PRIM'X TECHNOLOGIES

ZonePoint

Version 3.0

Cible de Sécurité

Critères Communs niveau EAL3+

Document v1 r9

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 :	ZonePoint version 3.0 build 330 Cible de sécurité CC niveau EAL3+
Version de la ST :	PX128371 v1r9 – Février 2014
Cible d'évaluation (TOE) :	- ZonePoint version 3.0 - ZonePoint version 3.0 Edition Light pour serveur SharePoint 2010 et clients sous Windows Seven (32 et 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

ZonePoint est un produit de sécurité destiné aux organismes utilisant des serveurs SharePoint. Son rôle est de préserver la confidentialité des documents manipulés par les utilisateurs sur ces serveurs. Pour cela, les documents sont stockés chiffrés en permanence sur les portails SharePoint et sont chiffrés / déchiffrés localement sur les postes de travail par l'utilisateur autorisé.

ZonePoint sera évalué pour les serveurs SharePoint 2010 avec des clients PC sous les systèmes d'exploitation Microsoft Windows Seven (32 et 64 bits) utilisant les navigateurs Internet Explorer (version 8 et suivantes), Firefox (version 10 et suivantes) et Chrome (version 10 et suivantes).

1.3. Conformité aux Critères Communs

Cette cible de sécurité respecte les exigences des Critères Communs version 3.1 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.

Tous les composants fonctionnels décrits dans cette cible de sécurité sont issus de la Partie 2 « stricte » des Critères Communs version 3.1 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] Mécanismes de cryptographie : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - Version 1.20 du 26 janvier 2010, ANSSI.

[CLES_STD] Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques - version 1.10 du 24 octobre 2008, DCSSI

[AUTH_STD] 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

ZonePoint est un produit à l'architecture client-serveur (voir la figure 1) :

- Côté serveur, ZonePoint installe une nouvelle bibliothèque de documents permettant la réception des documents chiffrés. Le produit opère sous SharePoint 2010.
- Côté client, le programme comprend notamment un plugin dépendant du navigateur ainsi qu'un filtre WebDAV (extension du protocole HTTP permettant de simplifier la gestion de fichiers avec des serveurs distants) pour l'explorateur Windows et la suite Office réalisant le chiffrement et le déchiffrement à la volée des documents téléchargés depuis ou vers les bibliothèques de documents chiffrés. il fait appel à des composants opérant sous Windows XP, Windows Vista et Windows Seven (32/64 bits).

ZonePoint permet de gérer un stockage chiffré en ligne au sein de **bibliothèques de documents chiffrés SharePoint** de façon la plus transparente possible pour les utilisateurs. ZonePoint réalise le chiffrement et le déchiffrement **local** et « à la volée » des documents téléchargés depuis ou vers les bibliothèques de documents chiffrés : **à aucun moment les données sensibles circulent en clair entre le serveur SharePoint et le poste de travail de l'utilisateur.** En conséquence il n'y a aucun résidu en clair sur les supports de stockage du serveur.

Pour chaque fichier chiffré, il est possible de **définir un certain nombre d'accès** : l'accès de l'utilisateur principal, d'un ou plusieurs collègues partageant des documents avec l'utilisateur, l'accès réservé du responsable de la sécurité, l'accès de secours de l'entreprise (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 ZonePoint de la calculer), soit une clé RSA hébergée dans un porte-clés comme un fichier de clé, une carte à mémoire, un container CSP 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 fichiers.

Avec cette gestion des accès, ZonePoint assure le **droit d'en connaitre** sur les partages chiffrés, c'est-à-dire le cloisonnement cryptographique des documents entre utilisateurs.

ZonePoint se décline en différents packages :

- L'Edition qui contient le produit complet.
- L'Edition Light qui ne permet pas d'effectuer d'opération de gestion sur les zones et les accès. Cette édition ne permet que de télécharger des documents depuis ou vers une zone chiffrée à partir d'un navigateur (elle ne contient pas non plus de filtre WebDAV).
- Enfin, ZonePoint est également incorporé dans les différents produits de la gamme ZoneCentral.

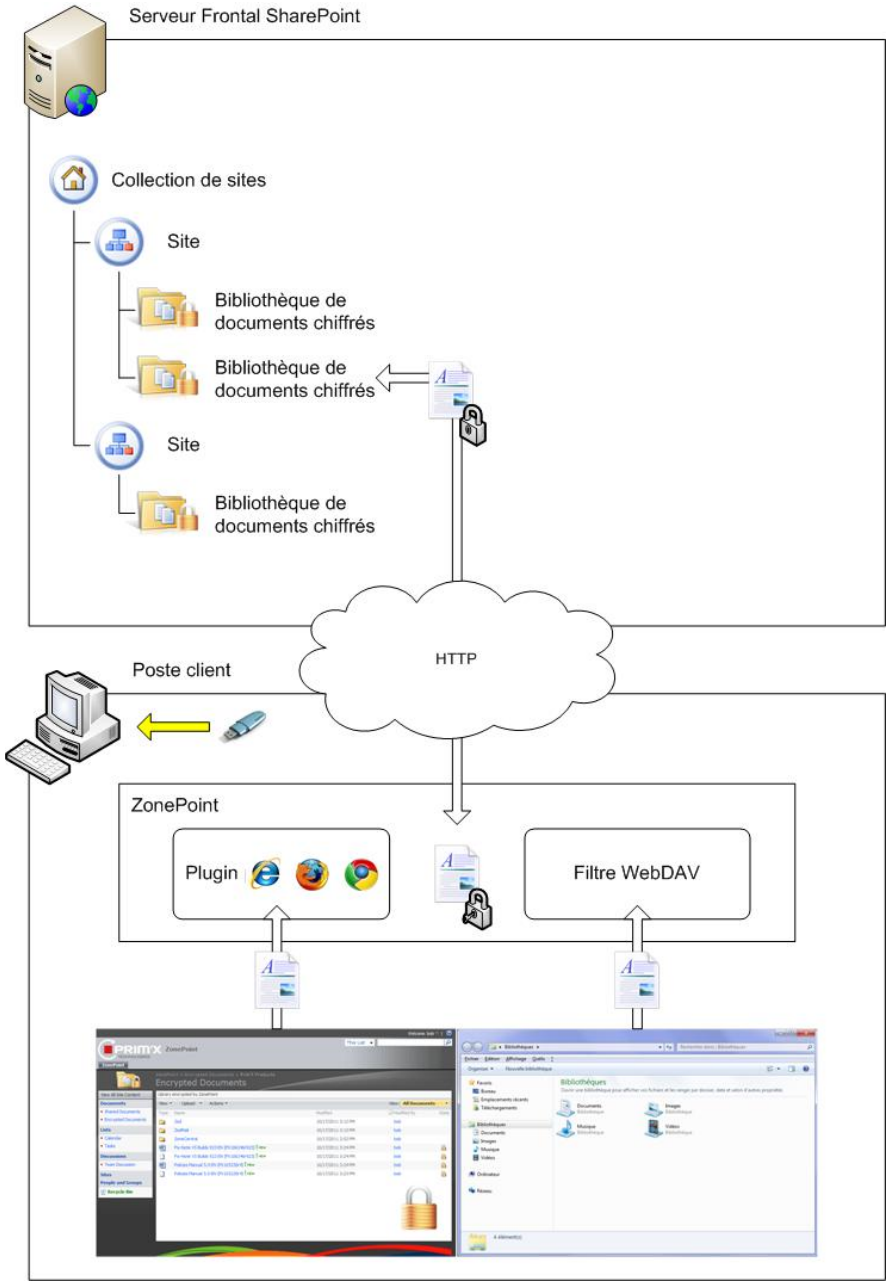


Figure 1 – Schéma de principe de ZonePoint

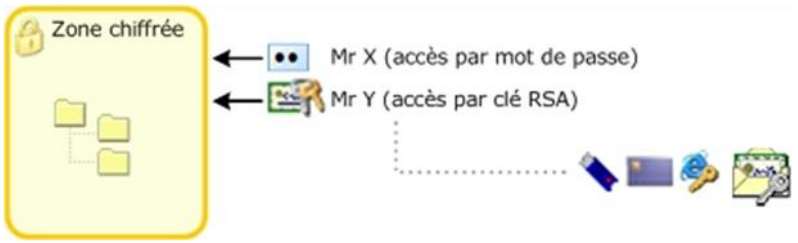
2.1.2. Les zones et les accès

ZonePoint gère des **zones chiffrées** au sein des bibliothèques de documents SharePoint. Une zone est un dossier créé dans une bibliothèque de documents chiffrés, avec tout ce qu'il contient (fichiers et sous-dossiers). Ce dossier peut-être un sous-dossier d'une arborescence ou bien situé à la racine même de la bibliothèque de documents chiffrés.

ZonePoint gère deux types de zones chiffrées :

- Chiffrement libre : Les dossiers à chiffrement libre permettent une gestion indépendante des accès cryptographiques de leurs fichiers : chaque fichier peut posséder des accès qui lui sont propres. L'utilisateur déposant un fichier dans ce dossier peut choisir les personnes autorisées à accéder à ce fichier qui peuvent être choisies différentes des ayant droits aux autres fichiers du dossier.
- Chiffrement imposé : Un dossier avec chiffrement imposé permet une gestion globale des accès cryptographiques aux fichiers de ce dossier (on se rapproche de la notion de zone au sens de ZoneCentral). Concrètement tous les fichiers du dossier possèdent les mêmes accès cryptographiques (qui sont donc gérés au niveau du dossier) et toute modification d'accès s'applique à l'ensemble des fichiers du dossier. Autrement dit, un utilisateur ayant accès à un fichier du dossier a également accès à tous les autres fichiers de ce dossier. La gestion collective des accès permet d'effectuer un transchiffrement de toute la zone c'est-à-dire de renouveler les clés de chiffrement des fichiers (opération recommandée en cas de suppression d'un accès par exemple).

