



version 3.1

Cible de Sécurité
CC niveau EAL2+

Document v2 révision 6.

Sommaire

1. INTRODUCTION DE LA CIBLE DE SECURITE	6
1.1. Identification de la cible de sécurité	6
1.2. Vue d'ensemble de la cible de sécurité	6
1.3. Conformité aux Critères Communs	6
1.4. Conformité aux référentiels DCSSI.....	7
2. DESCRIPTION DE LA CIBLE D'EVALUATION (TOE)	8
2.1. Présentation du produit ZoneCentral	8
2.1.1. Description Générale.....	8
2.1.2. La technologie de ZoneCentral	9
2.1.3. Les zones et les accès	10
2.1.4. Les fichiers d'accès	11
2.1.5. Autres fonctionnalités	12
2.1.6. Les conteneurs chiffrés (module Zed!).....	13
2.1.7. Restrictions et avertissements sur la sécurité	13
2.2. Services d'administration et rôles	14
2.2.1. Définition des rôles.....	14
2.2.2. Exemple d'utilisation.....	15
2.3. Périmètre et architecture de la cible d'évaluation	17
2.3.1. Les composants de ZoneCentral	17
2.3.2. Périmètre de la TOE.....	18
2.4. Les biens sensibles	20
2.4.1. Biens sensibles de l'utilisateur	20
2.4.2. Biens sensibles de la TOE	21
2.4.3. Synthèse des biens sensibles	23
2.5. Plate-forme de tests pour l'évaluation de la TOE	24
3. ENVIRONNEMENT DE SECURITE DE LA TOE	25
3.1. Hypothèses	25
3.2. Menaces [contre les biens sensibles de la TOE].....	26
3.3. Politiques de sécurité de l'organisation	26
4. OBJECTIFS DE SECURITE	28
4.1. Objectifs de sécurité pour la TOE.....	28
4.1.1. Contrôle d'accès.....	28
4.1.2. Cryptographie.....	28
4.1.3. Gestion des zones	29
4.1.4. Effacement.....	29
4.1.5. Protections lors de l'exécution	29
4.2. Objectifs de sécurité pour l'environnement	30

4.2.1. Installation.....	30
4.2.2. Utilisation.....	30
4.2.3. Formation des utilisateurs	31
4.2.4. Administration	31
5. EXIGENCES DE SECURITE DES TI	33
5.1. Exigences de sécurité de la TOE	33
5.1.1. Exigences fonctionnelles de sécurité de la TOE.....	33
5.1.2. Niveau de résistance des exigences fonctionnelles.....	39
5.1.3. Exigences d'assurance de sécurité de la TOE	39
5.2. Exigences de sécurité sur la partie TI de l'environnement	43
5.2.1. Système d'horodatage fiable	43
5.2.2. Signature des composants de la TOE.....	43
6. SPECIFICATIONS GLOBALES DE LA TOE.....	44
6.1. Fonctions de sécurité de la TOE.....	44
6.2. Niveau de résistance des fonctions	45
6.3. Mesures d'assurance.....	46
6.3.1. Mesures de l'environnement de développement	46
6.3.2. MA.DEV : Documentation et outils de développement des fonctions de sécurité ..	47
6.3.3. Test des fonctions de sécurité	48
6.3.4. Documentation d'exploitation.....	48
6.3.5. MA.VUL : Estimation de la vulnérabilité.....	49
7. ANNONCES DE CONFORMITE A UN PP.....	51
8. ARGUMENTAIRE.....	52
8.1. Argumentaire pour les objectifs de sécurité.....	52
8.1.1. Hypothèses	52
8.1.2. Menaces	54
8.1.3. Politiques de sécurité de l'organisation	57
8.2. Argumentaire pour les exigences de sécurité.....	62
8.2.1. Dépendances entre exigences fonctionnelles de sécurité	62
8.2.2. Argumentaire pour les dépendances non satisfaites.....	63
8.3. Argumentaire de couverture des objectifs de sécurité par les exigences fonctionnelles.....	63
8.3.1. Contrôle d'accès.....	64
8.3.2. Cryptographie.....	66
8.3.3. Gestion des zones	67
8.3.4. Effacement.....	68
8.3.5. Protections lors de l'exécution	69
8.3.6. Objectifs sur l'environnement.....	69
8.3.7. Argumentaire pour le support mutuel des exigences fonctionnelles	70
8.4. Argumentaire pour les spécifications globales de la TOE.....	71

