d'une zone chiffrée ;
- Définir une zone en clair (à ne pas chiffrer, volontairement) ;
- Consulter les accès d'une zone chiffrée, ajouter des accès ou en retirer ;
- Consulter ou modifier certaines propriétés 'techniques' de zones (le label, les exceptions) ;
- Rechercher les zones chiffrées ;
- Créer ou modifier des listes d'accès ;
- Effectuer le recouvrement par l'administrateur de la TOE ;
- Effectuer le secours utilisateur par l'opérateur de secours de la TOE.

ZoneCentral 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 zones chiffrées, des accès etc.).

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

Par ailleurs, ZoneCentral 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 notamment les événements d'ouverture et de fermeture de zones chiffrées par les utilisateurs, certains problèmes courants pour réparation (ex : une liste d'accès non trouvée), et toutes les commandes d'administration, réussies ou non.

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 et les applications.

L'administrateur de la TOE définit les ***règles d'usage (policies)*** du produit puis les signe avec sa clé privée, ce qui se traduit par une configuration prédéfinie 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). Parmi ces règles, on trouve, par exemple, les longueurs des clés de chiffrement à utiliser, les opérations autorisées pour les utilisateurs standards, le comportement que doit adopter le logiciel dans certains cas, le nombre de passes de surcharge pour l'effacement sécurisé, 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 TOE de ***définir (fournir) les clés d'accès*** des utilisateurs (issues d'une PKI, par exemple). ZoneCentral 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 ou les partages réseau, en fonction de leur contenu et/ou de leur topologie : il s'agit en pratique de définir ***quelles zones doivent être chiffrées*** et d'exécuter la procédure de chiffrement initial (car, la plupart du temps, ces zones existent déjà et ont déjà un contenu). 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 zones chiffrées sont définies et chiffrées, et les accès à ces zones pour les utilisateurs sont définis. Seuls les utilisateurs disposant de clés d'accès valides pour les zones chiffrées pourront lire ou écrire des fichiers dans ces zones.

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 une zone chiffrée, 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. Un «double-click» pour ouvrir un fichier chiffré lance directement l'application concernée, qui accède au contenu. Un «glisser-déplacer» d'un fichier vers une zone chiffrée va le chiffrer automatiquement. Un «Enregistrer-sous» d'un fichier dans une zone chiffrée va chiffrer le fichier écrit automatiquement. Etc.

A la première tentative d'accès à un fichier chiffré dans une zone chiffrée, ZoneCentral demande à l'utilisateur une clé d'accès permettant de déchiffrer le fichier (en pratique, le schéma est plus complexe, et cette clé d'accès permet de déchiffrer des clés intermédiaires qui elles-mêmes chiffrent les fichiers). Si l'utilisateur peut la fournir, alors le fichier peut être déchiffré (ou chiffré, s'il s'agit d'une création ou d'une écriture). Sinon, l'application se voit refuser l'accès avec le code erreur habituel

« Accès non autorisé». Par la suite, tous les autres fichiers de la même zone seront «servis» puisque les clés en sont désormais connues. Ceci, bien entendu, tant que les zones ainsi ouvertes ne sont pas «fermées» (par l'utilisateur lui-même, par une fermeture de session Windows, etc.).

2.3. Périmètre et architecture de la cible d'évaluation

2.3.1. Les composants de ZoneCentral

La figure 1 présente l'architecture du produit, le périmètre de la TOE est délimité par des pointillés. L'installation configure les composants de base de ZoneCentral, qui sont trois drivers, un service système, et un «daemon» utilisateur (figure 1) :

- Le driver «**ZCK**», qui se place en filtre au-dessus des drivers de FileSystems et des volumes qu'il présente, et qui intercepte les requêtes d'accès au fichier. Il est possible de limiter ces drivers et ces volumes avec une stratégie de sécurité ;
- Le driver «**ZCCK**» qui est le centre cryptographique de ZoneCentral : il gère les clés de zone et exécute les opérations de calcul associées. Les clés ne sortent jamais de son enceinte, sauf lorsque le produit est configuré pour utiliser des porte-clés (comme des extensions PKCS#11 pour des cartes à puce ou des CSPs/CNGs). Cette implémentation de la cryptographie en mode kernel du système renforce le niveau de protection global car c'est un emplacement très difficilement accessible aux logiciels 'pirates' ;
- Le driver «**ZCKBD**», qui est un filtre de saisie clavier : il intercepte à très bas niveau les mots de passe et codes confidentiels saisis de façon à ce que leur valeur reste confinée le plus bas possible dans le système. Ils sont ensuite utilisés par le driver cryptographique ZCCK, ou remis aux moteurs externes (CSP et CNG/PKCS#11). Cela ne concerne QUE les mots de passe gérés par ZoneCentral, c'est-à-dire ceux qui conditionne les accès aux zones chiffrées. Cette implémentation renforce également la protection de ces données sensibles, qui ne remontent pas au niveau applicatif du système, source régulière et préférée des logiciels 'pirates' ;
- Le service «**ZCS**», qui coordonne les traitements entre le monde «kernel» (drivers) et le monde «user» (programmes et applications) ;
- Le service « **ZCP** » qui contrôle la signature des politiques ;
- Le «daemon» utilisateur «**ZCU**», instancié pour chaque session utilisateur Windows (ZoneCentral supporte le multisessions) gère les interfaces graphiques proposées aux utilisateurs (notamment la fenêtre de demande d'accréditation pour déverrouiller l'accès à une zone) et leurs clés d'accès. ZCU détecte le déclenchement du Screensaver pour fermer les zones chiffrées ouvertes et les clés d'accès.

D'autres composants sont également installés :

- Une extension de l'Explorateur Windows, «**ZCUSH**», qui personnalise les icônes des dossiers chiffrés (le comportement de ce composant est configurable dans les stratégies de sécurité), et qui affiche les propriétés des zones ; il peut également permette de chiffrer, déchiffrer, changer les accès des zones, si l'administrateur l'a autorisé ;

- L’extension Winlogon « **ZCCP** » qui permet d’entrer sa clé d’accès avant le login Windows ;
- Une interface graphique simple et légère pour les utilisateurs, «**ZCGU**» (‘Moniteur’) leur permet de voir la liste des zones chiffrées ouvertes, les clés d’accès présentées, et la version du logiciel. Il permet également de fermer manuellement des zones et des clés. Les actions qu’il autorise sont configurables dans une stratégie de sécurité ;
- Une interface graphique pour les administrateurs, « **ZoneBoard** » leur permet de visualiser et de gérer l’ensemble des accès cryptographique sur les zones chiffrées partagées.
- Deux outils de commande, «**ZCACMD**» et «**ZCUCMD**», le premier servant principalement à l’administrateur de la TOE pour la définition des zones chiffrées, le second étant un équivalent en mode commande de l’interface graphique «**ZCGU**».
- Un assistant de chiffrement « **ZCAPPLY** » qui est invoqué par ZoneCentral dés lors qu'une transformation de fichiers doit être effectuée : chiffrement, déchiffrement, transchiffrement. ZCAPPLY peut également être invoqué en mode commande par l’administrateur de la TOE.
- Un éditeur graphique de listes d’accès et de profils de zone, « **ZCEDIT** » permet à l’administrateur de la TOE de préparer le déploiement en amont et d’administrer ensuite les accès aux zones. ZCEDIT permet également d’effectuer le secours utilisateur (par l’opérateur de secours).

2.3.2. Périmètre de la TOE

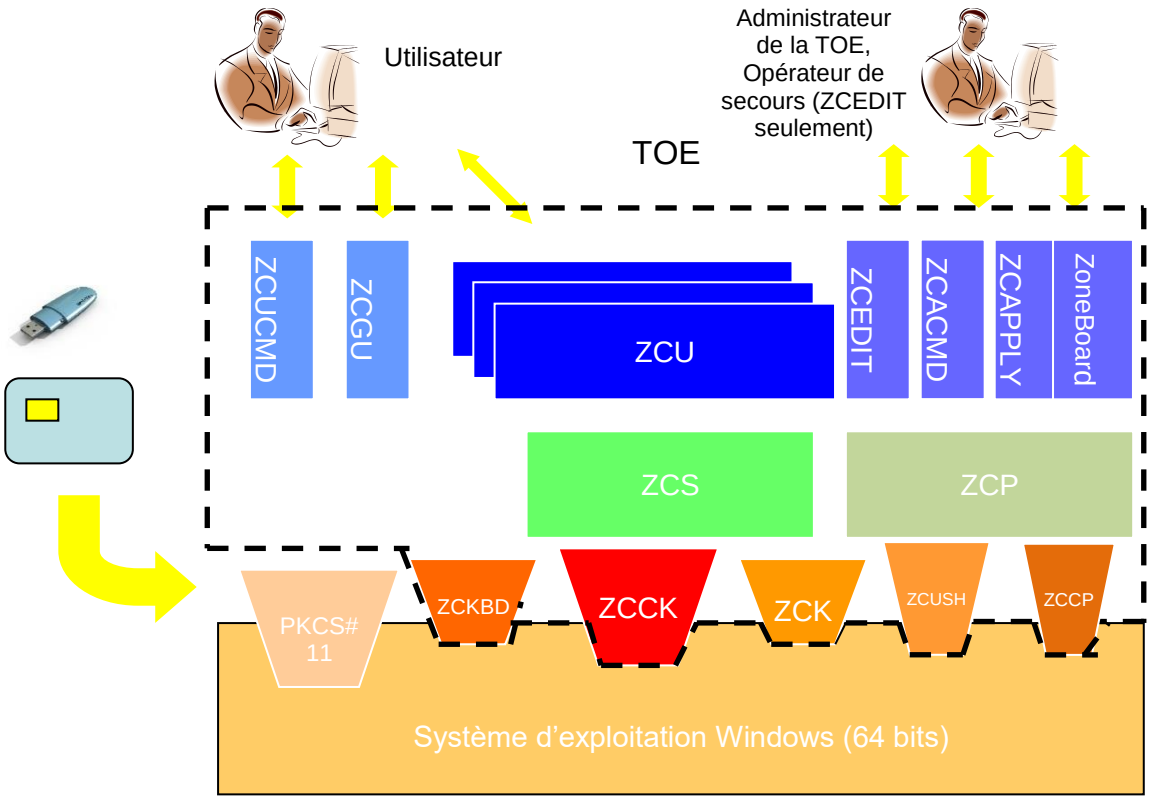

Figure 1 – Périmètre de la TOE

2.3.2.1 Périmètre logique

Seul le build 3030 configuré avec les politiques de sécurité activées suivantes est déclaré conforme :

- La politique P702 (durée de validité des mots de passe) doit être configurée à une valeur inférieure à 90 jours.
- 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 P380 (mécanisme de chiffrement) doit être configurée à « CTS-3 ».
- La politique P383 (mode de chiffrement RSA) doit être configurée à « PKCS#1 v2.2 avec utilisation de SHA-256 ».
- La politique P382 (autoriser l'utilisation du jeu d'instructions AES-NI) doit être configurée à « Non » (valeur par défaut).
- La politique P386 (mécanisme de signature) doit être configurée à « PKCS#1 v2.2 PSS ».

- La politique P292 (algorithme de hash utilisé) doit être configurée à « SHA-256 » (valeur par défaut)
- La politique P396 (contrôle des listes d'accès) doit être configurée à « contrôle de la signature et de la taille de clé ».

Le périmètre d'évaluation est constitué de l'ensemble des composants du logiciel (outils d'administration compris) hormis les fonctionnalités suivantes :

- L'outil GPOSign.exe permettant à l'administrateur de sécurité de signer les politiques. Par contre la vérification de la signature des politiques par ZoneCentral fait bien partie du périmètre de la TOE.
- L'utilisation du mode SSO (Single Sign On) qui permet d'ouvrir automatiquement les zones chiffrées lorsque la session Windows est ouverte (mais reporte le niveau de sécurité à celui de Windows ou du composant SSO tiers). Par contre l'entrée de la clé d'accès avant l'ouverture de session et qui permet à la fois d'ouvrir les zones et la session Windows est bien dans le périmètre.
- L'interface de programmation (API)

Le périmètre d'évaluation prend en compte la fourniture de clés d'accès dérivées à partir d'un mot de passe ou utilisant un certificat X509, ces certificats pouvant être stockés dans différents magasins et annuaires : magasins Windows locaux, fichiers de certificats et fichiers listes de certificats, annuaires LDAP, etc.

2.3.2.2 Périmètre physique

ZoneCentral sera évalué, en tant que produit, sur une plate-forme PC sous les systèmes d'exploitation de Microsoft suivants : Windows 7 et Windows 10 versions 1809 et 1903 (tous 64 bits).

L'utilisation avec les différentes clés d'accès sera évaluée (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, le dialogue réseaux entre la TOE et les données utilisateurs stockées sur des médias distants (serveur sur un réseau local ou sur Internet par exemple) 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 conteneurs CSP/CNG). Attention la dérivation des mots de passe utilisateur en clé d'accès fait bien partie du périmètre.

Le logiciel ZoneCentral utilise des clés utilisateurs (les «clés d'accès») fournis 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.

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

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

- Trois PC ou machines virtuelles équipés des systèmes d'exploitation suivants :
    - Windows 7 64 bits ;
    - Windows 10 version 1809 64 bits ;
    - Windows 10 version 1903 64 bits ;
- Un contrôleur de domaine (PC ou machine virtuelle) équipé de Windows Serveur 2008 R2 faisant également office de serveur de fichier (zone réseau).