Pour pouvoir utiliser un fichier dans 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 (le porte-clés intégrant la plupart du temps son propre dispositif d'authentification avec un code confidentiel). Le mot de passe peut être fourni par l'administrateur de la TOE ou choisi par l'utilisateur en fonction de la politique de sécurité mise en œuvre.

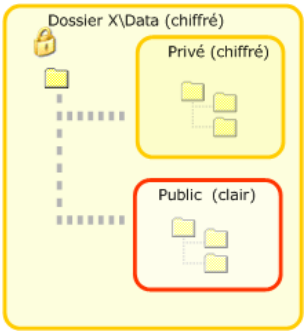


Lorsqu'un fichier est déposé dans une zone chiffrée, le fichier est chiffré avec une clé dédiée à la zone (chiffrement imposé) ou dédié au fichier (chiffrement libre), et cette clé a elle même été chiffrée avec les clés d'accès des utilisateurs à qui l'Administrateur de la TOE donne le droit d'accéder au contenu (confidentiel) de la zone. Bien entendu, les clés d'accès elles-mêmes ne figurent pas dans la zone.

ZonePoint 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

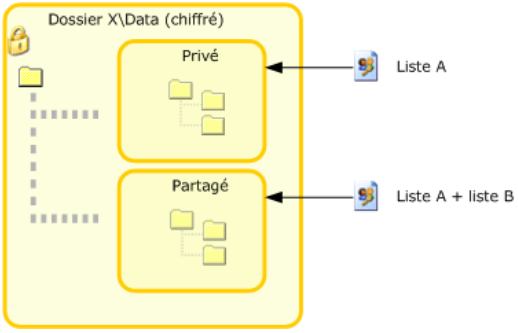
peuvent être utilisés en même temps sur les mêmes zones. Un schéma dit « symétrique » basé sur des mots de passe et des clés dérivées de mots de passe (réf. : PKCS#5) et un schéma dit « asymétrique » utilisant des clés RSA (standard PKCS#1 v1.5) embarquées dans des fichiers de clés (standard PKCS#12) ou des porte-clés (standard PKCS#11 et/ou CSP).

Quand un utilisateur veut ouvrir un fichier chiffré qu'il a téléchargé sur son poste, ZonePoint détecte qu'il a besoin de le déchiffrer pour restituer les informations qu'il contient. S'il ne dispose pas d'une clé d'accès valide pour ce fichier, il la demande en temps réel à l'utilisateur. Quand l'utilisateur accède à un autre fichier chiffré, ZonePoint 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 une fermeture de session ou l'arrêt du système par exemple).



L'administrateur de la TOE peut également définir des **zones en clair**. En effet, 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.

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. Sur l'exemple ci contre, une liste d'utilisateurs A accède aux données des zones « Privé » et « Partagés » alors que la liste des utilisateurs B ne peut accéder qu'à la zone « Partagé ».



2.2. Services d'administration et rôles

2.2.1. Définition des rôles

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

- Un rôle opérant uniquement dans l'environnement de la TOE : L'administrateur de la sécurité de l'environnement Windows des utilisateurs (appelé administrateur Windows dans la suite du document) en charge de définir les règles d'usage et de sécurité (les policies), c'est-à-dire le paramétrage de fonctionnement du produit :

cette opération de « haut-niveau » est effectuée sous le contrôle de l'administrateur 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 TOE et vérifiées par ZonePoint 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 Windows des niveaux supérieurs doivent interdire aux administrateurs des sous-niveaux (domaines, contrôleurs de domaines, postes de travail) la modification des « policies » de la TOE qu'ils souhaitent eux-mêmes contrôler.

- Un rôle **administrateur de la TOE** en charge de créer les zones dans les bibliothèques de documents chiffrées du serveur et de définir leurs propriétés. L'administrateur de la TOE a par ailleurs en charge les opérations de recouvrement et de signature des politiques. Sauf mention contraire dans la suite de ce document, toute référence à l'administrateur se rapporte à ce rôle. Pour chaque zone chiffrée, il faut configurer la liste des personnes pouvant y accéder en introduisant leurs clés d'accès. Par la suite, l'entretien consistera principalement à créer de nouvelles zones si besoin (nouveaux partages), à gérer les 'mouvements de personnel' (nouvel utilisateur pour une zone, retrait d'accès pour une personne en partance), et, éventuellement, à transchiffrer les zones chiffrées (sur compromission, retrait d'accès ou régulièrement).
- Un rôle **utilisateur** qui utilise la TOE selon la configuration imposée par l'administrateur Windows et l'administrateur de la TOE. Hormis les fonctions liées à la protection des fichiers, l'utilisateur retrouve les menus habituels et les principales fonctions de SharePoint à savoir notamment :
    - Le partage de tout type de documents avec la possibilité de télécharger ces documents depuis ou vers la station de travail ;
    - L'organisation des dossiers dans la bibliothèque sous forme d'arborescence avec des sous-dossiers ;
    - La possibilité d'extraire un document pour modification empêchant les autres utilisateurs de l'éditer tant que l'archivage n'a pas été réalisé ;
    - L'utilisation du navigateur Internet ou de l'explorateur Windows pour télécharger les documents.

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

2.2.2. Services d'administration

Les différentes commandes offertes permettent de réaliser les opérations d'administration suivantes (**édition complète seulement, l'édition Light ne permet que de télécharger les fichiers**):

- Lire ou modifier les policies, signer les policies ;
- Créer une zone;
- Déchiffrer une zone chiffrée (chiffrement imposé) ce qui en fera une zone en clair;
- Imposer le chiffrement pour obtenir une zone avec chiffrement imposé ;
- Transchiffrer une zone avec chiffrement imposé (changer les clés de chiffrement de bas niveau) ;
- Ajouter ou supprimer un accès à une zone avec chiffrement imposé ou à un fichier dans une zone avec chiffrement libre ;
- Dissocier un sous-dossier d'une zone chiffrée, pour en faire une zone indépendante, qui peut être gérée séparément (typiquement pour mettre des accès différents entre 2 zones à chiffrement imposé) ;
- Regrouper une zone chiffrée avec la zone chiffrée 'au-dessus' (opération contraire de la précédente);
- Vérifier la cohérence des accès d'une zone.
- Rechercher les zones chiffrées ;
- Consulter les accès d'une zone chiffrée, ajouter des accès ou en retirer ;

Par ailleurs, ZonePoint 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 des fichiers chiffrés par les utilisateurs, 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 de signature privée, ce qui se traduit par une configuration prédéfinie (policy) qui peut être masterisée (personnalisation de l'installation) ou télé-gérée (diffusée, mise à jour) soit par des commandes d'administration fournies par le produit soit par la logistique intégrée des réseaux bureautiques (exemple : contrôleurs de domaines). Ces règles sont généralement établies à « haut niveau » dans l'organisme par le Responsable de la Sécurité. Parmi ces règles, on trouve, par exemple, l'algorithme de chiffrement à utiliser, les opérations autorisées pour les utilisateurs standards, le comportement que doit adopter le logiciel dans certains cas, etc.

Le logiciel (édition complète), masterisé ou non, est ensuite ***installé*** sur un poste de travail, manuellement ou via les logiciels de télé-installation du marché. Le plugin de l'édition Light peut être directement téléchargé et installé sur le navigateur (cette

édition est notamment très utile pour les organismes utilisant des sous-traitants avec lesquels ils peuvent être amenés à échanger des documents).

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). ZonePoint 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 dans les bibliothèques de documents SharePoint en fonction de leur contenu : il s'agit en pratique de définir ***quelles zones doivent être chiffrées***.

Une fois ces opérations initiales effectuées, 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 l'utilisateur, le fonctionnement est alors ***très simple et transparent*** : Lorsqu'un fichier chiffré doit être téléchargé depuis le serveur, ZonePoint 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. Sinon, l'utilisateur se voit refuser l'accès avec le message d'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 une fermeture de session Windows par exemple). Pareillement lors d'une tentative de téléchargement montant d'un nouveau fichier vers une zone chiffrée du serveur, ZonePoint demandera à l'utilisateur une clé d'accès permettant de chiffrer le fichier.

2.3. Périmètre et architecture de la cible d'évaluation

2.3.1. Les composants de ZonePoint

2.3.1.1 ZonePoint (édition complète):

L'installation configure les composants de base de ZonePoint (voir la figure 2, les limites de la TOE sont indiquées en pointillées) :

- **Le gestionnaire de bibliothèque ZonePoint** permettant la réception des documents chiffrés.
- Le **plugin** qui consiste en une extension dynamique dépendant du navigateur (accès au serveur SharePoint par l'intermédiaire d'Internet Explorer, Firefox ou Chrome).
- L'administration **(« commandes administratives »)** des zones et des accès accessible uniquement à l'administrateur
- Le **driver crypto** qui est le centre cryptographique de ZonePoint : 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). 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 clavier**, 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, ou remis aux moteurs externes (CSP/PKCS#11). Cela ne concerne QUE les mots de passe gérés par ZonePoint, c'est-à-dire ceux qui conditionne les accès aux fichiers chiffrés. 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 **ZPS**, qui coordonne les traitements entre le monde «kernel» (drivers) et le monde «user ».
- Le service **ZPP** qui contrôle la signature des politiques.
- Le «daemon» utilisateur **ZPU**, instancié pour chaque session utilisateur Windows gère les interfaces graphiques proposées aux utilisateurs (notamment la fenêtre d'authentification) et leurs clés d'accès.