8.5. Argumentaire pour les mesures d'assurance	81
8.6. Argumentaire pour les annonces de conformité à un PP	82
8.7. Pertinence du niveau d'assurance	82
8.8. Pertinence du niveau de résistance des fonctions exigées.....	83
9. ANNEXE A : EXIGENCES DE SECURITE DE LA TOE	84
9.1. Exigences fonctionnelles de sécurité de la TOE	84
9.1.1. Class FAU : Security audit	85
9.1.2. Class FCS : Cryptographic support	86
9.1.3. Class FDP : User data protection.....	86
9.1.4. Class FIA : Identification and authentication.....	88
9.1.5. Class FMT : Security management	88
9.1.6. Class FPT : Protection of the TSF	89
9.1.7. Class FTA : TOE access	90
9.1.8. Class FTP : Trusted path/channels	90
9.2. Exigences d'assurance de sécurité de la TOE.....	90
9.2.1. Class ADV : Développement.....	90
9.2.2. Class ALC : Life cycle support.....	92

Liste des figures

Figure 1 - Périmètre de la TOE.....	18
Figure 2 - Plate-forme de tests pour l'évaluation de la TOE	24

Liste des tableaux

Tableau 1 : Synthèse des biens sensibles	23
Tableau 2 : Exigences fonctionnelles de sécurité pour la TOE	33
Tableau 3 : Composants d'assurance de sécurité.....	39
Tableau 4 : Mécanismes de sécurité non cryptographiques	45
Tableau 5 : Couverture des hypothèses par les objectifs de sécurité	52
Tableau 6 : Couverture des menaces par les objectifs de sécurité	55
Tableau 7 : Couverture des politiques de sécurité de l'organisation par les objectifs de sécurité	57
Tableau 8 : Satisfaction des dépendances entre exigences fonctionnelles de sécurité	62
Tableau 9 : Couverture des objectifs de sécurité sur l'environnement par les exigences fonctionnelles de sécurité sur l'environnement	63
Tableau 10 : Couverture des objectifs de sécurité par les exigences fonctionnelles de sécurité	64
Tableau 11 : Couverture des exigences fonctionnelles par les spécifications globales de la TOE	71
Tableau 12 : Couverture des exigences d'assurance sécurité par les mesures d'assurance.....	81
Tableau 13 : Exigences fonctionnelles de sécurité pour la TOE	84

1. Introduction de la cible de sécurité

1.1. Identification de la cible de sécurité

Cible d'évaluation (TOE) :	ZoneCentral v3.1 Build 533 pour les plates-formes PC sous Microsoft Windows 2000/XP/Vista/2003
Niveau EAL :	EAL2 augmenté de ALC_FLR.3, AVA_VLA.2, ADV_HLD.2, AVA_MSU.1 et ALC_DVS.1, ainsi que ADV_LLD.1, ALC_TAT.1 et ADV_IMP.1 pour les mécanismes cryptographiques (FCS).
Résistance des fonctions :	SOF-High
Conformité à un PP existant :	Aucune.
Référence des CC :	Critères Communs version 2.3, Parties 1 à 3 – Août 2005

1.2. Vue d'ensemble de la cible de sécurité

ZoneCentral est un produit de sécurité pour la confidentialité des données des entreprises. Il agit comme une couche de sécurité intégré au système, il devient transparent pour les utilisateurs et peut appliquer la sécurité à tous les systèmes de fichiers : locaux, amovibles, réseau... En appliquant le chiffrement « in-place », il n'y a aucun impact sur l'organisation des données de l'entreprise.

ZoneCentral sera évalué pour une plate-forme PC sous les systèmes d'exploitation Microsoft Windows 2000/XP/Vista/2003.

1.3. Conformité aux Critères Communs

Cette cible de sécurité respecte les exigences des Critères Communs version 2.3 de Août 2005. Tous les composants fonctionnels décrits dans cette cible de sécurité sont issus de la Partie 2 des Critères Communs version 2.3 de Août 2005. Le niveau d'assurance « EAL2 augmenté » retenu est conforme à la Partie 3 de Critères Communs version 2.3 d'Août 2005.

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

Le niveau de résistance minimum demandé pour les fonctions de sécurité de la TOE et pour les exigences fonctionnelles de sécurité de la TOE est « SOF-High ». Aucune annonce spécifique supplémentaire de résistance des fonctions n'est formulée.