Le type physique de porte-clés (carte à puce ou clé USB) étant transparent pour ZoneCentral (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.

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.

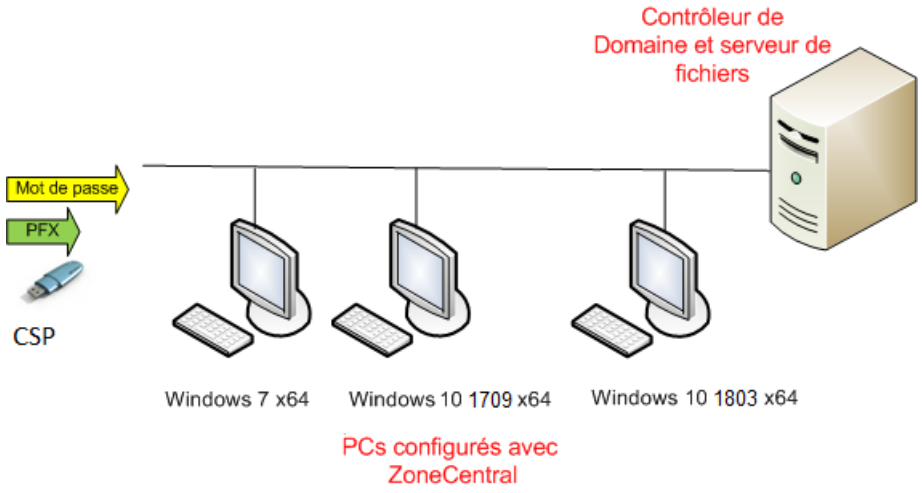

Figure 2 – Plate-forme de tests pour l'évaluation de la TOE

Il existe une combinatoire de 12 possibilités (3 systèmes d'exploitation et 4 moyens d'authentification). Les tests seront réalisés sur 4 combinatoires:

- Windows 7 et mot de passe
- Windows 10 version 1809 et fichier de clé (pfx)
- Windows 10 version 1903 et token physique
- Windows 10 version 1903 et CSP

L'analyse d'impact sur les autres combinatoires est étudiée dans le document « PRIMX-ZoneCentral 6.1 Analyse d'impact différentielle (PX176777) ».

3. Définition du problème de sécurité

3.1. Les biens sensibles

3.1.1. Biens sensibles de l'utilisateur

3.1.1.1 Clés d'accès : D. AUTH_USER

Pour ouvrir les zones chiffrées, ZoneCentral 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 : ZoneCentral 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 des zones chiffrées par cette clé d'accès. La politique de complexité des mots de passe est configurable par les politiques de sécurité.
- Accès par clé RSA (2048 à 4096 bits) hébergée dans un fichier de clés : ZoneCentral 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 des zones chiffrées par cette clé d'accès.
- Accès par clé RSA (2048 à 4096 bits) 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) : ZoneCentral gère la saisie du code confidentiel du token logique, le remet au composant externe pour le déverrouiller. ZoneCentral fournit également au composant externe la clé de chiffrement des zones chiffrée par sa clé publique. Le composant déchiffre la clé de chiffrement avec sa clé privée puis la transmet à ZoneCentral qui peut alors effectuer le déchiffrement des zones.
- Accès par clé RSA (2048 à 4096 bits) 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) : ZoneCentral ne gère pas la saisie du code confidentiel du token logique, c'est le composant externe qui le fait spontanément avec ses propres moyens. ZoneCentral 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 ZoneCentral qui peut alors effectuer le déchiffrement des zones.

En fonction de ces cas, donc, ZoneCentral 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 ZoneCentral 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 ZoneCentral (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 ou l'utilisateur 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.

3.1.1.2 Bi clé de signature : D.ID_ADMIN

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

3.1.1.3 Fichiers chiffrés : D.DONNEES_UTILISATEUR

ZoneCentral permet de conserver sous forme chiffrée les fichiers (et dossiers) relatifs à une zone chiffrée. Les fichiers ainsi chiffrés dans des zones chiffrées sont des biens sensibles de l'utilisateur protégés par la TOE (qui doit conserver leur image stockée chiffrée sans copie en clair) tant qu'ils demeurent dans leur zone chiffrée.

Que les fichiers soient stockés ou non dans des zones chiffrées, ZoneCentral procède à une surcharge de leur contenu dès lors que ces fichiers sont supprimés, quelle que soit la façon dont ils sont supprimés (action utilisateur ou par programme), ou lorsqu'ils sont redimensionnés (réduction de taille : le résidu est également surchargé avant la réduction). Les fichiers ainsi traités ne sont pas des biens sensibles de l'utilisateur au sens de la TOE pendant leur durée de vie, mais le deviennent dès lors qu'ils font l'objet d'une suppression (fin de vie).

Enfin ZoneCentral chiffre le ou les fichiers d'échange de la mémoire virtuelle du système (les fichiers 'swap') car ces fichiers contiennent des 'images mémoire instantanées' des applications actives, qui peuvent contenir des données utilisateur sensibles.

3.1.2. Biens sensibles de la TOE

3.1.2.1 Les clés symétriques de chiffrement de fichiers : D.CLES_ZONES

Les dossiers et fichiers des zones sont chiffrés par une clé de chiffrement générée lors de la création de la zone (clé AES 128, 192 ou 256 bits selon configuration, 256 bits par défaut). Ces biens sont stockés chiffrés par les accès dans le fichier de contrôle de la zone. A noter que toutes les zones chiffrées présentes dans le profil Windows de l'utilisateur, ou sous une de ses redirections, utilisent la même clé de chiffrement (clé de profil). Cela permet de fiabiliser la sauvegarde/restauration de fichiers chiffrés entre différentes zones du profil utilisateur. Ce comportement n'est pas préjudiciable puisque seul l'utilisateur (et le recouvrement) accède à ce profil.

3.1.2.2 Les programmes : D.PROGRAMMES

Pour assurer son fonctionnement, la TOE met en œuvre ses ***programmes*** (exécutables, drivers, bibliothèques dynamiques). La sécurité en intégrité de ces programmes est assurée par l'environnement : il faut être administrateur Windows pour les modifier. Ces programmes sont également signés (système authenticode Windows).

3.1.2.3 La configuration : D.POLITIQUES

Pour assurer son fonctionnement, la TOE met en œuvre des policies (plus précisément 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). 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 sécurité et vérifiées par ZoneCentral avant d'être appliquées.

3.1.2.4 Les fichiers de fonctionnement :

- ***Les fichiers de contrôle de zone*** **(D. FICHIERS_CONTROLE)**: il s'agit de fichiers délimitant et décrivant les zones chiffrées.

Ils contiennent le libellé de la zone, un identifiant unique, les exceptions applicables à la zone, quelques informations de gestion, et les 'wrappings' d'accès, c'est-à-dire la clé de chiffrement de la zone chiffrée par les clés d'accès des utilisateurs habilités à la zone. Un contrôle d'intégrité est effectué sur le fichier de contrôle.

Il existe un fichier de ce type par zone chiffrée, situé dans le dossier de tête de la zone chiffrée. Pour des raisons sanitaires, ces fichiers sont cachés, mais il en existe une copie visible (sous un autre nom) pour en permettre la sauvegarde.

- ***Les listes d'accès*** **(D.LISTES_ACCES)**: il s'agit de fichiers permettant de définir des accès indépendamment des zones elles-mêmes, pour une gestion plus simple, éventuellement centralisée, et/ou pour appliquer à plusieurs zones les mêmes accès.

Chacun de ces fichiers contient une clé RSA (2048 par défaut, 3072 ou 4096 bits selon configuration), appelée 'clé indirecte d'accès', dédiée au fichier et générée par le produit, chiffrée autant de fois que nécessaire par les différentes clés d'accès des utilisateurs de la liste.

Lorsqu'on applique une liste d'accès à une zone, on trouvera dans le fichier de contrôle de zone un «wrapping» d'accès correspondant calculé avec la clé publique de ce fichier d'accès.

3.1.2.5 Remarques

Le swap aurait pu être un bien sensible de la TOE, puisqu'il est susceptible de contenir des morceaux d'image mémoire de n'importe quel composant logiciel, dont ZoneCentral, et donc, notamment, les clés cryptographiques manipulées par ZoneCentral. Même si cela avait été le cas, elles auraient été protégées par le chiffrement du swap. Cependant, ce n'est pas le cas, car ZoneCentral utilise pour ces données en mémoire de la mémoire spéciale «non paginable» (disponible uniquement en mode Kernel pour les drivers).

Par ailleurs, ZoneCentral n'utilise aucun fichier temporaire en mode de fonctionnement 'utilisateur'. Ce n'est que lorsqu'une opération d'administration de zone est exécutée (création d'une zone chiffrée avec chiffrement initial des fichiers qu'elle contient) que ZoneCentral met en œuvre des fichiers temporaires pour assurer la fiabilité de

l’opération (points de reprise sur coupure de courant). Ces fichiers sont situés dans les zones elles-mêmes et sont effacés par surcharge en fin de traitement.

3.1.3. Synthèse des biens sensibles

Le tableau ci-dessous résume la liste des biens sensibles protégés par ZoneCentral 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 3.3). Une sensibilité nécessitant une protection en confidentialité ou intégrité 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 n'en nécessitant pas 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). De même la divulgation d'un fichier de contrôle de zone fournira le résultat du chiffrement des clés de zone par les clés d'accès (information inexploitable), par contre sa modification illicite ne doit pas conduire à pouvoir ouvrir la zone. A noter également que de manière générale, toute altération des clés (clés d'accès ou clé de zone) rendra impossible l'ouverture de la zone (ou bien conduira à un déchiffrement incohérent) mais ne portera pas atteinte à la confidentialité des données.

Remarque : de façon générale, l'intégrité n'est pas un objectif de ZoneCentral. 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, ZoneCentral 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 ZoneCentral : cas des mots de passe ou codes confidentiels éventuels (D.AUTH_USER).	Oui	*N/A*
Eléments des clés d'accès manipulés par ZoneCentral : cas des clés d'accès elles-mêmes si elles sont directement utilisées par ZoneCentral (D.AUTH_USER).	Oui	*Non*
Bi clé de signature pour l'utilisateur avec le rôle Administrateur de la TOE (D.ID_ADMIN)	Oui (clé privée)	*Non*
Fichiers et dossiers de l'utilisateur stockés dans des zones chiffrées, dans la corbeille ou dans le fichier swap (D.DONNEES_UTILISATEUR)	Oui	*Non*
Biens sensibles de la TOE		
Clés de chiffrement de zones (D.CLES_ZONES)	Oui	*Non*
Fichiers de contrôle des « zones » (D. FICHIERS_CONTROLE)	*Non*	Oui
Fichiers d'accès (D.LISTES_ACCES)	*Non*	Oui
Configuration de ZoneCentral (D.POLITIQUES)	*Non*	Oui
Programmes de ZoneCentral (D.PROGRAMMES)	*Non*	Oui

Tableau 1 : Synthèse des biens sensibles

3.2. Hypothèses

Pour ZoneCentral, 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 :

H.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 (clavier sans fil…) par d'autres utilisateurs ou attaquants potentiels. Des mesures organisationnelles adaptées doivent permettre à l'opérateur de secours d'authentifier l'utilisateur distant avant toute transmission du mot de passe de secours.
H.POSTE_SAIN	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 (i.e. lorsqu'une session est ouverte). 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.).
H.CONFIANCE_ADMIN	L'administrateur de la TOE et l'opérateur de secours sont des personnes de confiance. Les administrateurs Windows sont des personnes de confiance en charge de la configuration (avec des valeurs sures) des « policies ». Tous les administrateurs et opérateurs sont formés à l'utilisation de la TOE tout comme les utilisateurs.
H.CONSERVATION_CLES_ACCES	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 un administrateur de la TOE. L'administrateur de la TOE 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.
H.CERTIFICATS	L'administrateur de la TOE est 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.
H.ENV_PROTECT_TOE	L'environnement technique de la TOE assure l'intégrité des composantes de la TOE.

	L'administration et la mise à jour de la TOE sont assurées par des personnes formées et habilitées.
H.FIDELE_ENV	L'environnement d'exécution fournit à la TOE une date et une heure exacte pour assurer les fonctions d'horodatage.
H.ENV_ALEA	La TOE met en œuvre des mécanismes pour fournir les aléas nécessaires à la génération des secrets.
H.CRYPTO_EXT	Les clés d'accès générées ou stockées à l'extérieur de la TOE doivent être conformes au document [CRYPTO_STD] pour le niveau Standard.

3.3. Menaces

Les menaces présentes dans cette section sont uniquement celles portant atteinte à la sécurité de la TOE et non aux services rendus par la TOE (couvertes par les Politiques de Sécurité Organisationnelles, services du produit, décrites plus loin). Un agent menaçant est, d'une manière générale, une personne n'ayant pas le droit d'en connaitre et accédant à des zones chiffrées de l'utilisateur (zones locales suite à un vol ou un accès illégitime à la station de travail session non ouverte, partages réseau chiffrée, clé USB chiffrée).

Les administrateurs, les opérateurs de secours 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.

M.DETOURN_COMPOSANT	Un attaquant met en œuvre, éventuellement à bas niveau, les composants internes de la TOE, pour contourner certaines fonctions de sécurité. Il peut pour cela effectuer du «reverse-ingeniering» sur les programmes, développer des programmes d'appel des fonctions internes de la TOE ou s'aider d'un debugger. Il ne doit pas pouvoir, avec ces moyens, réussir à «pénétrer» une zone chiffrée dans laquelle il n'aurait pas normalement accès. Les biens impactés sont le programme de la TOE (intégrité) et les données utilisateur (confidentialité).
M.INT_POLITIQUE	Un attaquant modifie les politiques configurées par l'administrateur de sécurité. Il peut par exemple configurer son propre accès de recouvrement qui sera automatiquement ajouté comme accès licite lorsque les zones seront chiffrées. Le bien impacté

est la configuration (intégrité) et indirectement les données utilisateur (confidentialité).