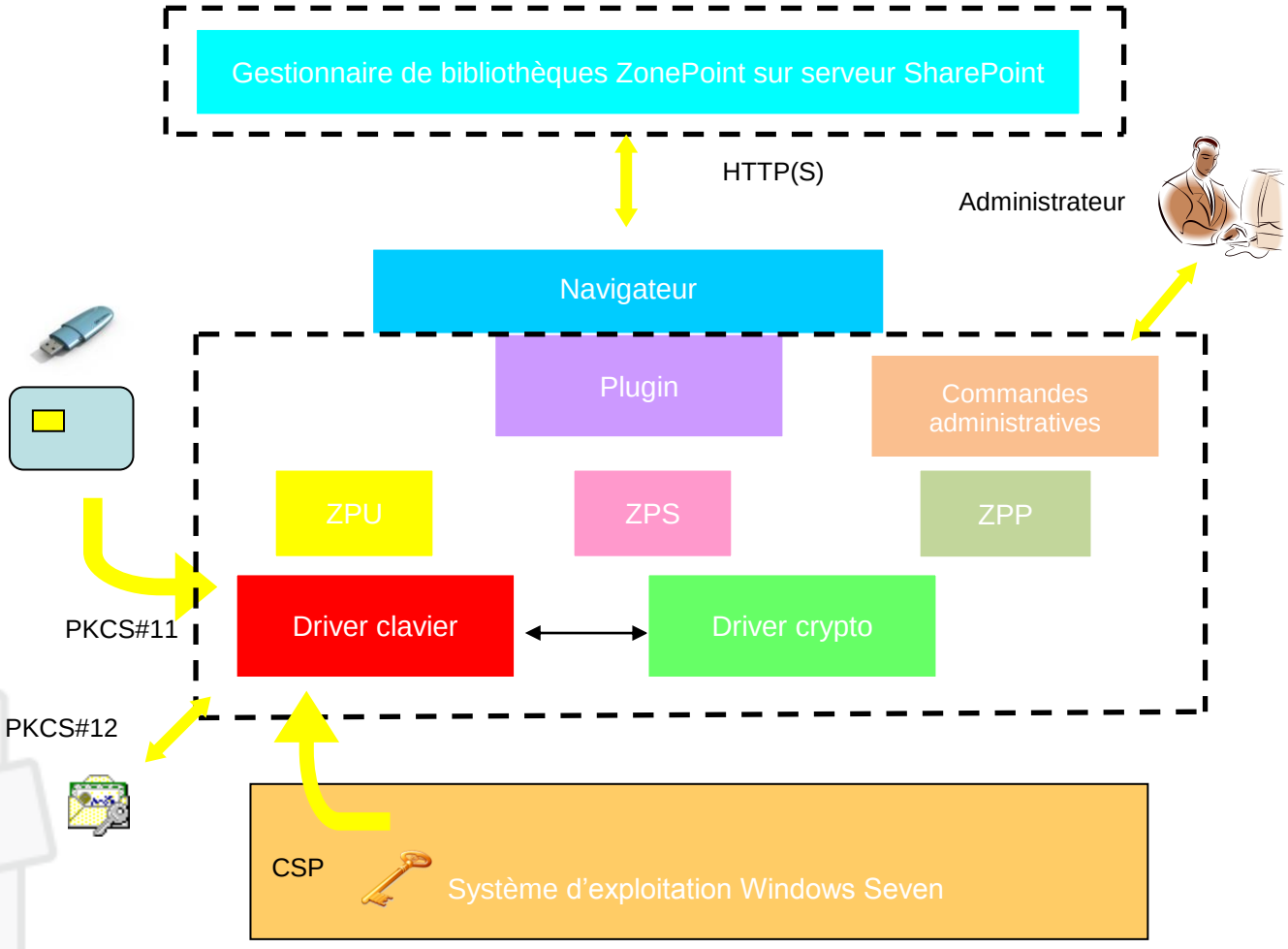


Figure 2 - Architecture de l'édition complète

2.3.1.2 ZonePoint édition Light :

L'installation configure les composants de base de ZonePoint (voir la figure 3, les limites de la TOE sont indiquées en pointillées) :

- **Le plugin**, **ZPU (intégré dans le plugin ici)**, le **centre cryptographique** (il n'y a pas de **driver clavier)** déjà décrits (leur fonctionnement s'effectue ici en mode user). **L'administration** n'est pas disponible dans cette édition qui n'est pas concernée non plus par les **politiques** qui touchent essentiellement la gestion des accès et des zones (effectuée par l'administrateur de l'édition complète).
- «**PXCA**» référence les clés utilisateur saisies via l'entrée d'un mot de passe, l'interface PKCS#11 ou le CSP.

Remarques:

- Le gestionnaire de bibliothèques ZonePoint est installé par l'édition complète.
- Seule l'édition complète permet la configuration et la gestion du produit, les accès autorisés aux bibliothèques sont ensuite communiqués aux utilisateurs de ZonePoint Light afin de travailler sur les fichiers de ces bibliothèques. Cette édition limitée permet aux correspondants de lire et modifier le contenu de documents chiffrés.

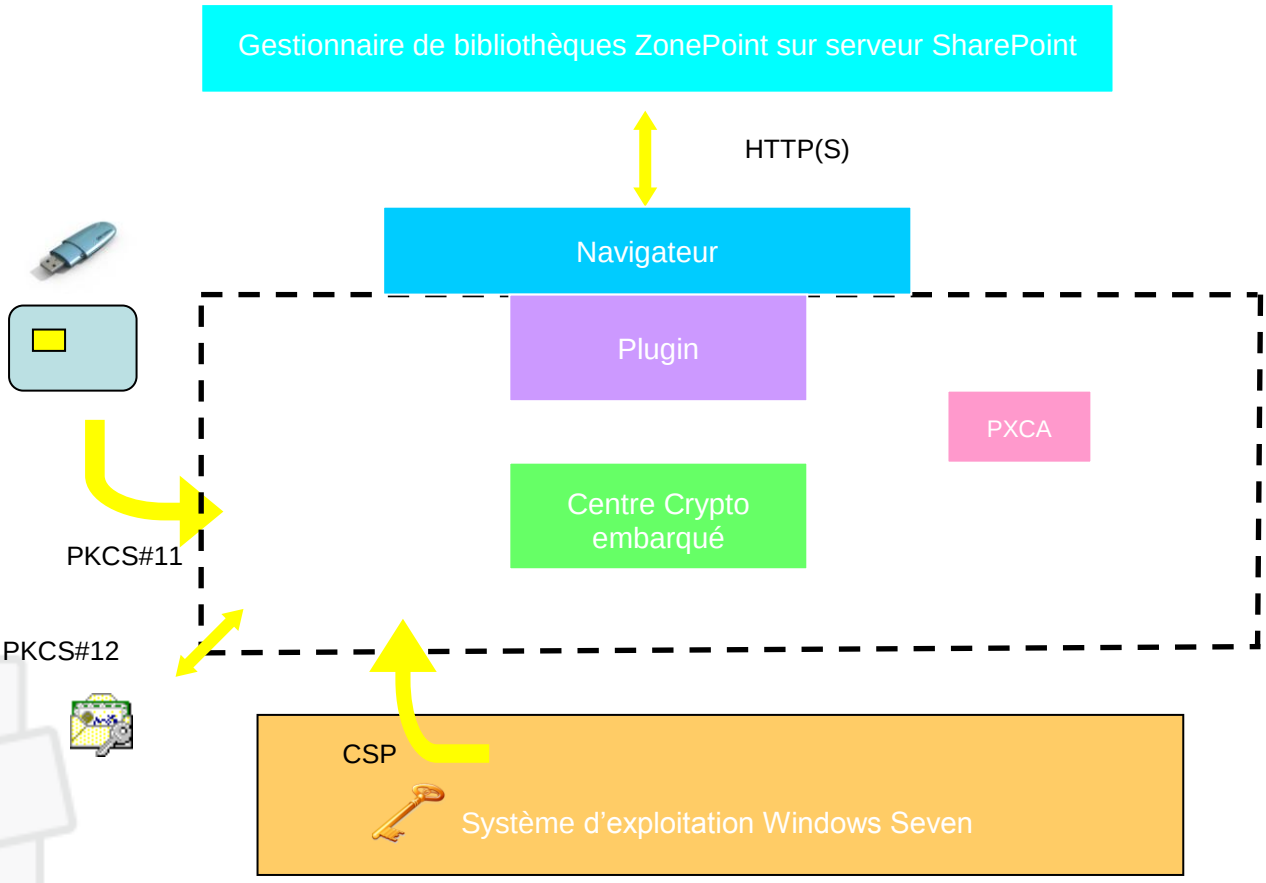


Figure 3 **– Architecture de l'édition Light**

2.3.2. Périmètre de la TOE

2.3.2.1 Périmètre logique

Le périmètre d'évaluation est constitué de l'ensemble des composants du logiciel hormis les fonctionnalités suivantes :

- Le contrôle de version ;
- L'utilisation de zones à chiffrement libre ;
- L'utilisation de WebDAV ;
- L'outil GPOSign.exe permettant à l'administrateur de la TOE de signer les politiques ainsi que la génération de la clé de signature. Par contre la vérification de la signature des politiques par ZonePoint fait bien partie du périmètre de la TOE.

La TOE est constitué de ZonePoint et ZonePoint Light. Le produit intégré dans ZoneCentral ne fait donc pas partie du périmètre de l'évaluation.

2.3.2.2 Périmètre physique

ZonePoint sera évalué, en tant que produit, sur les serveurs SharePoint 2010 et sur une plate-forme PC pour les systèmes d'exploitation de Windows Seven (32 et 64 bits).

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

Les éléments suivants sont hors évaluation :

- La protection des documents utilisateur sur les postes client
- Les portes clés utilisés (comme les porte-clés de type Token USB, les fichiers de clés ou les containers CSP).
- Le logiciel ZonePoint 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. Par contre la génération des clés de chiffrement des zones par ZonePoint entre bien dans le périmètre de l'évaluation.

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

Pour l'évaluation du produit ZonePoint, la plate-forme minimale suivante devra être mise en place par l'évaluateur. Le type physique de porte-clés (carte à puce ou clé USB) étant transparent pour ZonePoint (seul le dialogue PKCS#11 est important), les tests de l'évaluateur pourront s'effectuer avec un seul type de porte-clés. Le produit sera évalué sur les systèmes d'exploitation Windows Seven 32 et 64 bits avec les navigateurs Internet Explorer (8+), Firefox (10+) et Chrome (10+).