1.4. Conformité aux référentiels DCSSI

Cette cible de sécurité est conforme aux référentiels de la DCSSI suivants :

- [QUALIF_STD] « Processus de qualification d'un produit de sécurité – niveau standard – version 1.0 du 28 juillet 2003 n° 001591/SGDN/DCSSI/SDR », DCSSI.
- [CRYPTO_STD] « Mécanismes de cryptographie : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard. Version 1.10 du 19 décembre 2006 n°2739/SGDN/DCSSI/SDS/LCR », DCSSI.
- [CLES_STD] « Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques de niveau de robustesse standard - version 1.0 du 13 mars 2006 n° 724/SGDN/DCSSI/SDS/AsTeC »,DCSSI
- [AUTH_STD] « Authentification : Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard - version 0.13 du 12 avril 2007 n° 729/SGDN/DCSSI/SDS/AsTeC », DCSSI

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

2.1. Présentation du produit ZoneCentral

2.1.1. Description Générale

ZoneCentral est un **produit de sécurité** pour postes de travail opérant sous Windows 2000, Windows XP et Windows Vista. Son rôle est de préserver la confidentialité des documents manipulés par les utilisateurs, sur des postes isolés, des ordinateurs portables, ou des postes de travail connectés à un réseau d'entreprise.

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

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

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

Pour chaque zone chiffrée, il est possible de définir un certain nombre d'**accès** : l'accès de l'utilisateur principal, d'un collègue ou d'un chef de service éventuel, l'accès réservé du responsable de la sécurité, l'accès de secours de l'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 un mot de passe 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 zones et des fichiers.

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

Il intègre également un service automatique et transparent d'**effacement sécurisé par surcharge** : tout fichier (chiffré ou non) supprimé sur un disque local est

automatiquement effacé (réécriture de son contenu avec du « bruit ») avant d'être effectivement supprimé. Cela concerne également les fichiers temporaires créés par les applications.

ZoneCentral intègre également une technologie appelé **ZED!** qui permet aux utilisateurs de fabriquer des **conteneurs chiffrés**, dans lesquels ils peuvent copier des fichiers, et qu'ils peuvent envoyer à des correspondants ou archiver. L'utilisateur peut définir lui-même les accès à ces conteneurs, par exemple pour introduire un mot de passe dont il a convenu avec un correspondant. Il est à noter que les logiciels « ZED! » et « ZED ! Edition limitée », qui s'appuient sur cette technologie, sont des produits extérieurs à ZoneCentral.

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

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

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

2.1.2. La technologie de ZoneCentral

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

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

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

2.1.3. Les zones et les accès

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

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

Pour pouvoir utiliser une zone chiffrée, un utilisateur doit disposer d'une **clé d'accès**. Cette clé lui a été remise par l'Administrateur de la Sécurité (appelé Administrateur de la TOE dans la suite du document). Il peut s'agir soit d'un mot de passe, soit 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).

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

ZoneCentral propose différents algorithmes et mécanismes de sécurité, tous conformes à l'état de l'art en la matière. Il propose deux schémas de gestion de clés d'accès qui peuvent être utilisés en même temps sur les mêmes zones. Un schéma dit « symétrique » basé sur des mots de passe et des clés dérivées de mots de passe (réf. : PKCS#5) et un schéma dit « asymétrique » utilisant des clés RSA (réf. : PKCS#1 v1.5) embarquées dans des fichiers de clés (réf. : PKCS#12) ou des porte-clés (ref: PKCS#11 et/ou CSP).

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

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

événement système ne s'est pas produit, comme un verrouillage de session Windows, un déclenchement de l'économiseur d'écran ou l'arrêt du système.

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

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

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

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

2.1.4. Les fichiers d'accès

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

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

Les fichiers d'accès sont référencés par leur nom de fichier, mais sans l'emplacement qui, lui, est spécifié dans une stratégie de sécurité («Policy»). Il y a **l'emplacement principal** et un emplacement **secondaire**, pouvant servir de «cache local». Quand un utilisateur ouvre une zone référençant des fichiers d'accès, ZoneCentral recherche le fichier dans l'emplacement principal. S'il le trouve, il en fait une copie dans l'emplacement secondaire. S'il ne le trouve pas, il regarde dans l'emplacement secondaire. S'il ne le trouve toujours pas, il proposera les autres solutions disponibles, s'il y en a dans la zone. Ce mécanisme a été prévu pour que l'emplacement principal soit sur un partage réseau et que l'emplacement secondaire soit local. La copie de secours permet de continuer à fonctionner si le réseau n'est pas disponible (cas des postes nomades)

Les zones deviennent de cette façon des entités 'techniques' et l'administration réelle, celles des utilisateurs, est facilitée et centralisée.