M.ANALYSE_FIC_INTERNES Un attaquant copie les fichiers chiffrées d'une zone, avec les fichiers internes de la TOE associés et tente à partir de ces éléments de retrouver des informations protégées telles que les clés de chiffrement ou directement les fichiers utilisateurs (analyse par force brute ou faille due à un dysfonctionnement). Les biens impactés sont donc les clés de chiffrement de zone et les données utilisateur (tous en confidentialité).

M.INT_FIC_INTERNES Un attaquant modifie les fichiers internes de la TOE pour tenter d'accéder aux informations protégées (par exemple il modifie les exceptions dans le fichier de contrôle ou la liste d'accès 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.DONNEES_UTILISATEUR	M.DETOURN_COMPOSANT M.INT_POLITIQUE M.ANALYSE_FIC_INTERNES M.INT_FIC_INTERNES
D.CLES_ZONES	M.ANALYSE_FIC_INTERNES
D. FICHIERS_CONTROLE	M.INT_FIC_INTERNES
D.LISTES_ACCES	M.INT_FIC_INTERNES
D.POLITIQUES	M.INT_POLITIQUE
D.PROGRAMMES	M.DETOURN_COMPOSANT

Tableau 2 Association biens sensibles vers menaces

Note :

- D.AUTH_USER est couvert par H.NON_OBSERV et H.CONSERVATION_CLES_ACCES
- D.ID_ADMIN est couvert par l'hypothèse H.CONSERVATION_CLES_ACCES

3.4. Politiques de sécurité organisationnelles

OSP.ZONE	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. Pour des raisons de gestion, d'administration, et de facilité de compréhension, ce service doit se baser sur des périmètres («zones») définissables par l'administrateur de la TOE à l'intérieur desquels le service s'applique automatiquement.
OSP.ACCES	La TOE doit permettre aux utilisateurs de fournir une clé d'accès permettant d'accéder aux fichiers sensibles d'une zone protégée à laquelle ils désirent accéder. S'ils ne peuvent fournir une clé d'accès valide pour la zone considérée, l'accès doit être rejeté, quelle que soit l'application avec laquelle l'utilisateur effectue cet accès.
OSP.RECOUVREMENT	La TOE doit offrir un service de recouvrement des fichiers sensibles 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 de l'initialisation des zones. La TOE doit également permettre un recouvrement distant (secours utilisateur) si l'utilisateur a oublié son mot de passe ou perdu/cassé son porte-clés physique. 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.
OSP.ADMIN_ZONES	La TOE doit offrir un service de gestion des « zones » claires et chiffrées : créer une zone en clair, créer une zone chiffrée, déchiffrer une zone chiffrée, affecter un accès de recouvrement.
OSP.ADMIN_ACCES	La TOE doit offrir un service de gestion des accès aux zones chiffrées.
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.EFF_FICHIERS	La TOE doit offrir un service de surcharge, transparent pour l'utilisateur, pour tout fichier supprimé sur les volumes fixes locaux de son poste de travail, et pour tout fichier non effacé mais dont la taille est réduite (effacement du résidu de réduction).
OSP.SWAP	La TOE doit offrir un service de chiffrement, transparent pour les utilisateurs, des fichiers d'échanges de la mémoire virtuelle (swap) de Windows. Les clés des fichiers swap doivent être renouvelées automatiquement à chaque redémarrage du système.
OSP.CRYPTO	Le référentiel de l'ANSSI ([CRYPTO_STD], [CLES_STD] et [AUTH_STD]) défini pour le niveau de résistance standard doit être suivi pour la gestion des clés et pour les mécanismes cryptographiques et d'authentification utilisés dans la TOE.

4. Objectifs de sécurité

4.1. Objectifs de sécurité pour la TOE

4.1.1. Contrôle d'accès

O.AUTH	La TOE doit permettre d'identifier et authentifier tout utilisateur. Pour cela, la TOE ne doit autoriser l'accès à une zone chiffrée qu'après présentation d'une clé d'accès valide pour la zone.
O.ROLES	La TOE doit gérer trois rôles d'utilisateurs pour une zone chiffrée : un rôle 'utilisateur normal' ou plus simplement 'utilisateur' (utilisation des fichiers de la zone chiffrée sous condition de présentation d'une clé d'accès valide), un rôle 'administrateur' (utilisation, recouvrement local, plus possibilité d'administrer la zone chiffrée, c'est-à-dire gérer ses accès, la chiffrer et la déchiffrer complètement) et un rôle opérateur de secours (dépannage distant des utilisateurs). Le «pouvoir» d'un utilisateur doté du rôle «administrateur» sur une zone chiffrée peut être restreint globalement par les policies, qui peuvent lui interdire certaines actions (globalement, toutes zones confondues).

4.1.2. Cryptographie

O.CHIFFREMENT	La TOE doit chiffrer les « zones » configurées et les fichiers swap par l'emploi de clés cryptographiques. Les clés des fichiers swap sont renouvelées automatiquement à chaque redémarrage du système.
O.ALGO_STD	La TOE doit fournir un choix d'algorithmes cryptographiques et de tailles de clés conformes à l'état de l'art et aux standards de ce domaine, prévus dans [CRYPTO_STD] et complétés par [CLES_STD] et [AUTH_STD].

4.1.3. Gestion des zones

O.GEST_SECRETS	La TOE doit utiliser des clés différentes pour protéger les différentes «zones» configurées (hors zones dans le profil utilisateur Windows qui possèdent la même clé), même si les utilisateurs sont les mêmes pour ces « zones ».
O.ADM_ZONES	La TOE doit offrir une interface à l'administrateur, lui permettant de visualiser et gérer le chiffrement, le déchiffrement et le transchiffrement des «zones».
O.ADM_ACCES	La TOE doit offrir une interface à l'administrateur, comme à l'utilisateur, lui permettant de visualiser les accès et gérer les clés d'accès aux «zones» (en particulier l'accès de recouvrement).
O.RECOUVREMENT	La TOE doit permettre d'affecter des clés d'accès de recouvrement et de secours.

4.1.4. Effacement

O.EFF_RESIDUS	La TOE doit assurer le nettoyage des traces de données sensibles (fichiers utilisateurs ou clés d'accès) dans la mémoire (RAM) ou sur le disque dur (fichier SWAP ou temporaire), dès la fin des opérations réalisées par la TOE.
O.EFF_FICHIERS	La TOE doit offrir un service d'effacement par surcharge des fichiers supprimés sur les disques locaux, et des fichiers réduit en taille. Ce service doit s'appliquer notamment aux fichiers qui sont dans des zones en clair, mais peut également, par configuration, s'appliquer aux fichiers qui sont dans des zones chiffrées.

4.1.5. Protections lors de l'exécution

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.INT_CONTROLE	La TOE doit vérifier l'intégrité du fichier de contrôle à l'ouverture de zone. En cas d'échec lors de la vérification, l'accès à la zone doit être interdit.
O.AUDIT	La TOE doit générer des événements en rapport avec son fonctionnement dans le journal d'audit du système d'exploitation.

4.2. Objectifs de sécurité pour l'environnement

4.2.1. Utilisation

OE.NON_OBSERV	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). Des mesures organisationnelles adaptées doivent permettre à l'opérateur de secours d'authentifier l'utilisateur distant avant toute transmission du mot de passe de secours.
OE.ENV_OPERATIONNEL	Lorsque l'utilisateur est authentifié, l'environnement opérationnel doit assurer la confidentialité des données sensibles 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 entrainer 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.
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 (horodatage 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	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). L'administrateur de la TOE et l'opérateur de secours doivent recevoir une formation adaptée à leur fonction.
OE.CRYPTO_EXT	L'administrateur de la TOE doit être sensibilisé sur la qualité des clés d'accès qu'ils apportent 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.
OE.CONSERV_CLES	Les utilisateurs doivent conserver, dans un lieu sûr, les clés d'accès qui leurs ont été transmises par un administrateur de la TOE et empêcher leur divulgation. L'administrateur de la TOE doit conserver les clés de recouvrement et sa clé privée de signature dans un lieu sûr et empêcher leur divulgation.

4.2.3. Administration

OE.CERTIFICATS	L'administrateur de la TOE doit, 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 également aux certificats racines dits «authenticode» à partir desquels la vérification d'intégrité de la TOE peut être effectuée.
OE.CONFIANCE_ADMIN	L'administrateur de la TOE et l'opérateur de secours sont des personnes de confiance.. Les administrateurs Windows sont des personnes de confiance en charge de la configuration (avec des valeurs sures définies par l'administrateur de la TOE) des « policies ».
OE.ENV_PROTECT_TOE	L'environnement technique de la TOE assure l'intégrité des composantes de la TOE et notamment ses programmes. L'administration et la mise à jour de la TOE sont assurées par les administrateurs habilitées.

5. Exigences de sécurité des TI

5.1. Exigences de sécurité de la TOE

Dans cette section, les exigences de sécurité de la TOE ont été traduites en français afin d'améliorer leur compréhension. Le texte officiel servant de référence se trouve dans l'annexe A. Dans le texte français, toutes les opérations sur les composants (assignation, sélection, itération et raffinement) sont représentées par des caractères en italiques (et en caractères gras pour la partie servant de référence).

5.1.1. Exigences fonctionnelles de sécurité de la TOE

Les composants fonctionnels sélectionnés pour répondre aux objectifs de sécurité de la TOE sont les suivants :

Composants CC retenus	
FAU_GEN.1	Génération de données d'audit
FAU_GEN.2	Lien entre l'identité de l'utilisateur
FCS_CKM.1	Génération de clés cryptographiques
FCS_CKM.3	Accès aux clés cryptographiques
FCS_CKM.4	Destruction de clés cryptographiques
FCS_COP.1	Opération cryptographique
FDP_ACC.1	Contrôle d'accès partiel
FDP_ACF.1	Contrôle d'accès basé sur les attributs de sécurité
FDP_ITC.1	Importation depuis une zone hors du contrôle de la TSF
FDP_RIP.2	Protection totale des informations résiduelles
FIA_AFL.1	Gestion d'une défaillance de l'authentification
FIA_UAU.2	Authentification d'un utilisateur préalablement à toute action
FIA_UID.2	Identification d'un utilisateur préalablement à toute action
FMT_MOF.1	Administration des fonctions de la TSF
FMT_MSA.1	Gestion des attributs de sécurité
FMT_MSA.2	Attributs de sécurité sûrs
FMT_MSA.3	Initialisation statique d'attribut
FMT_MTD.1	Gestion des données de la TSF
FMT_SMF.1	Spécification des fonctions d'administration
FMT_SMR.1	Rôles de sécurité
FTA_SSL.3	Clôture de la session, initiée par la TSF

Tableau 3 : Exigences fonctionnelles de sécurité pour la TOE

5.1.1.1 Introduction

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

- Administrateur, opérateur de secours et utilisateurs de la TOE avec comme attributs de sécurité leur rôle et leur clé d'accès permettant ou non d'effectuer les opérations sur les zones et les accès.

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

- Zones chiffrées manipulés par les utilisateurs de la TOE et qui contiennent les données sensibles des utilisateurs (fichiers, clés),

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

- Gestion des zones (chiffrement/déchiffrement/transchiffrement)
- Gestion des accès (dont opérations de recouvrement et de secours)
- Utilisation des zones

5.1.1.2 Classe FAU : Audit de Sécurité

FAU_GEN	**Génération des données de l'audit de sécurité**
FAU_GEN.1	Génération de données d'audit
FAU_GEN.1.1	La TSF doit pouvoir générer un enregistrement d'audit des événements auditables suivants : a) démarrage et arrêt des fonctions d'audit ; b) tous les événements auditables pour le niveau d'audit *minimum* ; c) et : *- Evénements journalisés au titre de la gestion des zones ;* *- Evénements journalisés au titre de la gestion des accès aux zones ;* *- Evénements journalisés au titre de l'utilisation des zones (authentification, ouverture ou fermeture d'une zone) ;* *- Evénements journalisés au titre de la vérification des policies (réussite, échec, nouvelles politiques appliquées)*
FAU_GEN.1.2	La TSF doit enregistrer au minimum les informations suivantes dans chaque enregistrement d'audit : a) date et heure de l'événement, type d'événement, identité du sujet, ainsi que le résultat (succès ou échec) de l'événement ; b) et, pour chaque type d'événement d'audit, sur la base des définitions d'événements auditables contenues dans les composants fonctionnels inclus dans la ST, *pas d'autre information d'audit.*

FAU_GEN.2	Lien entre l'identité de l'utilisateur
FAU_GEN.2.1	Pour les enregistrements d'audit résultant d'actions d'utilisateur identifiés, la TSF doit pouvoir associer chaque événement auditable avec l'identité de l'utilisateur qui est à l'origine de l'événement.