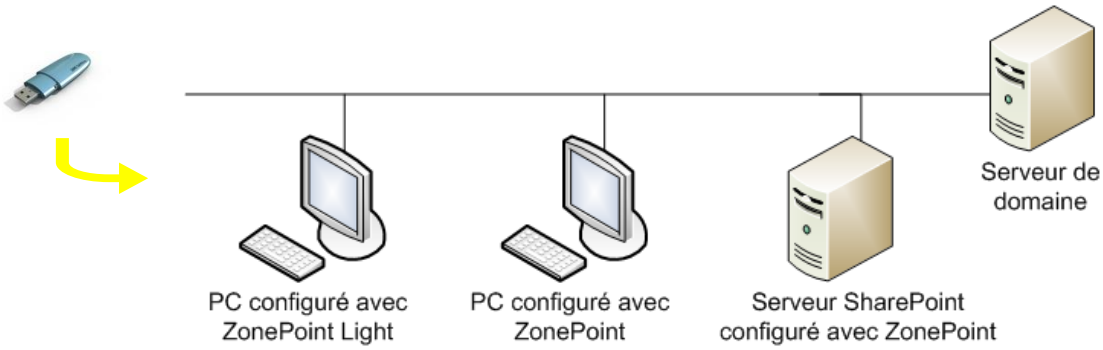


Figure 4 – Plate-forme de tests pour l'évaluation de la TOE

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

Pour chiffrer et déchiffrer les fichiers, ZonePoint 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 : ZonePoint 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 chiffrés par cette clé d'accès. La politique de complexité des mots de passe est configurable par les politiques de sécurité.
- Accès par clé RSA hébergée dans un fichier de clés en utilisant le mécanisme PKCS#12 : ZonePoint 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 chiffrés par cette clé d'accès.
- Accès par clé RSA hébergée dans un token logique accédé au travers d'un composant externe PKCS#11 (ce composant pouvant piloter une carte à mémoire, un token USB ou tout autre dispositif hardware ou software) : ZonePoint gère la saisie du code confidentiel du token logique, le remet au composant externe pour le déverrouiller. ZonePoint fournit également au composant externe la clé de chiffrement des fichiers chiffrés par sa clé publique. Le composant déchiffre la clé de chiffrement avec sa clé privée puis la transmet à ZonePoint qui peut alors effectuer le déchiffrement des fichiers.
- Accès par clé RSA hébergée dans un token logique accédé au travers d'un composant externe CSP (ce composant pouvant piloter une carte à mémoire, un token USB ou tout autre dispositif hardware ou software) : ZonePoint ne gère pas la saisie du code confidentiel du token logique, c'est le composant externe qui le fait spontanément avec ses propres moyens, et il n'accède pas à la clé RSA et n'effectue pas lui-même les chiffrements/déchiffrements avec cette clé, ceux-ci sont effectués par le composant externe ;

En fonction de ces cas, donc, ZonePoint 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 ZonePoint 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 ZonePoint (en général une PKI), de même que le porte-clés éventuel et le code confidentiel de protection. Quand il s'agit de mots de passe, c'est l'administrateur de la TOE 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 Fichiers chiffrés

ZonePoint permet de conserver les fichiers sous forme chiffrée dans des bibliothèques de documents SharePoint. Les biens sensibles sont donc les fichiers et dossiers utilisateurs, de tous types, stockés dans des zones chiffrées du serveur. La TOE n'est pas concernée par la protection des documents sur les postes client.

Les fichiers ainsi chiffrés sont des biens sensibles de l'utilisateur protégés par la TOE (qui doit assurer leur image stockée chiffrée sans copie en clair) tant qu'ils demeurent dans leur zone chiffrée.

3.1.2. Biens sensibles de la TOE

3.1.2.1 Les programmes

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

3.1.2.2 La configuration

Pour assurer son fonctionnement, la TOE met en œuvre des ***policies*** (au sens Windows du terme). La sécurité en intégrité de ces policies est assurée :

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

3.1.2.3 Les fichiers de fonctionnement

- ***Les fichiers de contrôle de zone*** : Chaque dossier d'une zone chiffrée contient un fichier caché appelé "*fichier de contrôle de zone*". Pour des raisons sanitaires, ZonePoint masque ce fichier et le rend invisible.

  Ce fichier contient :

  - le type de zone (chiffrement libre/chiffrement imposé/en clair) ;
  - les éléments de chiffrement de la zone (algorithme, etc.) ;
  - les 'wrappings' d'accès, c'est-à-dire les clés de chiffrement de la zone chiffrées par les clés d'accès des utilisateurs habilités à la zone, tous identifiés par un libellé, un identifiant unique, leur nature et leur rôle.

  C'est grâce à la présence de ce fichier que ZonePoint peut vérifier la cohérence des fichiers déposés dans les zones. En effet, chaque fichier chiffré est préfixé par ses informations de chiffrement (clé de chiffrement/accès) en fonction du type de zone (chiffrement libre ou imposé).

3.1.3. Synthèse des biens sensibles

Le tableau ci-dessous résume la liste des biens sensibles protégés par ZonePoint et indique la nature de la sensibilité associée.

Remarque : de façon générale, l'intégrité n'est pas un objectif de ZonePoint. 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, ZonePoint 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 ZonePoint, en fonction des cas explicités plus haut : mot de passe ou code confidentiel éventuel, clé d'accès elle-même si elle est directement utilisée par ZonePoint	Forte	Forte
Fichiers et dossiers de l'utilisateur stockés dans des zones chiffrées	Forte	*N/A*
Biens sensibles de la TOE		
Fichiers de contrôle des « zones » dont : les clés de chiffrement de zones	*Faible* Forte	Forte
Configuration de ZonePoint (policies)	*Faible*	Forte
Programmes de ZonePoint	*Faible*	Forte

Tableau 1 : Synthèse des biens sensibles

3.2. Hypothèses

Pour ZonePoint, 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.POSTE_UTILISATEUR_NON_OBSER	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.
H.POSTE_UTILISATEUR_SUR	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 son poste. Le poste utilisateur 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.POSTE_ADMIN_NON_OBSER	L'environnement physique de la TOE permet à l'administrateur de la TOE d'entrer son 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 (poste isolé dans une pièce close par exemple).
H.POSTE_ADMIN_SUR	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 administrateur de la TOE sur son poste. Le poste de l'administrateur 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.). Ce poste doit être uniquement utilisé pour les opérations d'administration de la TOE.

H.CONFIANCE_ADMIN	L'administrateur de la TOE est une personne de confiance et est formé à l'utilisation de la TOE. Les administrateurs Windows sont des personnes de confiance en charge de la configuration (avec des valeurs sures) des « policies ».
H.CONSERVATION_CLES	Les utilisateurs sont chargés de la conservation dans un lieu sûr et de la non divulgation des clés d'accès qui leurs ont été transmises par 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.
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.REVOCATION	L'administrateur de la TOE est chargé de renouveler les clés de chiffrement des zones toutes les fois qu'il supprime l'accès d'un utilisateur à ces zones.
H.CRYPTO_EXT	Les clés d'accès sont générées ou stockées à l'extérieur de la TOE et leur gestion est conforme au document [CRYPTO_STD] pour le niveau standard.

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

Il s'agit ici des menaces portant sur les biens sensibles de la TOE elle-même. Celles qui concernent les biens des utilisateurs sont couvertes par les Politiques de Sécurité Organisationnelles (services du produit) décrites plus loin.

L'agent menaçant accède aux données stockées sur le serveur SharePoint ou intercepte ces données lorsqu'elles transitent entre le poste client et le serveur. Il tente ensuite de les attaquer en installant ou pas l'une des éditions du produit ZonePoint sur son poste. Par hypothèse, on considère que d'autres moyens sont utilisés pour protéger les données sensibles de l'utilisateur résidant sur le poste utilisateur (chiffrement du disque par exemple). Les administrateurs et les utilisateurs légitimes ne sont pas considérés comme des attaquants.

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

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, agir sur la configuration interne de la TOE ou s'aider d'un debugger. Le bien impacté est le programme de la TOE (confidentialité et intégrité) ainsi que la configuration (intégrité).

Il ne doit pas pouvoir, avec ces moyens, réussir à «pénétrer» une zone chiffrée dans laquelle il n'aurait pas normalement accès.

M.DIVUL_FIC_INTERNES

Un attaquant récupère des fichiers de contrôle de la TOE pour pénétrer dans une zone chiffrée.

Par exemple, il copie les fichiers chiffrées d'une zone, avec les fichiers de contrôle de la TOE et tente à partir de ces éléments de retrouver des informations protégées telles que les clés de chiffrement. Les biens impactés sont donc les fichiers de contrôle de la TOE (confidentialité).

M.MODIF_FIC_INTERNES

Un attaquant modifie les fichiers de contrôle de la TOE pour tenter de retrouver des informations protégées (par exemple il récupère le fichier de contrôle et le modifie afin de s'ajouter parmi les accès autorisés). Les biens impactés sont donc les fichiers de contrôle de la TOE (intégrité).

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 dans des bibliothèques de documents chiffrés SharePoint, 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. S'ils ne peuvent fournir une clé d'accès valide pour la zone considérée, l'accès doit être rejeté.
OSP.ADMIN_ZONES	La TOE doit offrir un service de gestion des « zones » (Edition complète seulement). Ce service doit permettre l'affectation de clés de recouvrement aux fichiers et le renouvellement des clés de chiffrement des zones en cas de révocation d'un utilisateur.
OSP.ADMIN_ACCES	La TOE doit offrir un service de gestion des accès aux zones chiffrées (Edition complète seulement).
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 (Edition complète seulement). L'application de toute nouvelle politique est conditionnée par le succès de cette vérification.
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 un fichier chiffrée qu'après présentation d'une clé d'accès valide pour le fichier.