Pour simplifier la procédure d'administration, il existe un mode de gestion appelé «fichier d'accès personnel». Ce mode permet à l'utilisateur, la toute première fois qu'il utilise le produit, de créer un fichier d'accès, qui comprendra son propre accès (il fournit sa clé d'accès) et les accès obligatoires définis en «Policy» par l'administrateur (accès du chef de service, du responsable de la sécurité, du recouvrement d'entreprise, ...). Ce mode évite à l'administrateur de devoir préparer des fichiers d'accès pour chaque utilisateur, tout en imposant quand même les contraintes de sa politique de sécurité. Ce fichier d'accès sera ensuite utilisé à chaque fois que l'utilisateur définit une zone chiffrée (si l'administrateur lui en a laissé le droit).

2.1.5. Autres fonctionnalités

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

ZoneCentral détecte les **fichiers d'échange** ('swap') de Windows et assure leur chiffrement en permanence.

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

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

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

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

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

ZoneCentral supporte également les **profils itinérants** (« roaming ») chiffrés, les **dossiers redirigés** du profil (« redirected folders »), ainsi que les **dossiers**

synchronisés disponibles hors connexion (« offline folders »), qui peuvent à la fois être chiffrés sur l'image serveur et sur la copie local (« CSC »).

2.1.6. Les conteneurs chiffrés (module Zed!)

ZoneCentral fournit également un sous-produit applicatif permettant aux utilisateurs de fabriquer des **conteneurs de fichiers compressés et chiffrés**. Ces conteneurs sont destinés à servir d'archive, ou, plus généralement, de pièce-jointe chiffrée dans des courriers électroniques.

L'ergonomie est similaire aux fichiers «ZIP» standards sous XP. L'utilisateur peut déposer des fichiers, les renommer, les supprimer, les extraire, etc.

Le conteneur reprend les principes de ZoneCentral pour le chiffrement et les accès (il est, de ce point de vue, totalement intégré à ZoneCentral). Après avoir fabriqué un conteneur (qui sera par défaut chiffré avec la clé de l'utilisateur et les accès définis par l'administrateur), l'utilisateur peut ajouter des accès pour ses correspondants (mots de passe ou certificats RSA).

Il existe un logiciel compagnon appelé «**Zed! Edition Limitée**» qui permet aux correspondants de lire les conteneurs (moyennant la fourniture d'une clé d'accès) et d'en extraire les fichiers. Il a également le droit de modifier le contenu du conteneur (enlever, ajouter des fichiers) pour pouvoir le renvoyer à l'émetteur d'origine. L'édition limitée (gratuite) ne lui permet pas, cependant, de créer de nouveaux conteneurs ou d'en modifier les accès.

Cette édition limitée embarque tous les composants de ZoneCentral nécessaires à son fonctionnement, mais sous une forme technique différente, embarquée et allégée, fonctionnant en mode «user» (i.e non driver) uniquement.

2.1.7. Restrictions et avertissements sur la sécurité

- Fichiers d'hibernation (hiberfil.sys) : ZoneCentral est compatible avec les suspensions prolongées : les zones (et les clés d'accès) sont correctement fermées automatiquement et les «caches» de fichiers du système sont correctement purgés. L'hibernation n'introduit donc pas de facteur de risque pour ZoneCentral. Néanmoins, ZoneCentral -dans sa version actuelle- ne sait pas chiffrer les fichiers d'hibernation et ne les protège donc pas. Les résidus d'informations qui se trouvaient en mémoire des applications utilisateur au moment de la suspension prolongée peuvent donc subsister à l'intérieur de ce fichier (ce qui n'est pas le cas des fichiers swap, que ZoneCentral sait chiffrer). Il est donc recommandé, pour une meilleure sécurité du poste, de désactiver la suspension prolongée (et de lui préférer une fermeture de session Windows).
Nota : dans tous les cas, au réveil, ZoneCentral détecte qu'il existe un fichier d'hibernation et alors procède automatiquement à l'effacement par surcharge de son contenu.
- Autres systèmes de chiffrement utilisant la même technologie, dont l'EFS : ZoneCentral n'est pas compatible avec un système de chiffrement sous-jacent. Par contre, ZoneCentral reste compatible avec les produits 'applicatifs' de chiffrement courants du marché.