5.1.1.3 Classe FCS : Support Cryptographique

FCS_CKM	**Gestion des clés cryptographiques**
FCS_CKM.1	Génération des clés cryptographiques
FCS_CKM.1.1	La TSF doit générer les clés cryptographiques conformément à un algorithme de génération de clés cryptographiques spécifié parmi les suivants - *génération de nombres pseudo-aléatoires utilisés pour la génération des clés de scellement des fichiers de contrôle, 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#12 à partir des mots de passe* et à des tailles de clés cryptographiques *de 128, 192 et 256 bits pour les clés symétriques et de 2048, 3072 et 4096 bits pour les clés asymétriques* qui satisfont *aux exigences cryptographiques de l'ANSSI définies dans [CRYPTO_STD] et [CLES_STD].*
FCS_CKM.3	Accès aux clés cryptographiques
ITFCS_CKM.3.1	La TSF doit réaliser *l'utilisation de clés* conformément à une méthode d'accès aux clés cryptographiques spécifiée *par utilisation du driver clavier et déchiffrement (« déwrapping ») des clés de zone par la clé d'accès.*
FCS_CKM.4	Destruction de clés cryptographiques
FCS_CKM.4.1	La TSF doit détruire les clés cryptographiques conformément à une méthode de destruction spécifiée de clés cryptographiques *par réécriture de motifs composés de zéros*.

FCS_COP	**Opération cryptographique**
FCS_COP.1	Opération cryptographique
FCS_COP.1.1	La TSF doit exécuter *le hachage, le calcul et la vérification d'intégrité, le chiffrement, le déchiffrement, la vérification de la signature des politiques de sécurité, le « wrapping » et « déwrapping » de clés* conformément à un algorithme cryptographique spécifié *SHA-256 et SHA-512, RSA, AES* et avec des tailles de clés cryptographiques *de 128, 192 et 256 bits pour les clés symétriques et de 2048 à 4096 bits pour les clés asymétriques* qui satisfont à ce qui suit: exigences cryptographique de l'*ANSSI définies dans [CRYPTO_STD] et [CLES_STD].*

5.1.1.4 Classe FDP : Protection des données de l'utilisateur

FDP_ACC	**Politique de contrôle d'accès**
FDP_ACC.1	Contrôle d'accès partiel
FDP_ACC.1.1	La TSF doit appliquer la politique *SFP.ACCESS_OBJ* aux : *Sujets: Utilisateurs, opérateur de secours et administrateur de la TOE* *Objets : Fichiers protégés par la TOE dans une « zone »* *Opérations : Gestion des zones, gestion des accès et utilisation.*

FDP_ACF	**Fonctions de contrôle d'accès**
FDP_ACF.1	Contrôle d'accès basé sur les attributs de sécurité
FDP_ACF.1.1	La TSF doit appliquer la politique *SFP.ACCESS_OBJ* aux objets en fonction des : *Sujets : Utilisateurs, opérateur de secours et administrateur de la TOE* *Attributs de sécurité : Clés d'accès utilisateur permettant ou non d'ouvrir la zone et rôle*.
FDP_ACF.1.2	La TSF doit appliquer les règles suivantes pour déterminer si une opération entre des sujets contrôlés et des objets contrôlés est autorisée : *Objet : Zone chiffrée* *Opération: Gestion des zones et utilisation* *Règle : authentification réussie après présentation de la clé d'accès associée à la zone concernée avec accès à la gestion des zones uniquement pour le rôle administrateur*
FDP_ACF.1.3	La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : *Aucune*.
FDP_ACF.1.4	La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de : *Aucune*.

FDP_ITC	**Importation depuis une zone hors du contrôle de la TSF**
FDP_ITC.1	Importation de données utilisateur sans attributs de sécurité
FDP_ITC.1.1	La TSF doit appliquer *la politique de sécurité des fonctions (SFP) SFP.ACCESS_OBJ* lors de l'importation de données utilisateur, contrôlées par les SFP, en provenance de l'extérieur de la TOE.
FDP_ITC.1.2	La TSF doit ignorer tout attribut de sécurité associé aux données utilisateur lorsqu'elles sont importées depuis l'extérieur de la TOE.
FDP_ITC.1.3	La TSF doit appliquer les règles suivantes lors de l'importation des données utilisateur contrôlées par la SFP en provenance de l'extérieur de la TOE : *Aucune*
FDP_RIP	**Protection des informations résiduelles**
FDP_RIP.2	Protection totale des informations résiduelles
FDP_RIP.2.1	La TSF doit garantir que toute information contenue précédemment dans une ressource est rendue inaccessible lors de *la désallocation de la ressource* de tous les objets.

5.1.1.5 Classe FIA : Identification et authentification

FIA_AFL	**Défaillances de l'authentification**
FIA_AFL.1	Gestion d'une défaillance de l'authentification
FIA_AFL.1.1	La TSF doit détecter le fait que *trois* tentatives d'authentification infructueuse ont eu lieu en relation avec *l'ouverture d'une zone.* Note : il a été nécessaire d'effectuer un raffinement éditorial afin de rendre le texte correct.
FIA_AFL.1.2	Quand le nombre spécifié de tentatives d'authentification infructueuses a été atteint ou dépassé, la TSF doit *temporiser l'accès à cette zone.*
FIA_UAU	**Authentification de l'utilisateur**
FIA_UAU.2	Authentification d'un utilisateur préalablement à toute action
FIA_UAU.2.1	La TSF doit exiger que chaque utilisateur soit authentifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.
FIA_UID	**Identification de l'utilisateur**
FIA_UID.2	Identification d'un utilisateur préalablement à toute action
FIA_UID.2.1	La TSF doit exiger que chaque utilisateur soit identifié avec succès avant d'autoriser toute autre action transitant par la TSF pour le compte de cet utilisateur.

5.1.1.6 Classe FMT : Administration de la sécurité

FMT_MOF	**Administration des fonctions de la TSF**
FMT_MOF.1	Administration du comportement des fonctions de sécurité
FMT_MOF.1.1	La TSF doit restreindre l'aptitude d'*activer ou désactiver* les fonctions *de gestion des zones et de gestion des accès à l'administrateur de la TOE.*
FMT_MSA	**Administration des attributs de sécurité**
FMT_MSA.1	Gestion des attributs de sécurité
FMT_MSA.1.1	La TSF doit mettre en œuvre la *politique SFP.ACCESS_OBJ* pour restreindre à *l'administrateur de la TOE* la possibilité de *changer la valeur par défaut, modifier ou supprimer* les attributs de sécurité *clés d'accès (clés RSA et clés dérivées de mots de passe des personnes ayant accès à la zone) et rôles (utilisateur, opérateur de secours et administrateur).*
FMT_MSA.2	Attributs de sécurité sûrs
FMT_MSA.2.1	La TSF doit garantir que seules des valeurs sûres sont acceptées pour les attributs de sécurité.
FMT_MSA.3	Initialisation statique d'attribut
FMT_MSA.3.1	La TSF doit mettre en œuvre *la politique SFP.ACCESS_OBJ* afin de fournir des valeurs par défaut *restrictives* pour les attributs de sécurité qui sont utilisés pour appliquer la SFP.
FMT_MSA.3.2	La TSF doit permettre à *l'administrateur de la TOE* de spécifier des valeurs initiales alternatives pour remplacer les valeurs par défaut lorsqu'un objet ou une information est créé.
FMT_MTD	**Gestion des données de la TSF**
FMT_MTD.1	Gestion des données de la TSF
FMT_MTD.1.1	La TSF doit restreindre, à *l'administrateur de la TOE*, la possibilité de *changer la valeur par défaut, modifier ou supprimer* les *stratégies de sécurité*.
FMT_SMF	**Spécification des fonctions d'administration**
FMT_SMF.1	Spécification des fonctions d'administration
FMT_SMF.1.1	La TSF doit être capable d'exécuter les fonctions d'administration suivantes : - *Les fonctions de gestion des zones* - *Les fonctions de gestion des accès (recouvrement et secours compris)*

FMT_SMR	Rôle pour l'administration de la sécurité
FMT_SMR.1	Rôles de sécurité
FMT_SMR.1.1	La TSF doit tenir à jour les rôles *administrateur de la TOE, opérateur de secours et utilisateur de la TOE*.
FMT_SMR.1.2	La TSF doit être capable d'associer les utilisateurs aux rôles

5.1.1.7 Classe FTA : Accès à la TOE

FTA_SSL	Verrouillage de session
FTA_SSL.3	Clôture de la session, initiée par la TSF
FTA_SSL.3.1	La TSF doit clôturer une session interactive *après un délai de 5 secondes d'inactivité de l'utilisateur, comptées à partir du lancement de l'économiseur d'écran Windows.*

5.1.2. Exigences d'assurance de sécurité de la TOE

Comme indiqué au paragraphe 3.3, la TOE doit être résistante aux attaques de pénétration effectuées par un attaquant ayant un potentiel d'attaque « enhanced-basic ».

Le niveau d'assurance visé par la TOE est le niveau :

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].

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 4 : Composants d'assurance de sécurité

Ce niveau d'assurance respecte les dépendances entre les composants d'assurance CC mentionnés dans la Partie 3 des Critères Communs.

6. Spécifications 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 qui sont signées par l'administrateur de la TOE et exploitées par la TOE après vérification de leur signature. Ces données définissent notamment les types d'accès supportés, les longueurs de clé utilisées (AES 256 bits par défaut), 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.GESTION_OP_ZONE Gestion des zones

Cette fonction de sécurité constitue le point d'entrée des opérations sur les zones (création et primo chiffrement, suppression, déchiffrement, transchiffrement, reprise en cas de problème, affichage des informations de zone …).

F.OPERATIONS_CRYPTO Implémentation des opérations cryptographiques

Cette fonction de sécurité couvre la génération des clés de scellement et de chiffrement ainsi que 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. Elle assure que ces opérations sont réalisées en utilisant des zones mémoires dédiées et met en œuvre le nettoyage des traces de données sensibles (fichiers utilisateurs ou clés d'accès) dans la mémoire (RAM) ou sur le disque dur (fichier SWAP ou temporaire), dès la fin des opérations réalisées.

F.GESTION_CLES_ACCES Gestion des clés

Cette fonction de sécurité gère les attributs de sécurité que sont les clés d'accès des utilisateurs et les rôles (utilisateur, opérateur de secours et administrateur de la TOE) qui leur sont associés. Un accès correspond à une clé d'accès (une clé cryptographique) que possède un utilisateur et permettant d'obtenir les éléments de la clé de chiffrement de zone. Si ces éléments sont extraits pour effectuer des opérations de gestion des accès, la clé d'accès présentée doit être associée au rôle administrateur de la TOE. Cette fonction gère également l'accès de recouvrement qui est un accès particulier ainsi que la clé permettant d'effectuer un secours utilisateur.

La fonction F.GESTION_CLES_ACCES réalise également les opérations de génération des clés RSA des listes d'accès, d'ajout et de suppression des clés d'accès ainsi que les opérations d'accès à ces clés (par l'intermédiaire des tokens pkcs#11 notamment).

F.ENTREE_SECURISEE **Entrée sécurisée**

Cette fonction de sécurité recouvre la communication sécurisée de données fournies en entrée de la TOE en utilisant pour cela des fonctions de chiffrement et déchiffrement de clé de zone et le driver clavier quand il s'agit d'entrer un mot de passe ou un code de fichier de clés.

F.CONTROLE_ACCES_ZONE **Contrôle d'accès aux zones**

Cette fonction de sécurité constitue l'interface obligatoire entre le système d'exploitation et les zones contrôlées par la TOE. La TSF autorise ou refuse l'accès à une zone chiffrée sur la base de la vérification d'un couple identifiant/authentifiant fourni par l'utilisateur de la TOE. Une temporisation est appliquée après trois échecs d'authentification consécutifs.

F.AUDIT **Audit**

Cette fonction de sécurité assure l'enregistrement des événements liés aux opérations réalisées par la TOE.

7. Annonces de conformité à un PP

Cette cible de sécurité ne déclare aucune conformité à un Profil de Protection.

8. Argumentaire

8.1. Argumentaire pour les objectifs de sécurité

Cette section présente les liens de couverture entre les objectifs de sécurité et les éléments qui constitue la définition de l'environnement de la TOE (hypothèses, politiques de l'organisation et menaces).

8.1.1. Hypothèses

Le tableau ci-dessous présente la couverture des hypothèses retenues par les objectifs de sécurité :

		OE.NON_OBSERV	OE.ENV_OPERATIONNEL	OE.HORODATAGE	OE.ENV_ALEA	OE.FORMATION	OE.CRYPTO_EXT	OE.CONSERV_CLES	OE.CERTIFICATS	OE.CONFIANCE_ADMIN	OE.ENV_PROTECT_TOE
Hypothèses	**H.NON_OBSERV**	X									
	H.POSTE_SAIN		X								
	H.CONFIANCE_ADMIN					X				X	
	H.CONSERVATION_CLES_ACCES					X		X			
	H.CERTIFICATS								X		
	H.ENV_PROTECT_TOE					X					X
	H.FIDELE_ENV			X							
	H.ENV_ALEA				X						
	H.CRYPTO_EXT						X				

Tableau 5 : Couverture des hypothèses par les objectifs de sécurité

H.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 (clavier sans fil…) par d'autres utilisateurs ou attaquants potentiels. Des mesures organisationnelles adaptées doivent permettre à l'opérateur de secours d'authentifier l'utilisateur distant avant toute transmission du mot de passe de secours.

L'objectif OE.NON_OBSERV couvre directement cette hypothèse en mettant à disposition de l'utilisateur un environnement adéquat.

H.POSTE_SAIN	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 (i.e. lorsqu'une session est ouverte). 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'objectif OE.ENV_OPERATIONNEL couvre directement cette hypothèse en mettant à disposition de l'utilisateur un environnement opérationnel adéquat.