O.ROLES La TOE doit gérer deux 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) et un rôle 'administrateur' (utilisation, recouvrement, plus possibilité d'administrer la zone chiffrée, c'est-à-dire gérer ses accès, modifier ses propriétés).

4.1.2. Cryptographie

O.CHIFFREMENT La TOE doit chiffrer (déchiffrer/transchiffrer) les « zones » configurées par l'emploi de clés cryptographiques. Ces opérations cryptographiques doivent s'effectuer sur le poste de travail de l'utilisateur ou de l'administrateur. La TOE doit utiliser des clés différentes pour protéger les différentes «zones» configurées, même si les utilisateurs sont les mêmes pour ces « zones ».La TOE doit générer ces clés de chiffrement conformément aux exigences pour le niveau de robustesse standard des référentiels cryptographiques [CRYPTO_STD] et [CLES_STD] de l'ANSSI.

O.EFFACEMENT_CLES La TOE doit assurer le nettoyage des traces de données sensibles (clés de chiffrement des fichiers, éléments permettant de retrouver les clés d'accès) dans la mémoire (RAM) dès la fin des opérations réalisées par la TOE.

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.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» (Edition complète seulement).

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

4.1.4. Protections lors de l'exécution

O.INT_POLICIES La TOE doit vérifier la signature de toutes nouvelles politiques de sécurité à appliquer (Edition complète seulement). En cas d'échec lors de la vérification, les politiques appliquées restent inchangées.

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. Pendant l'utilisation

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

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

Note d'application :
Le poste de l'utilisateur 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 le poste ne doivent pas perturber le bon fonctionnement de la TOE.
OE.POSTE_ADMIN_NON_OBSER	L'administrateur ne doit accéder à ses données sensibles que lorsqu'il se trouve seul dans un environnement de confiance.
OE.POSTE_ADMIN_SUR	Lorsque l'administrateur est authentifié, l'environnement opérationnel doit assurer la confidentialité des données sensibles, des clés et des données d'authentification. Note d'application : Le poste de l'administrateur est utilisé uniquement pour assurer l'administration de la TOE. Il 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 (minimales) installées sur son poste ne doivent pas perturber le bon fonctionnement de la TOE.

4.2.2. Formation des utilisateurs et de l'administrateur

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 doit recevoir une formation adaptée à cette fonction.
OE.CRYPTO_EXT	L'administrateur de la TOE doit être sensibilisé sur la qualité des clés d'accès qu'il apporte à la TOE afin que ces clés soient conformes à l'état de l'art dans leur implémentation. Il doit également être sensibilisé à la qualité du support de ces clés lorsqu'elles sont hébergées par un porte-clés externe.

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 dans un lieu sûr et empêcher leur divulgation.

4.2.3. Administration

OE.CONFIANCE_ADMIN	L'administrateur de la TOE doit être une personne de confiance. Les administrateurs Windows sont des personnes de confiance en charge de la configuration (avec des valeurs sures) des « policies ».
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 en particulier aux certificats racines dits «authenticode» à partir desquels la vérification d'intégrité de la TOE peut être effectuée.
OE.REVOCATION	En cas de retrait de l'accès d'un utilisateur dans une zone, l'administrateur doit assurer le renouvellement des clés de chiffrement de cette zone en effectuant un transchiffrement de celle-ci. Le transchiffrement doit être opéré sur toutes les zones si la suppression de l'accès concerne toute la bibliothèque de documents chiffrés (cas du départ d'un collaborateur par exemple).

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_ITT.1	Protection de base des transferts internes
FDP_RIP.1	Protection d'une partie 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_REV.1	Revocation
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

Tableau 2 : Exigences fonctionnelles de sécurité pour la TOE

5.1.1.1 Introduction

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

- Administrateur et utilisateur 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.

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

- Zones chiffrées manipulées 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, modification des accès)
- 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 du contrôle d'accès (succès et échecs) ;* *- Evénements journalisés au titre de la gestion des zones (chiffrement, déchiffrement, transchiffrement) ;* *- Evénements journalisés au titre de la gestion des accès aux zones (modification ou ajout d'accès sur 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 (si applicable), 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, *aucune 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'utilisateurs 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, génération d'exposants Diffie-Hellman et diversification de clés* et à des tailles de clés cryptographiques *de 128, 192 et 256 bits pour les clés symétriques et de 1024 à 2048 bits pour les clés asymétriques* qui satisfont aux standards exigences cryptographique de l'*ANSSI définies dans [CRYPTO_STD] et [CLES_STD].* *Raffinement non éditorial :* *L'Edition Light n'effectue que la diversification de clés pour obtenir la clé d'accès de l'utilisateur à partir de son mot de passe.*
FCS_CKM.3	Accès aux clés cryptographiques
FCS_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 par la clé d'accès.* *Raffinement non éditorial :* *Ce composant s'applique en totalité à l'Edition complète qui réalise notamment toutes les fonctions d'administration sensibles. Par contre, l'Edition Light ne contient pas de driver clavier et utilise exclusivement la fonction de déchiffrement des clés.*
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 chiffrement, le déchiffrement, la vérification de la signature des politiques de sécurité, la génération de clés, le wrapping de clés et la dérivation de clés conformément à un algorithme cryptographique spécifié *SHA-1 (dérivation de clé), SHA-256, RSA, AES* et avec des tailles de clés cryptographiques *de 128, 192 et 256 bits pour les clés symétriques et de 1024 à 2048 bits pour les clés asymétriques* qui satisfont à ce qui suit: exigences cryptographique de l'*ANSSI*

	définies dans [CRYPTO_STD] et [CLES_STD]. *Raffinement non éditorial :* *L'Edition Light ne permet que le chiffrement et déchiffrement des fichiers ainsi que la dérivation de clé et la fonction de hachage associée.*

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: Administrateur et utilisateurs de la TOE* *Objets: Fichiers protégés par la TOE dans une « zone »* *Opérations : Gestion des zones 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: Administrateur et utilisateurs de la TOE* *Attributs de sécurité : Clés d'accès permettant ou non d'ouvrir la zone et rôle*. *Raffinement non éditorial :* *Il n'y a pas de rôle administrateur dans l'Edition Light, cette édition ne gère que le rôle utilisateur.*
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 des règles complémentaires suivantes : *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 *les politiques de sécurité des fonctions (SFP) SFP.ACCESS_OBJ et SFP.ACCESS_ROLES* 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_ITT	**Transferts internes à la TOE**
FDP_ITT.1	Protection de base des transferts internes
FDP_ITT.1.1	La TSF doit appliquer *les politiques de sécurité des fonctions (SFP) SFP.ACCESS_OBJ* pour prévenir la *divulgation* des données utilisateurs quand elles sont transmises entre des parties physiquement séparées de la TOE. *Note d'application :* *Concerne le transfert des données entre la partie serveur de la TOE et la partie sur le poste client.*
FDP_RIP	**Protection des informations résiduelles**
FDP_RIP.1	Protection d'une partie des informations résiduelles
FDP_RIP.1.1	La TSF doit garantir que toute information contenue précédemment dans une ressource est rendue inaccessible lors de *la désallocation de la ressource* des objets *clés de chiffrement des fichiers et clés d'accès.*

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 de *déterminer le comportement ou modifier le comportement* des fonctions *de contrôle d'accès (rôles), de gestion des accès et de gestion des zones* à *l'administrateur de la TOE*. *Raffinement non éditorial :* *Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion).*
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_ROLES* 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 et rôles.* *Raffinement non éditorial :* *Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion d'accès).*
FMT_MSA.2	Attributs de sécurité sûrs
FMT_MSA.2.1	La TSF doit garantir que seules des valeurs sûres sont acceptées pour *les clés d'accès et les rôles*.
FMT_MSA.3	Initialisation statique d'attribut
FMT_MSA.3.1	La TSF doit mettre en œuvre *la politique SFP.ACCESS_ROLES* 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. *Raffinement non éditorial :* *Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion).*
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*. *Raffinement non éditorial :* *Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion).*

FMT_REV	**Révocation**
FMT_REV.1	Révocation
FMT_REV.1.1	La TSF doit restreindre à *l'administrateur de la TOE*, la possibilité de révoquer *les clés d'accès* associés aux *utilisateurs*.
FMT_REV.1.2	La TSF doit mettre en œuvre la règle suivante **:** *accès de l'utilisateur supprimé par l'administrateur et transchiffrement des zones contenant cet accès*. *Raffinement non éditorial :* *Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion).*

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 contrôle d'accès aux opérations d'administration de la sécurité (rôle)* - *Les fonctions de gestion des clés (y compris les clés de recouvrement)* - *Les fonctions de gestion des zones* *Raffinement non éditorial :* *Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion).*

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 et utilisateur de la TOE*.
FMT_SMR.1.2	La TSF doit être capable d'associer les utilisateurs aux rôles

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 3 : 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). Les données de configuration concernent les «« policies »» de Windows qui sont signées par l'administrateur de sécurité et exploitées par la TOE après vérification de leur signature. Ces données définissent notamment les types d'accès supportés, les algorithmes utilisés (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.OPERATIONS_CRYPTO **Implémentation des opérations cryptographiques**

Cette fonction de sécurité couvre l'ensemble des opérations cryptographiques mises au service des autres fonctions de sécurité.

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

Cette fonction de sécurité constitue l'interface obligatoire entre l'utilisateur 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 plusieurs échecs consécutifs (nombre d'essais paramétrable). Les données sont déchiffrées sur le poste de travail et l'accès autorisé ne s'applique donc qu'à l'utilisateur localement sur son poste.

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 (version complète uniquement) quand il s'agit d'entrer un mot de passe ou un code de fichier de clés.

F.GESTION_CLES **Gestion des clés d'accès**

Cette fonction de sécurité gère les attributs de sécurité que sont les clés d'accès des utilisateurs et les rôles (utilisateur ou administrateur) 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 chiffrement / déchiffrement de la 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. Cette fonction gère également l'accès de recouvrement qui est un accès particulier.