- « Crash Dumps » : ZoneCentral ne sait pas chiffrer -dans sa version actuelle- les «dumps» effectués par Windows en cas de crash du système. Ces dumps peuvent contenir des résidus d'informations en mémoire des applications de l'utilisateur au moment du crash. Il est donc recommandé, pour une meilleure sécurité du poste, de désactiver la production de tels dumps (propriétés du poste de travail, onglet «avancé», option «Démarrage et récupération», choix «Ecriture des informations de débogage» à «aucun»).
- Registry : ZoneCentral ne sait pas chiffrer -dans sa version actuelle- les différents fichiers composant la Registry du système (partie 'machine' ou partie 'utilisateur'). Ces fichiers ne contiennent normalement pas d'informations confidentielles.
- Pour anticiper le départ d'un utilisateur qui serait le seul détenteur d'une zone chiffrée et dont les données ne seraient plus accessibles, l'administrateur doit systématiquement ajouter un accès à une personne désignée (lui-même, responsable sécurité ...) lors de la création de chaque zone.
- Pour révoquer un utilisateur, l'administrateur doit renouveler les clés de zone en effectuant une opération de déchiffrement puis chiffrement des zones auxquelles l'utilisateur avait accès.

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 (administrateur Windows) en charge de définir les règles d'usage et de sécurité (les polices), c'est-à-dire le paramétrage de fonctionnement du produit : cette opération de « haut-niveau » est effectuée sous le contrôle du Responsable de la Sécurité 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. Ces règles ne changeront ensuite que de façon très exceptionnelle. Il est à noter que ce rôle peut se décliner en plusieurs rôles hiérarchiques correspondant aux différents niveaux des domaines Windows. Dans ce cas les administrateurs des niveaux supérieurs doivent interdire aux administrateurs des sous-niveaux (domaines, contrôleurs de domaines, postes de travail) la modification des « polices » de la TOE qu'ils souhaitent eux-mêmes contrôler.

- Un rôle administrateur de la TOE en charge de définir les zones chiffrées du « parc » et effectuer la procédure de migration initiale qui consiste à chiffrer leur contenu actuel, sur les serveurs (partages) et sur les postes de travail. Pour chaque zone chiffrée, il faut configurer la liste des personnes pouvant y accéder en introduisant leurs clés d'accès (ou en paramétrant des listes d'accès). Par la suite, l'entretien consistera principalement à créer de nouvelles zones si besoin est

(nouveaux ordinateurs, nouveaux partages), à gérer les 'mouvements de personnel' (nouvel utilisateur pour une zone, retrait d'accès pour une personne en partance), et, éventuellement, de transchiffrer les zones chiffrées (sur compromission ou régulièrement). Sauf mention contraire dans la suite de ce document, toute référence à l'administrateur se rapporte à ce rôle.

- Un rôle utilisateur qui utilise la TOE selon la configuration imposée par l'administrateur Windows et l'administrateur de la TOE.

Il faut noter que, à part la définition des politiques, 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'entreprise.

ZoneCentral fournit différents outils permettant d'effectuer ces opérations, sous différentes formes techniques et ergonomiques pour s'adapter aux différentes méthodes de gestion : lignes de commandes scriptables, interfaces graphiques de préparation en 'amont', interfaces simplifiées et conviviales pour une utilisation par les utilisateurs eux-mêmes, etc.

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

- Lire ou modifier les politiques ;
- Créer une zone chiffrée (i.e. chiffrement initial d'un emplacement) ;
- Déchiffrer une zone chiffrée ;
- Transchiffrer (renouveler les clés de chiffrement) d'une zone chiffrée ;
- Définir une zone en clair (à ne pas chiffrer, volontairement) ;
- Consulter les accès d'une zone chiffrée, ajouter des accès ou en retirer ;
- Consulter ou modifier certaines propriétés 'techniques' de zones (le label, les exceptions) ;
- Rechercher les zones chiffrées ;
- Créer ou modifier des listes d'accès.

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

Par ailleurs, ZoneCentral émet des événements Windows consultables avec **l'Observateur d'Événements Windows** (Eventvwr). La liste des événements est configurable, et ils peuvent également être envoyés vers un serveur Windows. On y trouve notamment les événements d'ouverture et de fermeture de zones chiffrées par les utilisateurs, certains problèmes courants pour réparation (ex : une liste d'accès non trouvée), et toutes les commandes d'administration, réussies ou non.