H.CONFIANCE_ADMIN	L'administrateur de la TOE et l'opérateur de secours sont des personnes de confiance. Les administrateurs Windows sont des personnes de confiance en charge de la configuration (avec des valeurs sures) des « policies ». Tous les administrateurs et opérateurs sont formés à l'utilisation de la TOE tout comme les utilisateurs.

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

H.CONSERVATION_CLES_ACCES	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 un administrateur de la TOE. L'administrateur de la TOE 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.

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

H.CERTIFICATS	L'administrateur de la TOE est 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.

L'objectif OE.CERTIFICATS couvre directement cette hypothèse.

H.ENV_PROTECT_TOE	L'environnement technique de la TOE assure l'intégrité des composantes de la TOE. L'administration et la mise à jour de la TOE sont assurées par des personnes formées et habilitées.

Les objectifs OE.ENV_PROTECT_TOE et OE.FORMATION couvrent cette hypothèse en assurant l'intégrité des programmes de la TOE et en formant les administrateurs.

H.FIDELE_ENV	L'environnement d'exécution fournit à la TOE une date et une heure exacte pour assurer les fonctions d'horodatage.

L'objectif OE.HORODATAGE couvre directement cette hypothèse.

H.ENV_ALEA	La TOE met en œuvre des mécanismes pour fournir les aléas nécessaires à la génération des secrets.

L'objectif OE.ENV_ALEA couvre directement cette hypothèse.

H.CRYPTO_EXT	Les clés d'accès générées ou stockées à l'extérieur de la TOE doivent être conformes au document [CRYPTO_STD] pour le niveau Standard.

L'objectif OE.CRYPT_EXT couvre directement cette hypothèse.

8.1.2. Menaces

Le tableau ci-dessous présente les liens de couverture entre les objectifs de sécurité et les menaces retenues :

		O.AUTH	O.ROLES	O.CHIFFREMENT	O.ALGO_STD	O.GEST_SECRETS	O.ADM_ZONES	O.ADM_ACCES	O.RECOUVREMENT	O.EFF_RESIDUS	O.EFF_FICHIERS	O.INT_POLICIES	O.INT_CONTROLE	O.AUDIT	OE.CONSERV_CLES	OE.ENV_PROTECT_TOE
Menaces	**M.DETOURN_COMPOSANT**	X			X					X						X
	M.INT_POLITIQUE											X		X	X	
	M.ANALYSE_FIC_INTERNES	X			X	X										
	M.INT_FIC_INTERNES	X			X								X			

Tableau 6 : Couverture des menaces par les objectifs de sécurité

M.DETOURN_COMPOSANT	Un attaquant met en œuvre, éventuellement à bas niveau, les composants internes de la TOE, pour contourner certaines fonctions de sécurité. Il peut pour cela effectuer du «reverse-ingeniering» sur les programmes, développer des programmes d'appel des fonctions internes de la TOE ou s'aider d'un debugger. Il ne doit pas pouvoir, avec ces moyens, réussir à «pénétrer» une zone chiffrée dans laquelle il n'aurait pas normalement accès. Les biens impactés sont le programme de la TOE (intégrité) et les données utilisateur (confidentialité).

➔ Pour prévenir cette menace, la TOE doit :

- Garantir le fait qu'avant toute opération sur la TOE, une authentification est nécessaire (O.AUTH),
- Garantir le fait que l'environnement et les administrateurs assurent un contrôle sur l'intégrité des programmes (lors de l'installation et la mise à jour notamment) (OE.ENV_PROTECT_TOE).

➔ Pour se protéger, la TOE doit :

- Garantir le fait qu'il n'est pas possible, cryptographiquement, d'accéder aux données sensibles d'une zone chiffrée sans fournir une clé d'accès valide : le détournement d'un composant (i.e. sa mise en œuvre de façon détournée ou non prévue) ne peut pas permettre de franchir cette barrière (O.ALGO_STD),
- Garantir le fait que la TOE ne conserve pas de résidus permettant de présenter un chemin pour une attaque lors d'un détournement postérieur (O.EFF_RESIDUS).

➔ Pour détecter l'occurrence de la menace, la TOE doit :

rien

➔ Pour limiter l'impact de la menace, la TOE doit :

Rien

M.INT_POLITIQUE	Un attaquant modifie les politiques configurées par l'administrateur de sécurité. Il peut par exemple configurer son propre accès de recouvrement qui sera automatiquement ajouté comme accès licite lorsque les zones seront chiffrées. Le bien impacté est la configuration (intégrité) et indirectement les données utilisateur (confidentialité).

➔ Pour prévenir cette menace, la TOE doit :

- Garantir le fait que l'administrateur de sécurité conserve sa clé privée de signature dans un lieu sûr (OE.CONSERV_CLES)

➔ Pour se protéger, la TOE doit :

- Garantir le fait qu'il n'est pas possible d'appliquer des politiques de sécurité (et donc modifier le fichier des politiques) sans qu'elles soient signées par la clé privée du responsable de sécurité (O.INT_POLICIES)

➔ Pour détecter l'occurrence de la menace, la TOE doit :

Tracer la vérification de toute nouvelle politique appliquée, succès ou échec (O.AUDIT).

➔ Pour limiter l'impact de la menace, la TOE doit :

Rien

M.ANALYSE_FIC_INTERNES	Un attaquant copie les fichiers chiffrées d'une zone, avec les fichiers internes de la TOE associés et tente à partir de ces éléments de retrouver des informations protégées telles que les clés de chiffrement ou directement les fichiers utilisateurs (analyse par force brute ou faille due à un dysfonctionnement). Les biens impactés sont donc les clés de chiffrement de zone et les données utilisateur (tous en confidentialité).

➔ Pour prévenir cette menace, la TOE doit :

- Garantir le fait qu'avant toute opération sur la TOE, une authentification est nécessaire (O.AUTH).

➔ Pour se protéger, la TOE doit :

- Garantir le fait qu'il n'est pas possible, cryptographiquement, de retrouver les clés de chiffrement de zones sans fournir une clé d'accès valide, et par le fait que cet objectif prévoit que les fichiers internes de la TOE respectent également ce principe (O.AUTH et O.ALGO_STD).

➔ Pour détecter l'occurrence de la menace, la TOE doit :

rien

➔ Pour limiter l'impact de la menace, la TOE doit :

- Garantir le fait que les fichiers de contrôle des différentes zones (hors zones à l'intérieur du profil utilisateur) sont rendus «cryptographiquement différents» par l'utilisation de clés de chiffrement différentes, ne permettant pas de tirer des enseignements d'un fichier interne d'une zone pour attaquer la clé d'une autre zone (O.GEST_SECRETS).

M.INT_FIC_INTERNES	Un attaquant modifie les fichiers internes de la TOE pour tenter d'accéder aux informations protégées (par exemple il modifie le fichier de contrôle ou la liste d'accès 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).

➔ Pour prévenir cette menace, la TOE doit :

- Garantir le fait qu'avant toute opération sur la TOE, une authentification est nécessaire (O.AUTH),

➔ Pour se protéger, la TOE doit :

- Garantir le fait qu'il n'est pas possible, cryptographiquement, de retrouver les clés de chiffrement de zones sans fournir une clé d'accès valide (O.AUTH) en utilisant des algorithmes standards (O.ALGO_STD). En effet, toute modification d'un fichier interne, par exemple pour s'ajouter comme accès, nécessite de chiffrer (et donc de retrouver) la clé de chiffrement de zone par la clé d'accès de l'attaquant.
- Garantir le fait que toute modification du fichier de contrôle (pour modifier les exceptions par exemple) est détectée et empêche l'accès à la zone (O.INT_CONTROLE).

➔ Pour détecter l'occurrence de la menace, la TOE doit :

rien

➔ Pour limiter l'impact de la menace, la TOE doit :

rien

8.1.3. Politiques de sécurité de l'organisation

Le tableau ci-dessous présente les liens de couverture entre les objectifs de sécurité et les politiques de sécurité de l'organisation retenues :

		O.AUTH	O.ROLES	O.CHIFFREMENT	O.ALGO_STD	O.GEST_SECRETS	O.ADM_ZONES	O.ADM_ACCES	O.RECOUVREMENT	O.EFF_RESIDUS	O.EFF_FICHIERS	O.INT_POLICIES	O.INT_CONTROLE	O.AUDIT
OSP	**OSP.ZONES**	X		X		X				X			X	X
	OSP.ACCES	X								X				X
	OSP.RECOUVREMENT	X	X						X	X				X
	OSP.ADMIN_ZONES	X	X	X			X			X				X
	OSP.ADMIN_ACCES	X	X					X		X				X
	OSP.VERIF_POLICIES											X		X
	OSP.EFF_FICHIERS										X			
	OSP.SWAP			X						X				
	OSP.CRYPTO				X					X				

Tableau 7 : Couverture des politiques de sécurité de l'organisation par les objectifs de sécurité

OSP.ZONE	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. Pour des raisons de gestion, d'administration, et de facilité de compréhension, ce service doit se baser sur des périmètres («zones») définissables par l'administrateur de la TOE à l'intérieur desquels le service s'applique automatiquement.

Note: cette politique ne concerne pas la création initiale de la zone (avec le chiffrement de son contenu initial), qui relève de OSP.ADMIN_ZONES, mais le fait qu'une fois la zone créée, tout fichier déposé dans la zone, quelle que soit la méthode, est stocké chiffré. Cette politique ne concerne pas non plus les accès à la zone, qui relèvent de OSP.ACCES (et OSP.ADMIN_ACCES).

➔ Pour mettre en œuvre la politique, la TOE :

- Chiffre les fichiers dans les zones (O.CHIFFREMENT) ;
- Utilise des clés différentes pour protéger les différentes « zones » configurées (O.GEST_SECRETS).
- Demande une authentification avant de déposer tous fichiers dans la zone chiffrée (O.AUTH).

➔ Pour garantir la mise en œuvre de la politique, la TOE :

- Efface les traces mémoire liées aux clés de chiffrement des zones (O.EFF_RESIDUS) ;
- Vérifie que le fichier de contrôle n'a pas été compromis pour modifier les fichiers de la zone en exception par exemple (O.INT_CONTROLE).

➔ Pour contrôler la mise en œuvre de la politique, la TOE :

- Enregistre les événements relatifs au traitement de la zone (O.AUDIT).

OSP.ACCES	La TOE doit permettre aux utilisateurs de fournir une clé d'accès permettant d'accéder aux fichiers sensibles d'une zone protégée à laquelle ils désirent accéder. S'ils ne peuvent fournir une clé d'accès valide pour la zone considérée, l'accès doit être rejeté, quelle que soit l'application avec laquelle l'utilisateur effectue cet accès.

Note : cette politique ne concerne pas la gestion des accès (ajout ou suppression), mais l'utilisation d'un accès.

➔ Pour mettre en œuvre la politique, la TOE :

- Demande une authentification avant tout accès à une zone chiffrée et attribue un rôle à l'utilisateur (O.AUTH) ;
- Fait en sorte que seule une clé d'accès valide puisse permettre de retrouver les clés de chiffrement d'une zone, et que les fichiers ou informations internes de la TOE ne permettent pas de faire autrement (O.AUTH).

➔ Pour garantir la mise en œuvre de la politique, la TOE :

- Efface les traces mémoire liées aux éventuels calculs cryptographiques intermédiaires (dérivation de mots de passe) ou au transport des valeurs de clés de chiffrement lorsqu'elles sont calculées par un dispositif cryptographique externe (token) (O.EFF_RESIDUS) ;

➔ Pour contrôler la mise en œuvre de la politique, la TOE :

- Enregistre les événements en relation avec l'utilisation (ouverture ou fermeture) d'une zone (O.AUDIT).

OSP.RECOUVREMENT	La TOE doit offrir un service de recouvrement des fichiers sensibles 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 de l'initialisation des zones. La TOE doit également permettre un recouvrement distant (secours utilisateur) si l'utilisateur a oublié son mot de passe ou perdu/cassé son porte-clés physique. 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.

➔ Pour mettre en œuvre la politique, la TOE :

- Demande une authentification pour accéder à la gestion des clés de recouvrement et de secours (O.AUTH) ;
- Permet d'affecter des clés d'accès de recouvrement et de secours (O.RECOUVREMENT) ;
- N'autorise que l'administrateur de la sécurité et l'opérateur de secours à effectuer respectivement les opérations de recouvrement et de secours (O.ROLES) ;

➔ Pour garantir la mise en œuvre de la politique, la TOE :

- Efface les traces mémoire liées aux éventuels calculs cryptographiques intermédiaires (O.EFF_RESIDUS) ;

➔ Pour contrôler la mise en œuvre de la politique, la TOE :

- Enregistre les événements en relation avec l'ouverture par un accès de recouvrement ou un accès de secours (O.AUDIT).

OSP.ADMIN_ZONES	La TOE doit offrir un service de gestion des « zones » claires et chiffrées : créer une zone en clair, créer une zone chiffrée, déchiffrer une zone chiffrée, affecter un accès de recouvrement.

➔ Pour mettre en œuvre la politique, la TOE :

- Demande une authentification avant de permettre la gestion des zones (O.AUTH) ;
- Offre une interface à l'administrateur, lui permettant de visualiser et gérer le chiffrement, le déchiffrement et le transchiffrement des « zones » (O.ADM_ZONES).