Enfin la fonction F.GESTION_CLES réalise également les opérations d'ajout, de modification, de suppression (révocation) des clés d'accès ainsi que les opérations d'accès à ces clés (par l'intermédiaire des tokens pkcs#11 notamment). Elle assure le nettoyage de ces clés en mémoire après un verrouillage de la session, mise en veille ou une fermeture du poste.

F.GESTION_ZONES **Gestion des zones**

Cette fonction de sécurité constitue le point d'entrée des opérations sur les zones (tirage de la clé de zone, chiffrement, déchiffrement, transchiffrement, affichage des informations de zone). Elle nécessite de s'authentifier avec une clé d'accès associée au rôle administrateur. Cette fonction prend en charge le nettoyage des clés de chiffrement des zones dès que les fichiers ont été chiffrés ou déchiffrés sur le poste.

F.AUDIT **Audit**

Cette fonction de sécurité assure l'enregistrement des événements liés aux opérations réalisées par la TOE. Ces enregistrements peuvent être envoyés vers un serveur distant pour être traités.

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 constituent 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.POSTE_UTILISATEUR_NON_OBSER	OE. POSTE_UTILISATEUR_SUR	OE.POSTE_ADMIN_NON_OBSER	OE. POSTE_ADMIN_SUR	OE.FORMATION	OE.CRYPTO_EXT	OE.CONSERVION_CLES	OE.CONFIANCE_ADMIN	OE.CERTIFICATS	OE.REVOCATION
Hypothèses	**H.POSTE_UTILISATEUR_NON_OBSER**	X									
	H.POSTE_UTILISATEUR _SUR		X								
	H.POSTE_ADMIN_NON_OBSER			X							
	H.POSTE_ADMIN_SUR				X						
	H.CONFIANCE_ADMIN					X			X		
	H.CONSERVATION_CLES					X		X			
	H.CERTIFICATS									X	
	H.REVOCATION										X
	H.CRYPTO_EXT						X				

Tableau 4 : Couverture des hypothèses par les objectifs de sécurité

H.POSTE_UTILISATEUR_NON_OBSER	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.

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

H.POSTE_UTILISATEUR_SUR	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 son poste. Le poste utilisateur 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.POSTE_UTILISATEUR_SUR couvre directement cette hypothèse en mettant à disposition de l'utilisateur un environnement opérationnel adéquat.

H.POSTE_ADMIN_NON_OBSER	L'environnement physique de la TOE permet à l'administrateur de la TOE d'entrer son 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 (poste isolé dans une pièce close par exemple).

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

H.POSTE_ADMIN_SUR	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 administrateur de la TOE sur son poste. Le poste de l'administrateur 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.). Ce poste doit être uniquement utilisé pour les opérations d'administration de la TOE.

L'objectif OE.POSTE_ADMIN_SUR couvre directement cette hypothèse en mettant à disposition de l'administrateur un environnement opérationnel adéquat.

H.CONFIANCE_ADMIN	L'administrateur de la TOE est une personne de confiance et est formé à l'utilisation de la TOE. Les administrateurs Windows sont des personnes de confiance en charge de la configuration (avec des valeurs sures) des « policies ».

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	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.

Les objectifs OE.CONSERVATION_CLES et OE.FORMATION couvrent cette hypothèse en responsabilisant et en sensibilisant les utilisateurs et l'administrateur.

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.REVOCATION	L'administrateur de la TOE est chargé de renouveler les clés de chiffrement des zones toutes les fois qu'il supprime l'accès d'un utilisateur à ces zones.

L'objectif OE.REVOCATION couvre directement cette hypothèse.

H.CRYPTO_EXT	Les clés d'accès sont générées ou stockées à l'extérieur de la TOE et leur gestion est conforme au document [CRYPTO_STD] pour le niveau standard.

L'objectif OE.CRYPTO_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.EFFACEMENT_CLES	O.ALGO_STD	O.ADM_ZONES	O.ADM_ACCES	O.INT_POLICIES	O.AUDIT
Menaces	M.DETOURN_COMPOSANT	X							X	
	M.DIVULG_FIC_INTERNES	X		X		X				
	M.MODIF_FIC_INTERNES	X		X		X				

Tableau 5 : 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, agir sur la configuration interne de la TOE ou s'aider d'un debugger. Le bien impacté est le programme de la TOE (confidentialité et intégrité) ainsi que la configuration (intégrité).

Il ne doit pas pouvoir, avec ces moyens, réussir à «pénétrer» une zone chiffrée dans laquelle il n'aurait pas normalement accès.

➔ Pour prévenir cette menace, la TOE doit :

Rien

➔ Pour se protéger la TOE doit :

- Garantir le fait qu'il n'est pas possible de retrouver les clés de chiffrement sans accéder au fichier de contrôle de la zone après une authentification réussie : 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.AUTH).

- 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 le responsable de sécurité (O.INT_POLICIES)

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

Rien

M.DIVUL_FIC_INTERNES

Un attaquant récupère des fichiers de contrôle de la TOE pour pénétrer dans une zone chiffrée.

Par exemple, il copie les fichiers chiffrées d'une zone, avec les fichiers de contrôle de la TOE et tente à partir de ces éléments de retrouver des informations protégées telles que les clés de chiffrement. Les biens impactés sont donc les fichiers de contrôle de la TOE (confidentialité).

➔ Pour prévenir cette menace, la TOE doit :

- Garantir le fait que tout accès à une zone, pour récupérer des informations, nécessite une authentification réussie (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 posséder une clé d'accès valide (mécanisme de wrapping assuré par O.ALGO_STD).

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

- Garantir le fait que les fichiers de contrôle des différentes zones sont rendus «cryptographiquement différents» par l'utilisation d'aléas ne permettant pas de tirer des enseignements d'un fichier interne (par exemple clé de chiffrement d'une zone) pour en attaquer une autre (O.CHIFFREMENT).

M.MODIF_FIC_INTERNES

Un attaquant modifie les fichiers de contrôle de la TOE pour tenter de retrouver des informations protégées (par exemple il récupère le fichier de contrôle et le modifie afin de s'ajouter parmi les accès autorisés). Les biens impactés sont donc les fichiers de contrôle de la TOE (intégrité).

➔ Pour prévenir cette menace, la TOE doit :

- Garantir le fait que tout accès à une zone, pour récupérer des informations, nécessite une authentification réussie (O.AUTH),

➔ Pour se protéger la TOE doit :

- Garantir le fait qu'il n'est pas possible, cryptographiquement, d'ajouter un accès dans le fichier de contrôle sans accéder aux clés de chiffrement de zones

lesquelles nécessite de fournir une clé d'accès valide (mécanisme de wrapping assuré par O.ALGO_STD).

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

- Garantir le fait que les fichiers de contrôle des différentes zones sont rendus «cryptographiquement différents» par l'utilisation d'aléas ne permettant pas d'utiliser un fichier affecté à une zone pour en attaquer une autre (O.CHIFFREMENT).

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.EFFACEMENT_CLES	O.ALGO_STD	O.ADM_ZONES	O.ADM_ACCES	O.INT_POLICIES	O.AUDIT
Politiques de sécurité de l'organisation	OSP.ZONE	X		X	X					
	OSP.ACCES	X			X					X
	OSP.ADMIN_ZONES	X	X	X	X		X	X		X
	OSP.ADMIN_ACCES	X	X		X			X		X
	OSP.VERIF_POLICIES								X	X
	OSP.CRYPTO					X				

Tableau 6 : 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 dans des bibliothèques de documents chiffrés SharePoint, 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, 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 couvrir cette politique, la TOE :

- Chiffre les fichiers dans les zones en utilisant des clés de chiffrement différentes pour chaque zone (O.CHIFFREMENT) ;
- 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.EFFACEMENT_CLES) ;

OSP.ACCES	La TOE doit permettre aux utilisateurs de fournir une clé d'accès permettant d'accéder aux fichiers sensibles d'une zone protégée. S'ils ne peuvent fournir une clé d'accès valide pour la zone considérée, l'accès doit être rejeté.

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

➔ Pour couvrir cette politique, la TOE :

- Demande une authentification avant tout accès à une zone chiffrée et autorise l'accès aux fichiers de la zone si l'authentification de l'utilisateur est réussie (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.EFFACEMENT_CLES) ;

➔ 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.ADMIN_ZONES	La TOE doit offrir un service de gestion des « zones » (Edition complète seulement). Ce service doit permettre l'affectation de clés de recouvrement aux fichiers et le renouvellement des clés de chiffrement des zones en cas de révocation d'un utilisateur.

Note: l'administration des zones et l'administration des accès ont volontairement été distinguées parce que, en pratique, l'ajout ou la suppression sont des opérations bien plus fréquentes que la création de zones chiffrées, souvent effectuées au début lors du déploiement initial. Cependant, comme il est nécessaire, lorsqu'une zone chiffrée est créée, de définir les accès initiaux à cette zone, cette politique est en partie couverte par l'objectif O.ADM_ACCESS.

➔ Pour couvrir cette politique, la TOE :

- Demande une authentification avant de permettre la gestion des zones (O.AUTH) ;
- Contrôle que seul un utilisateur disposant du rôle 'administrateur' dans une zone chiffrée existante a le droit d'intervenir sur cette zone pour la gérer (O.ROLES)
- Offre une interface à l'administrateur, lui permettant de visualiser et gérer le chiffrement, le déchiffrement et le transchiffrement des « zones » (O.ADM_ZONES) ainsi que l'accès de recouvrement associé (O.ADM_ACCES).
- Chiffre les fichiers dans les zones chiffrées, transchiffre les fichiers sur demande de l'administrateur, 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.EFFACEMENT_CLES).

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

- 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 (Edition complète seulement).

➔ Pour couvrir cette politique, la TOE :

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

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

- Efface les traces mémoires des clés d'accès manipulées (O.EFFACEMENT_CLES).

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

- Enregistre les événements en relation avec la gestion des accès à une zone (O.AUDIT).

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 (Edition complète seulement). L'application de toute nouvelle politique est conditionnée par le succès de cette vérification.

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

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

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 couvrir cette 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),

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.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.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_ITT.1	FDP_ACC.1 ou FDP_IFC.1	FDP_ACC.1
FDP_RIP.1	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_REV.1	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	Aucune	Aucune
FMT_SMR.1	FIA_UID.1	FIA_UID.2

Tableau 7 : 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 8 : 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_ITT.1	FDP_RIP.1	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_REV.1	FMT_SMF.1	FMT_SMR.1
O.AUTH							X	X	X	X		X	X	X								
O.ROLES							X	X							X				X	X	X	X
O.CHIFFREMENT			X	X		X				X												
O.EFFACEMENT_CLES											X											
O.ALGO_STD			X	X	X	X																
O.ADM_ZONES															X						X	X
O.ADM_ACCES															X	X	X	X		X	X	X
O.INT_POLICIES						X													X			
O.AUDIT	X	X																				

Tableau 9 : 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 un fichier chiffrée qu'après présentation d'une clé d'accès valide pour le fichier.

Afin de remplir cet objectif :

- La TOE identifie et authentifie chaque utilisateur avant de permettre toute opérations (FIA_UAU.2 et FIA_UID.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). Cette authentification est également nécessaire en cas d'interception des données entre le serveur et le poste client dans la mesure où ces données transitent chiffrées (FDP_ITT.1) pendant le téléchargement.

O.ROLES	La TOE doit gérer deux 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) et un rôle 'administrateur' (utilisation, recouvrement, plus possibilité d'administrer la zone chiffrée, c'est-à-dire gérer ses accès, modifier ses propriétés).

Afin de remplir cet objectif :

- La TOE doit gérer et distinguer les rôles d'administrateur de la TOE et d'utilisateur de la TOE (FMT_SMR.1) et restreindre les fonctions d'administration à l'administrateur (FMT_MOF.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).
- Enfin, la TOE doit permettre de restreindre à l'administrateur les fonctions d'administration de la sécurité (FMT_SMF.1), la révocation des utilisateurs (FMT_REV.1) et la modification des « policies » (FMT_MTD.1).

8.2.4.2 Cryptographie

O.CHIFFREMENT	La TOE doit chiffrer (déchiffrer/transchiffrer) les « zones » configurées par l'emploi de clés cryptographiques. Ces opérations cryptographiques doivent s'effectuer sur le poste de travail de l'utilisateur ou de l'administrateur. La TOE doit utiliser des clés différentes pour protéger les différentes «zones» configurées, même si les utilisateurs sont les mêmes pour ces « zones ».La TOE doit générer ces clés de chiffrement conformément aux exigences pour le niveau de robustesse standard des référentiels cryptographiques [CRYPTO_STD] et [CLES_STD] de l'ANSSI.

Afin de remplir cet objectif :

- Pour chiffrer (déchiffrer/transchiffrer) les zones configurées, 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).

- Ces opérations s'effectuent en local sur le poste de travail et les données sont donc chiffrées lorsqu'elles transitent entre le poste et le serveur (FDP_ITT.1).

O.EFFACEMENT_CLES La TOE doit assurer le nettoyage des traces de données sensibles (clés de chiffrement des fichiers, éléments permettant de retrouver les clés d'accès) dans la mémoire (RAM) dès la fin des opérations réalisées par la TOE.

Afin de remplir cet objectif :

- La TOE assure un nettoyage totalement sécurisé des clés dans la mémoire RAM (FDP_RIP.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.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» (Edition complète seulement).

Afin de remplir cet objectif :

- La TOE offre des fonctions d'administration et de gestions (FMT_SMF.1) des zones
- La TOE assure que seul l'administrateur de la TOE peut gérer le comportement de chiffrement des « zones » (FMT_MOF.1 associé à FMT_SMR.1).

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

Afin de remplir cet objectif :

- La TOE offre des fonctions d'administration et de gestions (FMT_SMF.1) ainsi que de révocation (FMT_REV.1) des accès
- La TOE limite les accès à ces fonctions d'administration et de gestion en fonction du rôle associé aux utilisateurs (FMT_MOF.1 associé à FMT_SMR.1).
- La TOE assure que seul l'administrateur de la TOE peut gérer les attributs de sécurité des objets stockés : clés et rôles (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).

8.2.4.4 Protections lors de l'exécution

O.INT_POLICIES	La TOE doit vérifier la signature de toutes nouvelles politiques de sécurité à appliquer (Edition complète seulement). En cas d'échec lors de la vérification, les politiques appliquées restent inchangées.

Afin de remplir cet objectif :

- La TOE 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.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 qui considèrera un niveau d'attaquant correspondant au niveau élémentaire renforcé ou inférieur (l'utilisateur final est alors assuré que la TOE est résistante à des attaques de pénétration effectuées par des attaquants possédant un faible potentiel d'attaque).
- L'évaluation de l'architecture de sécurité et de l'architecture logiciel incluant l'analyse de l'implémentation (fonctions cryptographiques seulement) pour vérifier qu'il n'y a pas de défaut de sécurité
- De bonnes pratiques en matière de développement de la partie cryptographique (l'utilisateur final est alors assuré que le produit a été correctement et sécuritairement conçu et développé).
- De bonnes pratiques en matière de maintenance et support aux utilisateurs assurant que toutes les anomalies identifiées seront corrigées et rapportées aux utilisateurs du produit considéré qui pourraient être affectés par cette anomalie.

8.3. 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.OPERATIONS_CRYPTO	F.CONTROLE_ACCES_ZONE	F.ENTREE_SECURISEE	F.GESTION_CLES	F.GESTION_ZONES	F.AUDIT
FAU_GEN.1	Génération de données d'audit	X	X	X	X	X	X	X
FAU_GEN.2	Lien entre l'identité de l'utilisateur	X	X	X	X	X	X	X
FCS_CKM.1	Génération de clés cryptographiques					X	X	
FCS_CKM.3	Accès aux clés cryptographiques				X	X		
FCS_CKM.4	Destruction de clés cryptographiques					X	X	
FCS_COP.1	Opération cryptographique		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_ITT.1	Protection de base des transferts internes			X				
FDP_RIP.1	Protection d'une partie 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			
FIA_UID.2	Identification d'un utilisateur préalablement à toute action			X	X			
FMT_MOF.1	Administration des fonctions de la TSF			X		X	X	
FMT_MSA.1	Gestion des attributs de sécurité			X		X		
FMT_MSA.2	Attributs de sécurité sûrs	X				X		
FMT_MSA.3	Initialisation statique d'attribut					X		
FMT_MTD.1	Gestion des données de la TSF	X						
FMT_REV.1	Révocation					X	X	
FMT_SMF.1	Spécification des fonctions d'administration					X	X	
FMT_SMR.1	Rôles de sécurité					X		

Tableau 10 : 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:

- La vérification de la signature des politiques de sécurité (F.CONFIGURATION_TOE),
- Les opérations de gestion des zones : chiffrement, déchiffrement, transchiffrement de zone (F. GESTION_ZONES),
- Les opérations de gestion des clés d'accès : création, suppression (F.GESTION_CLES),
- Les opérations de contrôle d'accès : réussite ou échec de l'authentification (F.CONTROLE_ACCESS_ZONES).
- Les opérations d'accès aux clés, succès ou échec (F.ENTREE_SECURISEE)
- Les opérations cryptographiques nécessaires au fonctionnement de ZonePoint (F.OPERATIONS_CRYPTO)

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 :

- La vérification de la signature des politiques de sécurité (F.CONFIGURATION_TOE),
- Les opérations de gestion des zones : chiffrement, déchiffrement, transchiffrement de zone, (F. GESTION_ZONES),
- Les opérations de gestion des clés d'accès : création, suppression (F.GESTION_CLES),
- Les opérations de contrôle d'accès : réussite ou échec de l'authentification (F.CONTROLE_ACCESS_ZONES).
- Les opérations d'accès aux clés, succès ou échec (F.ENTREE_SECURISEE)
- Les opérations cryptographiques nécessaires au fonctionnement de ZonePoint (F.OPERATIONS_CRYPTO)

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. 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.

Les fonctions de sécurité F.GESTION_ZONES (clé de zone) F.GESTION_CLES (clé RSA) implémente cette exigence fonctionnelle.

FCS_CKM.3 Accès aux clés cryptographiques

L'accès aux clés cryptographiques gérées par la TOE est implémenté par la fonction de sécurité F.GESTION_CLES en s'appuyant sur F.ENTREE_SECURISEE pour la protection des données en entrée.

Cette fonction est utilisée lors de toute authentification utilisateur.

FCS_CKM.4 Destruction de clés cryptographiques

La clé qui a permis le chiffrement des fichiers de la zone est obtenue après entrée de la clé d'accès utilisateur. Cette clé de chiffrement est détruite dès la fin de l'opération sur le fichier (déchiffrement d'un fichier que l'on a téléchargé du serveur ou chiffrement d'un fichier que l'on télécharge vers le serveur).

La fonction de sécurité F.GESTION_ZONES implémente cette exigence.

Ensuite les éléments permettant de retrouver la clé d'accès (mot de passe, ouverture du fichier de clé ou du token) sont détruits lorsque le poste est réinitialisé ou la session fermée voire verrouillée.

La fonction de sécurité F.GESTION_CLES implémente cette exigence.