➔ Pour garantir la mise en œuvre de la politique, la TOE :

- Chiffre les fichiers quand on crée une zone chiffrée (chiffrement initial des fichiers qu'elle contient), déchiffre les fichiers quand on crée une zone en clair (déchiffrement quand les fichiers étaient initialement chiffrés) (O.CHIFFREMENT) ;
- Efface les traces mémoires des clés de chiffrement manipulées, mais intervient également plus fortement pour l'effacement de la version «en clair» des fichiers lorsqu'on crée une zone chiffrée (effacement de l'original) (O.EFF_RESIDUS).

➔ Pour contrôler la mise en œuvre de la politique, la TOE :

- Contrôle que seul un utilisateur disposant du rôle 'administrateur' dans une zone chiffrée existante a le droit d'intervenir sur cette zone (la déchiffrer, …) (O.ROLES) ;
- Enregistre les événements en relation avec la gestion d'une zone (O.AUDIT).

OSP.ADMIN_ACCES	La TOE doit offrir un service de gestion des accès aux zones chiffrées.

➔ Pour mettre en œuvre la politique, la TOE :

- Demande une authentification avant de permettre la gestion des accès aux zones chiffrées (O.AUTH) ;
- Offre une interface à l'administrateur, comme à l'utilisateur, lui permettant de visualiser les accès et gérer les clés d'accès aux « zones » (O.ADM_ACCES).

➔ Pour garantir la mise en œuvre de la politique, la TOE :

- Efface les traces mémoires des clés de chiffrement manipulées (O.EFF_RESIDUS).

➔ Pour contrôler la mise en œuvre de la politique, la TOE :

- Contrôle que seul un utilisateur disposant du rôle 'administrateur' dans une zone chiffrée existante a le droit d'intervenir sur cette zone (la déchiffrer, …) (O.ROLES) ;
- Enregistre les événements en relation avec la gestion des accès à une zone (O.AUDIT).

P.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.

➔ Pour mettre en œuvre la politique, la TOE :

- Vérifier la signature des nouvelles politiques de sécurité appliquées et refuser leur application si la signature est incorrecte (O.INT_POLICIES).

➔ Pour garantir la mise en œuvre de la politique, la TOE :

Rien

➔ Pour contrôler la mise en œuvre de la politique, la TOE :

- Enregistre les événements en relation avec la vérification des politiques (O .AUDIT).

OSP.EFF_FICHIERS	La TOE doit offrir un service de surcharge, transparent pour l'utilisateur, pour tout fichier supprimé sur les volumes fixes locaux de son poste de travail, et pour tout fichier non effacé mais dont la taille est réduite (effacement du résidu de réduction).

➔ Pour mettre en œuvre la politique, la TOE :

- Offre un service d'effacement par surcharge des fichiers supprimés sur les disques locaux. Ce service s'applique notamment aux fichiers qui sont dans des zones en clair, mais peut également, par configuration, s'appliquer aux fichiers qui sont dans des zones chiffrées (O.EFF_FICHIERS).

➔ Pour garantir la mise en œuvre de la politique, la TOE :

rien

➔ Pour contrôler la mise en œuvre de la politique, la TOE :

Rien

OSP.SWAP	La TOE doit offrir un service de chiffrement, transparent pour les utilisateurs, des fichiers d'échanges de la mémoire virtuelle (swap) de Windows. Les clés des fichiers swap doivent être renouvelées automatiquement à chaque redémarrage du système.

➔ Pour mettre en œuvre la politique, la TOE :

- Génère une nouvelle clé de chiffrement du swap à chaque démarrage du système, chiffre les fichiers quand on crée une zone chiffrée (chiffrement initial des fichiers qu'elle contient), déchiffre les fichiers quand on crée une zone en clair (déchiffrement quand les fichiers étaient initialement chiffrés) (O.CHIFFREMENT).

➔ Pour garantir la mise en œuvre de la politique, la TOE :

- Efface les traces mémoires des clés de chiffrement manipulées (O.EFF_RESIDUS) ;

➔ Pour contrôler la mise en œuvre de la politique, la TOE :

Rien

OSP.CRYPTO	Le référentiel de l'ANSSI ([CRYPTO_STD], [CLES_STD] et [AUTH_STD]) défini pour le niveau de résistance standard doit être suivi pour la gestion des clés et pour les mécanismes cryptographiques et d'authentification utilisés dans la TOE.

➔ Pour mettre en œuvre la politique, la TOE :

- Fournit un choix d'algorithmes cryptographiques et de tailles de clés conformes à l'état de l'art et aux standards de ce domaine, prévus dans [CRYPTO_STD] (O.ALGO_STD),
- Efface les traces mémoires des clés de chiffrement manipulées (O.EFF_RESIDUS).

➔ Pour garantir la mise en œuvre de la politique, la TOE :

rien

➔ Pour contrôler la mise en œuvre de la politique, la TOE :

rien

8.2. Argumentaire pour les exigences de sécurité

8.2.1. Dépendances entre exigences fonctionnelles de sécurité

Le tableau ci-dessous présente la couverture des dépendances entre les composants fonctionnels sélectionnés :

Composant	Dépendances	Dépendances satisfaites
FAU_GEN.1	FPT_STM.1*	
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2
FCS_CKM.1	[FCS_CKM.2 ou FCS_COP.1], FCS_CKM.4	FCS_COP.1, FCS_CKM.4
FCS_CKM.3	[FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FCS_CKM.4	FDP_ITC.1, FCS_CKM.1, FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1]	FDP_ITC.1, FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FCS_CKM.4	FDP_ITC.1, FCS_CKM.1, FCS_CKM.4
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FDP_ITC.1	[FDP_ACC.1 ou FDP_IFC.1], FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FDP_RIP.2	Aucune	Aucune
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	Aucune	Aucune
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 ou FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.2	[FDP_ACC.1 ou FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	Aucune	Aucune
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FTA_SSL.3	Aucune	Aucune

Tableau 8 : Satisfaction des dépendances entre exigences fonctionnelles de sécurité

8.2.2. Dépendances entre exigences d'assurance de sécurité

Le tableau ci-dessous présente la couverture des dépendances entre les composants d'assurance sélectionnés :

Composant	Dépendances	Dépendances satisfaites
ADV_ARC.1	ADV_FSP.1, 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	Aucune	Aucune
ALC_CMC.3	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	Aucune	Aucune
ALC_DEL.1	Aucune	Aucune
ALC_DVS.1	Aucune	Aucune
ALC_FLR.3	Aucune	Aucune
ALC_LCD.1	Aucune	Aucune
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.2
ASE_ECD.1	Aucune	Aucune
ASE_INT.1	Aucune	Aucune
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1
ASE_SPD.1	Aucune	Aucune
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.2, ADV_FSP.3
ATE_COV.2	ADV_FSP.2, ATE_FUN.1	ADV_FSP.3, ATE_FUN.1
ATE_DPT.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.2
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.3, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.3	ADV_ARC.1, ADV_FSP.4**, ADV_TDS.3**, ADV_IMP.1**, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Tableau 9 : Satisfaction des dépendances entre exigences d'assurance de sécurité

8.2.3. Argumentaire pour les dépendances non satisfaites

*La dépendance FAU_GEN.1 avec FPT_STM.1 n'est pas réalisée dans la mesure où la base de temps est fournie par la station de travail (recommandations à ce propos fournies dans le guide d'utilisation).

** La dépendance AVA_VAN.3 avec ADV_FSP.4, ADV_IMP.1 et ADV_TDS.3 ne sont pas satisfaites par construction du paquet d'assurance de la qualification de niveau standard défini par l'ANSSI.

8.2.4. Argumentaire de couverture des objectifs de sécurité par les exigences fonctionnelles

Les tableaux ci-dessous présentent la couverture des composants fonctionnels sélectionnés par les objectifs de sécurité :

Objectifs de sécurité de la TOE	FAU_GEN.1	FAU_GEN.2	FCS_CKM.1	FCS_CKM.3	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_ITC.1	FDP_RIP.2	FIA_AFL.1	FIA_UAU.2	FIA_UID.2	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FTA_SSL.3
O.AUTH							X	X	X		X	X	X								X
O.ROLES							X	X						X	X			X	X	X	
O.CHIFFREMENT			X	X		X															
O.ALGO_STD			X	X	X	X															
O.GEST_SECRETS			X																		
O.ADM_ZONES														X					X	X	
O.ADM_ACCES														X	X	X	X		X	X	
O.RECOUVREMENT														X				X	X	X	
O.EFF_RESIDUS					X					X											
O.EFF_FICHIERS										X											
O.INT_POLICIES						X												X			
O.INT_CONTROLE			X			X															
O.AUDIT	X	X																			

Tableau 10 : Couverture des objectifs de sécurité par les exigences fonctionnelles de sécurité

8.2.4.1 Contrôle d'accès

O.AUTH	La TOE doit permettre d'identifier et authentifier tout utilisateur. Pour cela, la TOE ne doit autoriser l'accès à une zone chiffrée qu'après présentation d'une clé d'accès valide pour la zone.

Afin de remplir cet objectif :

- La TOE identifie et authentifie chaque utilisateur avant de permettre toute opérations (FIA_UID.2 et FIA_UAU.2) et applique une règle de ralentissement d'affichage de la mire de connexion à un utilisateur, suite à plusieurs essais d'authentification infructueux (FIA_AFL.1).
- Pour que la TOE donne l'accès à une zone chiffrée, l'utilisateur doit présenter sa clé d'accès (token USB par exemple) en vue de son authentification (FDP_ITC.1). La TOE applique ensuite une politique de contrôle d'accès aux « zones » (FDP_ACC.1) et aux objets de la « zones » basé sur les attributs de sécurité (FDP_ACF.1).
- La TOE peut ensuite, à l'activation de l'économiseur d'écran, fermer les zones ouvertes de l'utilisateur (FTA_SSL.3) pour forcer la présentation d'une clé d'accès valide en cas d'absence momentanée de l'utilisateur.

O.ROLES	La TOE doit gérer trois rôles d'utilisateurs pour une zone chiffrée : un rôle 'utilisateur normal' ou plus simplement 'utilisateur' (utilisation des fichiers de la zone chiffrée sous condition de présentation d'une clé d'accès valide), un rôle 'administrateur' (utilisation, recouvrement local, plus possibilité d'administrer la zone chiffrée, c'est-à-dire gérer ses accès, la chiffrer et la déchiffrer complètement) et un rôle opérateur de secours (dépannage distant des utilisateurs). Le «pouvoir» d'un utilisateur doté du rôle «administrateur» sur une zone chiffrée peut être restreint globalement par les policies, qui peuvent lui interdire certaines actions (globalement, toutes zones confondues).

Afin de remplir cet objectif :

- La TOE doit gérer et distinguer les rôles d'administrateur de la TOE, opérateur de secours et utilisateur de la TOE (FMT_SMR.1)
- La TOE permet aussi de contrôler l'accès des utilisateurs aux « zones » et aux opérations sur ces « zones » (FDP_ACC.1), et de restreindre l'accès aux seuls utilisateurs possédant l'identifiant de la « zone » et la clé d'accès associée (FDP_ACF.1).
- La TOE doit donner la possibilité ou non à l'administrateur d'utiliser certaines fonctions de sécurité en fonction des politiques configurées (FMT_MOF.1).
- La TOE assure que seuls l'administrateur de la TOE peut gérer l'attribut de sécurité « rôles » (FMT_MSA.1).

- Enfin, la TOE doit permettre de restreindre à l'administrateur de la TOE les fonctions d'administration de la sécurité (FMT_SMF.1) et la gestion des « policies » (FMT_MTD.1).

8.2.4.2 Cryptographie

O.CHIFFREMENT	La TOE doit chiffrer les « zones » configurées et les fichiers swap par l'emploi de clés cryptographiques. Les clés des fichiers swap sont renouvelées automatiquement à chaque redémarrage du système.

Afin de remplir cet objectif :

- Pour chiffrer les zones configurées et les fichiers de swap, la TOE doit tout d'abord être capable de générer les clés cryptographiques (FCS_CKM.1) et y accéder de manière sécurisée (FCS_CKM.3), afin de les utiliser pour réaliser les opérations cryptographiques selon différents algorithmes (FCS_COP.1).

O.ALGO_STD	La TOE doit fournir un choix d'algorithmes cryptographiques et de tailles de clés conformes à l'état de l'art et aux standards de ce domaine, prévus dans [CRYPTO_STD] et complétés par [CLES_STD] et [AUTH_STD].

Afin de remplir cet objectif :

- La TOE doit être capable de fournir un choix d'algorithmes de génération (FCS_CKM.1), d'accès (FCS_CKM.3) et de destruction (FCS_CKM.4) de clés cryptographiques.
- Elle doit aussi permettre d'exécuter des opérations cryptographiques conformément à des algorithmes et tailles de clés cryptographique spécifiés (FCS_COP.1).

8.2.4.3 Gestion des zones

O.GEST_SECRETS	La TOE doit utiliser des clés différentes pour protéger les différentes «zones» configurées (hors zones dans le profil utilisateur Windows qui possèdent la même clé), même si les utilisateurs sont les mêmes pour ces « zones ».

Afin de remplir cet objectif :

- La TOE doit protéger les « zones » configurées en générant des clés cryptographiques différentes (FCS_CKM.1).

O.ADM_ZONES	La TOE doit offrir une interface à l'administrateur, lui permettant de visualiser et gérer le chiffrement, le déchiffrement et le transchiffrement des «zones».

Afin de remplir cet objectif :

- La TOE offre des fonctions d'administration et de gestions (FMT_SMF.1) des zones.
- La TOE limite les accès à ces fonctions d'administration et de gestion en fonction du rôle associé aux utilisateurs (FMT_SMR.1).
- La TOE donne la possibilité ou non à l'administrateur d'utiliser certaines fonctions de gestion des zones en fonction des politiques configurées (FMT_MOF.1).

O.ADM_ACCES	La TOE doit offrir une interface à l'administrateur, comme à l'utilisateur, lui permettant de visualiser les accès et gérer les clés d'accès aux «zones» (en particulier l'accès de recouvrement).

Afin de remplir cet objectif :

- La TOE offre des fonctions d'administration et de gestions (FMT_SMF.1) des accès
- La TOE limite les accès à ces fonctions d'administration et de gestion en fonction du rôle associé aux utilisateurs (FMT_SMR.1).
- La TOE donne la possibilité ou non à l'administrateur d'utiliser certaines fonctions de gestion des accès en fonction des politiques configurées (FMT_MOF.1).
- La TOE assure que seul l'administrateur de la TOE peut gérer les attributs de sécurité « clés d'accès » et « rôle » (FMT_MSA.1).
- L'administrateur peut aussi définir les données d'initialisation des attributs (tel que le rôle initialisé par défaut à « utilisateur ») (FMT_MSA.3).
- La TOE garantie, de plus, que seuls des valeurs sûres sont acceptées pour les attributs de sécurité en contrôlant la force des mots de passe par exemple (FMT_MSA.2).

O.RECOUVREMENT	La TOE doit permettre d'affecter des clés d'accès de recouvrement et de secours.

Afin de remplir cet objectif :

- La TOE offre des fonctions de recouvrement et de secours (FMT_SMF.1) contrôlés selon des rôles (FMT_SMR.1).
- La TOE doit permettre de restreindre à l'administrateur de la sécurité (FMT_MOF.1) l'activation ou la désactivation des fonctions de recouvrement et/ou de secours.
- La fonction de recouvrement est configurée dans les policies signées par l'administrateur de la sécurité (FMT_MTD.1).

8.2.4.4 Effacement

O.EFF_RESIDUS	La TOE doit assurer le nettoyage des traces de données sensibles (fichiers utilisateurs ou clés d'accès) dans la mémoire (RAM) ou sur le disque dur (fichier SWAP ou temporaire), dès la fin des opérations réalisées par la TOE.

Afin de remplir cet objectif :

- La TOE permet un nettoyage totalement sécurisé des traces dans la mémoire (RAM) ou sur le disque dur (FDP_RIP.2).
- L'effacement sécurisé des clés cryptographiques est effectué par surcharge de motifs composés de zéros (FCS_CKM.4).

O.EFF_FICHIERS	La TOE doit offrir un service d'effacement par surcharge des fichiers supprimés sur les disques locaux, et des fichiers réduit en taille. Ce service doit s'appliquer notamment aux fichiers qui sont dans des zones en clair, mais peut également, par configuration, s'appliquer aux fichiers qui sont dans des zones chiffrées.

Afin de remplir cet objectif :

- Le processus de suppression des fichiers est totalement sécurisé, tout d'abord en alimentant en bruit le fichier à supprimer avant de le supprimer définitivement (FDP_RIP.2).

8.2.4.5 Protections lors de l'exécution

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.

Afin de remplir cet objectif :

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

O.INT_CONTROLE	La TOE doit vérifier l'intégrité du fichier de contrôle à l'ouverture de zone. En cas d'échec lors de la vérification, l'accès à la zone doit être interdit.

Afin de remplir cet objectif :

- Elle doit être capable de générer des clés cryptographiques de scellement pour le calcul des HMAC (FCS_CKM.1)
- Elle doit permettre d'exécuter des opérations de vérification d'intégrité (HMAC) conformément aux algorithmes et tailles de clés cryptographique spécifiés (FCS_COP.1).

O.AUDIT	La TOE doit générer des événements en rapport avec son fonctionnement dans le journal d'audit du système d'exploitation.

Afin de remplir cet objectif :

- La TOE, lors des opérations de gestion et d'utilisation des zones, 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).

8.2.5. Pertinence du niveau d'assurance

Le niveau d'assurance EAL3 augmenté des composants ALC_FLR.3 et AVA_VAN.3 associé à une expertise de l'implémentation de la cryptographie a été choisi pour assurer la conformité au processus de qualification de niveau standard défini par l'ANSSI 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 (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 (l'utilisateur final est alors assuré que le produit a été correctement et sécuritairement conçu et développé et que tous les éventuels défauts de sécurité ont été tracés, analysés et corrigé).

8.3. Argumentaire pour les spécifications globales de la TOE

Le tableau ci-dessous justifie la nécessité des fonctions de sécurité de la TOE par rapport aux composants fonctionnels CC sélectionnés :

Exigences fonctionnelles de sécurité pour la TOE		F.CONFIGURATION_TOE	F.GESTION_OP_ZONE	F.OPERATIONS_CRYPTO	F.GESTION_CLES_ACCES	F.ENTREE_SECURISEE	F.CONTROLE_ACCES_ZONE	F.AUDIT
FAU_GEN.1	Génération de données d'audit	X	X		X		X	X
FAU_GEN.2	Lien entre l'identité de l'utilisateur	X	X		X		X	X
FCS_CKM.1	Génération de clés cryptographiques		X	X	X			
FCS_CKM.3	Accès aux clés cryptographiques				X	X		
FCS_CKM.4	Destruction de clés cryptographiques		X	X	X			
FCS_COP.1	Opération cryptographique	X	X	X	X	X	X	
FDP_ACC.1	Contrôle d'accès partiel				X		X	
FDP_ACF.1	Contrôle d'accès basé sur les attributs de sécurité				X		X	
FDP_ITC.1	Importation depuis une zone hors du contrôle de la TSF					X		
FDP_RIP.2	Protection totale des informations résiduelles		X	X				
FIA_AFL.1	Gestion d'une défaillance de l'authentification	X					X	
FIA_UAU.2	Authentification d'un utilisateur préalablement à toute action	X				X	X	
FIA_UID.2	Identification d'un utilisateur préalablement à toute action	X				X	X	
FMT_MOF.1	Administration des fonctions de la TSF	X						
FMT_MSA.1	Gestion des attributs de sécurité				X			
FMT_MSA.2	Attributs de sécurité sûrs	X						
FMT_MSA.3	Initialisation statique d'attribut				X			
FMT_MTD.1	Gestion des données de la TSF	X						
FMT_SMF.1	Spécification des fonctions d'administration	X	X		X			
FMT_SMR.1	Rôles de sécurité				X			
FTA_SSL.3	Clôture de la session, initiée par la TSF	X	X					

Tableau 11 : Couverture des exigences fonctionnelles par les spécifications globales de la TOE

FAU_GEN.1 Génération de données d'audit

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

- L'application de nouvelles politiques ainsi que la réussite ou l'échec de la vérification de ces politiques (F.CONFIGURATION_TOE),
- Les succès et échecs des opérations cryptographiques relatives aux zones: chiffrement, déchiffrement, transchiffrement reprise de chiffrement ou déchiffrement d'une zone (F.GESTION_OP_ZONE),L
- Les succès et échecs des opérations de gestion des clés d'accès: création, suppression, ouverture ou fermeture (F.GESTION_CLES_ACCES),
- Les opérations de contrôle d'accès : ouverture (succès ou échec de l'authentification après l'atteinte de la limite de trois tentatives consécutives de connexion infructueuses), fermeture de zone (F.CONTROLE_ACCES_ZONE).

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

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

La TOE permet de générer des données d'audit, à partir des événements suivants, en indiquant l'utilisateur associé à l'événement :

- L'application de nouvelles politiques ainsi que la réussite ou l'échec de la vérification de ces politiques (F.CONFIGURATION_TOE),
- Les succès et échecs des opérations cryptographiques relatives aux zones : chiffrement, déchiffrement, transchiffrement reprise de chiffrement ou déchiffrement d'une zone (F.GESTION_OP_ZONE),
- Les succès et échecs des opérations de gestion des clés d'accès: création, suppression, ouverture ou fermeture (F.GESTION_CLES_ACCES),
- Les opérations de contrôle d'accès : ouverture (succès ou échec de l'authentification après l'atteinte de la limite de trois tentatives consécutives de connexion infructueuses), fermeture de zone (F.CONTROLE_ACCES_ZONE).

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

FCS_CKM.1 Génération de clés cryptographiques

A chaque zone chiffrée est associée une clé de zone (exception faite du profil utilisateur qui comporte une seule clé pour toutes les zones du profil). Cette clé est tirée lors de

la création de la zone. Elle répond aux critères de choix d'algorithme et de longueurs de clés configurées dans les policies. Par défaut, c'est une clé AES de 256 bits.

Le format de certaines clés d'accès utilisateur (liste d'accès personnelle) peut également faire l'objet d'un chiffrement intermédiaire par un bi clé RSA générée par la TOE.

La fonction de sécurité F.GESTION_CLES_ACCES implémente la génération des clés RSA et F.GESTION_OP_ZONE (en utilisant F.OPERATIONS_CRYPTO) la génération des clés AES.

FCS_CKM.3 Accès aux clés cryptographiques

L'accès aux clés cryptographiques gérées par la TOE est implémenté par la fonction de sécurité F.ENTREE_SECURISEE.

Cette fonction est utilisée pour les opérations de contrôle d'accès et de gestion.

FCS_CKM.4 Destruction de clés cryptographiques

Les clés de chiffrement et les clés d'accès (ainsi que les secrets associés) sont détruites lors de la fermeture des zones, lors de certains événements système (veille, verrouillage ou fermeture de session etc.) ou lorsqu'elles n'ont plus à être utilisées.

La fonction de sécurité F.OPERATIONS_CRYPTO implémente cette exigence fonctionnelle au service de F.GESTION_CLES_ACCES et F.GESTION_OP_ZONE.

FCS_COP.1 Opération cryptographique

La TOE effectue les opérations cryptographiques suivantes :

- Récupère une clé d'accès de niveau administrateur avant de pouvoir créer une clé de zone et une clé de scellement du fichier de contrôle et chiffrer la zone,
- Récupère une clé d'accès de niveau administrateur pour déchiffrer la clé de la zone avant de pouvoir créer une nouvelle clé d'accès en chiffrant la clé de zone par ce nouvel accès,
- Récupère une clé d'accès de niveau administrateur avant de pouvoir déchiffrer la clé de zone, afin de pouvoir déchiffrer la ou les zones
- Récupère une clé d'accès de niveau administrateur avant de pouvoir transchiffrer (renouveler) la clé de zone, afin de pouvoir d'abord déchiffrer la zone, générer une nouvelle clé de zone et rechiffrer avec cette dernière.

- Récupère une clé d'accès avant de pouvoir utiliser la clé de zone et déchiffrer les fichiers répondant à l'exception,
- Récupère la clé de zone afin de pouvoir terminer les chiffrements inachevés,
- Récupère un mot de passe afin d'en dériver une clé d'accès qui va chiffrer ou déchiffrer la clé de zone.
- Transmet la clé de zone chiffrée au porte-clés puis récupère la clé de zone déchiffrée par le porte-clés afin de pouvoir déchiffrer la zone,
- Vérifie la signature des politiques avec le certificat de l'administrateur de sécurité

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

Les fonctions F.GESTION_CLES_ACCES (création de la clé d'accès) et F.CONTROLE_ACCES_ZONE (vérification de la clé d'accès) utilisent les fonctions de dérivation des clés (incluant un mécanisme de hachage) à partir des mots de passe.

La fonction F.GESTION_OP_ZONE effectue les opérations de chiffrement et déchiffrement.

La fonction F.ENTREE_SECURISEE utilise des fonctions de wrapping (incluant un mécanisme de hachage lorsqu'il s'agit de wrapping par une clé RSA) pour assurer le transfert sécurisé des clés entre la TOE et les porte-clés physique.

La fonction F.CONFIGURATION_TOE intervient pour la configuration cryptographique (longueur des clés, sel et nombre de tours pour la dérivation par exemple).

FDP_ACC.1 Contrôle d'accès partiel

Afin d'utiliser une zone gérée par la TOE, l'utilisateur doit impérativement présenter une clé d'accès valide, associée à la zone concernée. Cette exigence de sécurité est implémentée dans la TOE par les fonctions de sécurité

- F.GESTION_CLES_ACCES pour la configuration des accès aux zones par l'administrateur
- F.CONTROLE_ACCES_ZONE pour le contrôle d'accès aux zones

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

Afin d'utiliser une zone gérée par la TOE, l'utilisateur doit présenter une clé d'accès valide, associée à la zone concernée. Pour pouvoir mettre en place ce fonctionnement :

- Des droits sont associés aux utilisateurs (F.GESTION_CLES_ACCES),

- Et l'accès aux zones est donc contrôlé (F.CONTROLE_ACCES_ZONE).

FDP_ITC.1 Importation depuis une zone hors du contrôle de la TSF

Des données nécessaires au bon fonctionnement de la TOE sont importées depuis l'extérieur de la TSF comme les clés d'accès ou les mots de passe saisis par l'utilisateur. Ce ne sont que des données, aucun attribut de sécurité n'est importé.

La fonction de sécurité F.ENTREE_SECURISEE implémente la communication de données fournies en entrée vers la TOE, et couvre donc cette exigence.

FDP_RIP.2 Protection totale des informations résiduelles

Le processus d'effacement d'objets sécurisés d'une zone est totalement sécurisé. Outre l'effacement des clés, ZoneCentral offre un service automatique et transparent d'effacement sécurisé par surcharge : tout fichier (chiffré ou non) supprimé sur un disque local est automatiquement effacé (réécriture de son contenu avec du 'bruit') avant d'être effectivement supprimé. Cela concerne également les fichiers temporaires créés par les applications. Par ailleurs, la TOE assure le chiffrement du fichier swap susceptible de contenir également des informations sensibles.