FCS_COP.1 Opération cryptographique

La TOE effectue les opérations cryptographiques suivantes :

- Récupère une clé d'accès avant de pouvoir créer une clé de zone (initialisation),

- Récupère une clé d'accès pour déchiffrer la clé de la zone avant de pouvoir ajouter une nouvelle clé d'accès qui va chiffrer la clé de zone (ajout d'accès, si c'est un mot de passe une dérivation est également effectuée),
- Récupère une clé d'accès avant de pouvoir déchiffrer la clé de zone, afin de pouvoir chiffrer ou déchiffrer la zone,
- Récupère une clé d'accès avant de pouvoir transchiffrer la clé de zone (création d'une nouvelle clé, déchiffrement puis chiffrement de la zone)
- Récupère une clé d'accès avant de pouvoir déchiffrer une clé de zone et ainsi pouvoir chiffrer ou déchiffrer les fichiers de la zone.
- 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 les fichiers de 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.

La fonction F.GESTION_ZONES assure le chiffrement, déchiffrement et transchiffrement des zones.

Les fonctions F.GESTION_CLES (création de la clé d'accès à partir du mot de passe) et F.CONTROLE_ACCES_ZONE (vérification de la clé d'accès) utilisent les fonctions de dérivation des clés à partir des mots de passe.

La fonction F.ENTREE_SECURISEE utilise des fonctions de wrapping pour assurer le transfert sécurisé des clés entre la TOE et les porte-clés physique.

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 pour la configuration des droits d'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),
- 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_ITT.1 Protection de base des transferts internes

Les données utilisateurs ne sont pas déchiffrées sur le serveur mais localement sur le poste. Pour accéder à ces données chiffrées il faut alors fournir une clé d'accès valide (F.CONTROLE_ACCES_ZONE).

FDP_RIP.1 Protection d'une partie des informations résiduelles

Le processus d'effacement des clés est totalement sécurisé. En effet, ZonePoint efface les clés de chiffrement dès qu'elles sont utilisées et détruit les éléments des clés d'accès sur les événements système fermeture de session, mise en veille, verrouillage de session et fermeture du poste.

Cette exigence fonctionnelle est mise en œuvre par la fonction de sécurité F.GESTION_CLES qui gère l'effacement sécurisé des clés d'accès et par F.GESTION_ZONES qui gère l'effacement sécurisé des clés de chiffrement des zones.

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 doit recommencer sa demande d'authentification (ce qui le ralenti entre ses différentes séquences d'essais).

La fonction de sécurité F.CONTROLE_ACCES_ZONE couvre cette fonctionnalité et la configuration du nombre d'essais 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.

Cette exigence fonctionnelle est implémentée par F.CONTROLE_ACCES_ZONE pour contrôler l'accès aux zones et 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.

Cette exigence fonctionnelle est implémentée par F.CONTROLE_ACCES_ZONE pour contrôler l'accès aux zones et F.ENTREE_SECURISEE pour sécuriser la communication des données fournies en entrée vers la TOE.

FMT_MOF.1 Administration des fonctions de la TSF

Seul l'administrateur de la TOE peut déterminer le comportement, ou modifier le comportement des fonctions de contrôle d'accès (rôles), de gestion des accès et de gestion des zones.

Les fonctions de sécurité F.GESTION_CLES (contrôle du rôle pour la gestion des accès) et F.GESTION_ZONES (contrôle du rôle pour la gestion des zones) associées à F.CONTROLE_ACCES_ZONE (entrée de la clé) implémentent cette exigence.

FMT_MSA.1 Gestion des attributs de sécurité

Seuls l'administrateur a la possibilité de changer 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 ZonePoint.

Les fonctions de sécurité F.GESTION_CLES associée à F.CONTROLE_ACCES_ZONE (entrée de la clé) implémentent cette exigence.

FMT_MSA.2 Attributs de sécurité sûrs

Les fonctions de sécurité F.GESTION_CLES et F.CONFIGURATION_TOE (force des mots de passe, contrôle des certificats par exemple) permettent 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 (changement du rôle par exemple) met en œuvre cette exigence.

FMT_MTD.1 Administration des données de la TSF

Seuls l'administrateur 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_REV.1 Révocation

Seuls l'administrateur de la TOE a la possibilité de révoquer les utilisateurs en supprimant leurs accès et en transchiffrant les zones qui ont contenu cet accès.

Cette exigence est implémentée par la fonction de sécurité F.GESTION_CLES pour la destruction de l'accès et F.GESTION_ZONES pour l'opération de transchiffrement.

FMT_SMF.1 Spécification des fonctions d'administration

La TOE permet de réaliser :

- Les fonctions de contrôle d'accès aux opérations d'administration de la sécurité

- Les fonctions de gestion des clés (y compris les clés de recouvrement)
- Les fonctions de gestion des zones

Cette exigence fonctionnelle est implémentée par les fonctions de sécurité F.GESTION_ZONES (gestions des zones) et F.GESTION_CLES (rôles et gestion des clés)

FMT_SMR.1 Rôles de sécurité

La TOE supporte les rôles utilisateur et administrateur.

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

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 septembre 2012 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_ITT.1	Basic internal transfer protection
FDP_RIP.1	Subset 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_REV.1	Revocation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles

Tableau 11 : 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 du contrôle d'accès (succès et échecs) ;** **- Evénements journalisés au titre de la gestion des zones (chiffrement, déchiffrement, transchiffrement) ;** **- Evénements journalisés au titre de la gestion des accès aux zones (modification ou ajout d'accès sur 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 (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [**none**]**.**
FAU_GEN.2	User identity association
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

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, génération d'exposants Diffie-Hellman et diversification de clés**] and specified cryptographic key sizes [**de 128, 192 et 256 bits pour les clés symétriques et de 1024 à 2048 bits pour les clés asymétriques**] that meet the following: [**exigences cryptographique de l'ANSSI définies dans [CRYPTO_STD] et [CLES_STD]**]. **Non editorial refinement:** **L'Edition Light n'effectue que la diversification de clés pour obtenir la clé d'accès de l'utilisateur à partir de son mot de passe.**
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 par la clé d'accès**] that meets the following: [**Aucun**]. **Non editorial refinement:** **Ce composant s'applique en totalité à l'Edition complète qui réalise notamment toutes les fonctions d'administration sensibles. Par contre, l'Edition Light ne contient pas de driver clavier et utilise exclusivement la fonction de déchiffrement des clés.**
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 chiffrement, le déchiffrement, la vérification de la signature des politiques de sécurité, la génération de clés, le wrapping de clés et la dérivation de clés**] in accordance with a specified cryptographic algorithm [**SHA-1 (dérivation de clé), SHA-256, RSA, AES**] and cryptographic key sizes [**de 128, 192 et 256 bits pour les clés symétriques et de 1024 à 2048 bits pour les clés**

	asymétriques] that meet the following: [**exigences cryptographique de l'ANSSI définies dans [CRYPTO_STD] et [CLES_STD]**].
	Non editorial refinement :
	L'Edition Light ne permet que le chiffrement et déchiffrement des fichiers ainsi que la dérivation de clé et la fonction de hachage associée.

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** : **Administrateur et utilisateurs de la TOE** **Objets : Fichiers protégés par la TOE dans une « zone »** **Opérations : Gestion des zones 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: Administrateur et utilisateurs de la TOE** **Attributs de sécurité : Clés d'accès permettant ou non d'ouvrir la zone et rôle**]**.** **Non editorial refinement:** **Il n'y a pas de rôle administrateur dans l'Edition Light, cette édition ne gère que le rôle utilisateur.**
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 following additional rules: [**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 et SFP.ACCESS_ROLES**] 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_ITT	**Internal TOE transfer**
FDP_ITT.1	Basic internal transfer protection
FDP_ITT.1.1	The TSF shall enforce the [**SFP.ACCESS_OBJ**] to prevent the [**disclosure**] of user data when it is transmitted between physically-separated parts of the TOE. **Application note :** **Concerne le transfert des données entre la partie serveur de la TOE et la partie sur le poste client.**

FDP_RIP	**Residual information protection**
FDP_RIP.1	Subset residual information protection
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**désallocation de la ressource de**] the following objects: [**Clés de chiffrement des fichiers et clés d'accès**].

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 [**déterminer le comportement ou modifier le comportement de**] the functions [**de contrôle d'accès (rôles), de gestion des accès et de gestion des zones]** to [**administrateur de la TOE**]. **Non editorial refinement:** **Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion).**

FMT_MSA	**Management of security attributes**
FMT_MSA.1	Management of security attributes
FMT_MSA.1.1	The TSF shall enforce the [**SFP.ACCESS_ROLES]** to restrict the ability to [**changer la valeur par défaut, modifier ou supprimer**] the security attributes [**clés d'accès et rôles**] to [**administrateur de la TOE**]. **Non editorial refinement:** **Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion d'accès).**
FMT_MSA.2	Secure security attributes
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for [**les clés d'accès et les roles**].
FMT_MSA.3	Static attribute initialisation
FMT_MSA.3.1	The TSF shall enforce the [**SFP.ACCESS_ROLES**] 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. **Non editorial refinement:** **Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion).**
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 [**administrateur de la TOE**]. **Non editorial refinement:** **Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion d'accès).**
FMT_REV	**Revocation**
FMT_REV.1	Revocation
FMT_REV.1.1	The TSF shall restrict the ability to revoke [**clés d'accès utilisateur**] associated with the [**users**] under the control of the TSF to [**administrateur de la TOE**].
FMT_REV.1.2	The TSF shall enforce the rules [**accès de l'utilisateur supprimé par l'administrateur et transchiffrement des zones contenant cet accès**]. **Non editorial refinement:** **Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion d'accès).**
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 contrôle d'accès aux opérations d'administration de la sécurité (rôle)** - **Les fonctions de gestion des clés (y compris les clés de recouvrement)** - **Les fonctions de gestion des zones**] **Non editorial refinement:** **Ce composant ne s'applique qu'à l'Edition complète (l'Edition Light ne permet pas d'effectuer d'opérations de gestion**

	d'accès).
FMT_SMR	**Security management roles**
FMT_SMR.1.	Security roles
FMT_SMR.1.1	The TSF shall maintain the roles [**administrateur de la TOE et utilisateur de la TOE**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.