Cette exigence fonctionnelle est mise en œuvre par la fonction de sécurité F.GESTION_OP_ZONE (qui assure le nettoyage des traces de données sensibles et en particulier qui gère également l'effacement sécurisé des clés d'accès et des clés de zone (en utilisant F.OPERATIONS_CRYPTO).

FIA_AFL.1 Gestion d'une défaillance de l'authentification

La TOE permet de spécifier le nombre maximum d'essai de mots de passe ou de code confidentiel autorisés lors de l'ouverture d'une zone (paramétrable, et par défaut le nombre est fixé à trois). Passé ce nombre, la demande d'ouverture est rejetée. L'utilisateur pourra réessayer, passé un délai prédéfini.

Après une tentative d'ouverture de zone, si cette ouverture n'a pas été effectuée parce que l'utilisateur a annulé la demande ou parce qu'il n'y a pas eu de réponse dans les délais impartis, toute nouvelle ouverture de la même zone est automatiquement rejetée si elle intervient dans un délai court après ce premier refus.

Ces délais permettent de renforcer la sécurité lorsque quelqu'un tente de multiples essais de mots de passe ou de codes : il sera ralenti par ce délai entre ses différents essais.

La fonction de sécurité F.CONTROLE_ACCES_ZONE qui assure le contrôle d'accès couvre ces fonctionnalités et la configuration de ces options est assurée par la fonction de sécurité F.CONFIGURATION_TOE.

FIA_UAU.2 Authentification d'un utilisateur préalablement à toute action

Aucune action n'est possible sur la TOE sans une phase préalable d'authentification et d'identification de l'utilisateur. Pour chaque authentification, les utilisateurs doivent présenter une clé d'accès valide.

Les zones possèdent différents fichiers qui permettent de gérer l'accès (soit la zone possède l'accès directement, soit elle fait référence à une liste d'accès). Ces fichiers sont gérés par un administrateur, qui configure les zones. L'accès aux zones est donc contrôlé suivant les droits de l'utilisateur faisant la demande d'ouverture.

Cette exigence fonctionnelle est implémentée par :

- F.CONFIGURATION_TOE pour la configuration des accès autorisés aux zones (type d'accès, force des mots de passe, type de certificat …).
- F.CONTROLE_ACCES_ZONE pour contrôler l'accès aux zones,
- F.ENTREE_SECURISEE pour sécuriser la communication des données fournies en entrée vers la TOE.

FIA_UID.2 Identification d'un utilisateur préalablement à toute action

Aucune action n'est possible sur la TOE sans une phase préalable d'authentification et d'identification de l'utilisateur. Pour chaque identification, les utilisateurs doivent présenter une clé d'accès valide.

Les zones possèdent différent fichiers permettant de gérer l'accès (soit la zone possède l'accès directement, soit elle fait référence à une liste d'accès). Ces fichiers sont gérés par un administrateur, qui configure les zones. L'accès aux zones est donc contrôlé suivant les droits de l'utilisateur faisant la demande d'ouverture.

Cette exigence fonctionnelle est implémentée par :

- F.CONFIGURATION_TOE pour la configuration des accès autorisés au zones (type d'accès, force des mots de passe, type de certificat …).
- F.GESTION_CLES_ACCES pour contrôler l'accès aux zones,
- F.ENTREE_SECURISEE pour sécuriser la communication des données fournies en entrée vers la TOE.

FMT_MOF.1 Administration des fonctions de la TSF

Seuls l'administrateur de la TOE peut activer ou désactiver par politiques les fonctions réalisant les opérations cryptographiques sur les zones ainsi que la gestion des accès (dans ce dernier cas ils peuvent notamment activer ou désactiver les fonctions de recouvrement et de secours).

La fonction de sécurité F.CONFIGURATION_TOE implémente cette exigence.

FMT_MSA.1 Gestion des attributs de sécurité

Seuls l'administrateur de la TOE a la possibilité de modifier la valeur par défaut, modifier ou supprimer les attributs de sécurité « clés d'accès et rôle ».

Cet attribut de sécurité est stocké dans le fichier de contrôle de zone, lui-même masqué par ZoneCentral.

Le fonction de sécurité F.GESTION_CLES_ACCES implémente cette exigence.

FMT_MSA.2 Attributs de sécurité sûrs

La fonction de sécurité F.CONFIGURATION_TOE permet de garantir que les attributs de sécurité « clé d'accès et rôle » sont sûrs.

FMT_MSA.3 Initialisation statique d'attribut

La TSF permet à l'administrateur de la TOE de spécifier des valeurs initiales alternatives aux valeurs par défaut lorsqu'un objet ou une information est créé (choix du rôle par exemple).

La fonction de sécurité F.GESTION_CLES_ACCES (changement du rôle par exemple) met en œuvre cette exigence.

FMT_MTD.1 Administration des données de la TSF

Seuls l'administrateur de la TOE 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 Spécification des fonctions d'administration

La TOE permet de réaliser :

- Les fonctions de gestion des zones
- Les fonctions de gestion des accès

Cette exigence fonctionnelle est implémentée par les fonctions de sécurité :

- F.CONFIGURATION_TOE (configuration des fonctions par policies)
- F.GESTION_OP_ZONE (gestion des zones)
- F.GESTION_CLES_ACCES (gestion des clés)

FMT_SMR.1 Rôles de sécurité

La TOE supporte les rôles utilisateur, opérateur de secours et administrateur de la TOE.

Cette exigence est implémentée par F.GESTION_CLES_ACCES qui identifie les droits administrateur, opérateur de secours et utilisateur par l'intermédiaire de leur clé s'accès.

FTA_SSL.3 Clôture de la session, initiée par la TSF

Par défaut, ZoneCentral détecte le lancement de l'économiseur d'écran. Passé un délai de grâce de quelques secondes (durant lequel l'utilisateur peut « réveiller » tout de suite son poste et « annuler » le passage en mode de veille), ZoneCentral ferme automatiquement les zones ouvertes et vide la liste des clés d'accès en cours d'utilisation.

Cette exigence est implémentée par la fonction de sécurité F.GESTION_OP_ZONE qui doit mettre un terme à l'accès aux zones préalablement autorisée aux utilisateurs. La fonction de configuration de la TOE F.CONFIGURATION_TOE permet de paramétrer le comportement de la TOE en fonction d'événements, tels que le déclenchement de l'économiseur d'écran.

8.4. Argumentaire pour les annonces de conformité à un PP

Cette cible de sécurité ne déclare aucune conformité à un Profil de Protection. Aucun argumentaire n’est donc requis.

9. Annexe A : Exigences fonctionnelles de sécurité de la TOE

Cette annexe contient les textes officiels de la partie 2 des Critères Communs en version 3.1 de juillet 2009 avec l'ensemble des opérations réalisées pour la TOE.

Les composants fonctionnels CC sélectionnés pour répondre aux objectifs de sécurité de la TOE sont les suivants :

Composants CC retenus	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FCS_CKM.1	Cryptographic key generation
FCS_CKM.3	Cryptographic key access
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ITC.1	Import of user data without security attributes
FDP_RIP.2	Full residual information protection
FIA_AFL.1	Authentication failure handling
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FTA_SSL.3	TSF-initiated termination

Tableau 12 : Exigences fonctionnelles de sécurité pour la TOE

9.1. Class FAU : Security audit

FAU_GEN	**Security audit data generation**
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) [**- Evénements journalisés au titre de la gestion des zones ;** **- Evénements journalisés au titre de la gestion des accès aux zones ;** **- Evénements journalisés au titre de l'utilisation des zones (authentification, ouverture ou fermeture d'une zone) ;** **- Evénements journalisés au titre de la vérification des policies (réussite, échec, nouvelles politiques appliquées)]**
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, 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, [**pas d'autre information d'audit**] **.**
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.

9.2. Class FCS : Cryptographic support

FCS_CKM	**Cryptographic key management**
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 clés de scellement des**

	fichiers de contrôle, 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#12 à partir des mots de passe**] and specified cryptographic key sizes [**de 128, 192 et 256 bits pour les clés symétriques et de 2048, 3072 et 4096 bits pour les clés asymétriques**] that meet the following: [**exigences cryptographique de l'ANSSI définies dans [CRYPTO_STD] et [CLES_STD]**].
FCS_CKM.3	Cryptographic key access
FCS_CKM.3.1	The TSF shall perform [**l'utilisation de clés**] in accordance with a specified cryptographic key access method [**utilisation du driver clavier et déchiffrement (« déwrapping ») des clés de zone par la clé d'accès**] that meets the following: [**Aucun**].
FCS_CKM.4	Cryptographic key destruction
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**réécriture de motifs composés de zéros**] that meets the following: [**Aucun**].
FCS_COP	**Cryptographic operation**
FCS_COP.1	Cryptographic operation
FCS_COP.1.1	The TSF shall perform [**le hachage, le calcul et la vérification d'intégrité, le chiffrement, le déchiffrement, la vérification de la signature des politiques de sécurité, le « wrapping » et « déwrapping » de clés**] in accordance with a specified cryptographic algorithm [**SHA-256 et SHA-512, RSA, AES**] and cryptographic key sizes [**de 128, 192 et 256 bits pour les clés symétriques et de 2048 à 4096 bits pour les clés asymétriques**] that meet the following: [**exigences cryptographique de l'ANSSI définies dans [CRYPTO_STD] et [CLES_STD]**].

9.3. Class FDP : User data protection

FDP_ACC	**Access control policy**
FDP_ACC.1	Subset access control
FDP_ACC.1.1	The TSF shall enforce the [**SFP.ACCESS_OBJ**] on [**Sujets** : **Utilisateurs, opérateur de secours et administrateur de la TOE** **Objets : Fichiers protégés par la TOE dans une « zone »** **Opérations : Gestion des zones, gestion des accès et utilisation**].
FDP_ACF	**Access control functions**
FDP_ACF.1	Security attribute based access control
FDP_ACF.1.1	The TSF shall enforce the [**SFP.ACCESS_OBJ**] to objects based on the following: [**Sujets: Utilisateurs, opérateur de secours et administrateur de la TOE** **Attributs de sécurité : Clés d'accès utilisateur permettant ou non d'ouvrir la zone et rôle**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**Objet : Zone chiffrée** **Opération: Gestion des zones et utilisation** **Règle : authentification réussie après présentation de la clé d'accès associée à la zone concernée avec accès à la gestion des zones uniquement pour le rôle administrateur**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**Aucune**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the [**Aucune**].
FDP_ITC	**Import from outside TSF control**
FDP_ITC.1	Import of user data without security attributes
FDP_ITC.1.1	The TSF shall enforce the [**SFP.ACCESS_OBJ]** when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**Aucune**].

FDP_RIP	**Residual information protection**
FDP_RIP.2	Full residual information protection
FDP_RIP.2.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**désallocation de la ressource de**] all objects.

9.4. Class FIA : Identification and authentication

FIA_AFL	**Authentication failures**
FIA_AFL.1	Authentication failure handling
FIA_AFL.1.1	The TSF shall detect when [**trois**] unsuccessful authentication attempts occur related to [**l'ouverture d'une zone**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**temporiser l'accès à cette zone**].

FIA_UAU	**User authentication**
FIA_UAU.2	User authentication before any action
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID	**User identification**
FIA_UID.2	User identification before any action
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

9.5. Class FMT : Security management

FMT_MOF	**Management of functions in TSF**
FMT_MOF.1	Management of security functions behaviour
FMT_MOF.1.1	The TSF shall restrict the ability to [**activer ou désactiver**] the functions [**de gestion des zones et de gestion des accès**] to [**l'administrateur de la TOE**].

FMT_MSA	**Management of security attributes**
FMT_MSA.1	Management of security attributes
FMT_MSA.1.1	The TSF shall enforce the [**SFP.ACCESS_OBJ**] to restrict the ability to [**changer la valeur par défaut, modifier ou supprimer**] the security attributes [**clés d'accès (clés RSA et clés dérivées de mots de passe des personnes ayant accès à la zone) et rôles (utilisateur, opérateur de secours et administrateur)**] to [**l'administrateur de la TOE**].
FMT_MSA.2	Secure security attributes
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.
FMT_MSA.3	Static attribute initialisation
FMT_MSA.3.1	The TSF shall enforce the [**SFP.ACCESS_OBJ**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**administrateur de la TOE**] to specify alternative initial values to override the default values when an object or information is created.
FMT_MTD	**Management of TSF data**
FMT_MTD.1	Management of TSF data
FMT_MTD.1.1	The TSF shall restrict the ability to [**changer la valeur par défaut, modifier ou supprimer**] the [**stratégies de sécurité**] to [**l'administrateur de la TOE**].
FMT_SMF	**Specification of Management Functions**
FMT_SMF.1	Specification of Management Functions
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [- **Les fonctions de gestion des zones** - **Les fonctions de gestion des accès (recouvrement et secours compris)]**
FMT_SMR	**Security management roles**
FMT_SMR.1	Security roles
FMT_SMR.1.1	The TSF shall maintain the roles [**administrateur de la TOE, opérateur de secours et utilisateur de la TOE**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

9.6. Class FTA : TOE access

FTA_SSL	Session locking
FTA_SSL.3	TSF-initiated termination
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [**délai de 5 secondes d'inactivité de l'utilisateur, comptées à partir du lancement de l'économiseur d'écran Windows**].