2.2.2. 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 Windows définit les **règles d'usage (policies)** du produit, ce qui se traduit par une configuration prédéfinie (policy) qui peut être masterisée (personnalisation de l'installation) ou télé-gérée (diffusée, mise à jour) soit par des commandes d'administration fournies par le produit soit par la logistique intégrée des réseaux bureautiques (exemple : contrôleurs de domaines). Ces règles sont généralement établies à « haut niveau » dans l'entreprise par le Responsable de la Sécurité. Parmi ces règles, on trouve, par exemple, l'algorithme de chiffrement à utiliser, les opérations autorisées pour les utilisateurs standards, le comportement que doit adopter le logiciel dans certains cas, le nombre de passes de surcharge pour l'effacement sécurisé, etc.

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

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

Puis, l'administrateur de la TOE doit définir une politique de chiffrement sur les postes de travail ou les partages réseau, en fonction de leur contenu et/ou de leur topologie : il s'agit en pratique de définir **quelles zones doivent être chiffrées** et d'exécuter la procédure de chiffrement initial (car, la plupart du temps, ces zones existent déjà et ont déjà un contenu). L'exécution de la procédure peut être effectuée par l'administrateur lui-même ou être déléguée à l'utilisateur.

Une fois ces opérations initiales effectuées, les zones chiffrées sont définies et chiffrées, et les accès à ces zones pour les utilisateurs sont définis. Seuls les utilisateurs disposant de clés d'accès valides pour les zones chiffrées pourront lire ou écrire des fichiers dans ces zones.

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

A la première tentative d'accès à un fichier chiffré dans une zone chiffrée, ZoneCentral demande à l'utilisateur une clé d'accès permettant de déchiffrer le fichier (en pratique, le schéma est plus complexe, et cette clé d'accès permet de déchiffrer des clés intermédiaires qui elles-mêmes chiffreront les fichiers). Si l'utilisateur peut la fournir, alors le fichier peut être déchiffré (ou chiffré, s'il s'agit d'une création ou d'une écriture). Sinon, l'application se voit refuser l'accès avec le code erreur habituel « Accès non autorisé » (code que traitent bien toutes les applications). Par la suite, tous les autres fichiers de la même zone seront « servis » puisque les clés en sont désormais connues. Ceci, bien entendu, tant que les zones

ainsi ouvertes ne sont pas «fermées» (par l'utilisateur lui-même, par une fermeture de session Windows, etc.).

2.3. Périmètre et architecture de la cible d'évaluation

2.3.1. Les composants de ZoneCentral

L'installation configure les composants de base de ZoneCentral, qui sont trois drivers, un service système, et un «daemon» utilisateur (figure 1) :

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

D'autres composants sont également installés :

- Une extension du Winlogon de Windows, «**ZCWLX**», qui détecte les fermetures de session Windows, le déclenchement du Screensaver, ou l'arrêt du système pour fermer les zones chiffrées ouvertes et les clés d'accès ;
- Une extension de l'Explorateur Windows, «**ZCUSH**», qui personnalise les icônes des dossiers chiffrés (le comportement de ce composant est configurable dans les stratégies de sécurité), et qui affiche les propriétés des zones ; il peut également permette de chiffrer, déchiffrer, changer les accès des zones, si l'administrateur l'a autorisé ;
- Une extension de l'Explorateur Windows, «**ZEP**», qui gère les conteneurs chiffrés ;

- Une interface graphique simple et légère pour les utilisateurs, «**ZCGU**» ('Moniteur') leur permet de voir la liste des zones chiffrées ouvertes, les clés d'accès présentées, et la version du logiciel. Il permet également de fermer manuellement des zones et des clés. Les actions qu'il autorise sont configurables dans une stratégie de sécurité ;
- Deux outils de commande, «**ZCACMD**» et «**ZCUCMD**», le premier servant principalement à l'administrateur de la TOE pour la définition des zones chiffrées, le second étant un équivalent en mode commande de l'interface graphique «**ZCGU**».
- Un assistant de chiffrement «**ZCAPPLY**» qui est invoqué par ZoneCentral dès lors qu'une transformation de fichiers doit être effectuée : chiffrement, déchiffrement. ZCAPPLY peut également être invoqué en mode commande par l'administrateur de la TOE.
- Un éditeur graphique de listes d'accès et de profils de zone, «**ZCEDIT**» permet à l'administrateur de la TOE de préparer le déploiement en amont et d'administrer ensuite les accès aux zones.

2.3.2. Périmètre de la TOE

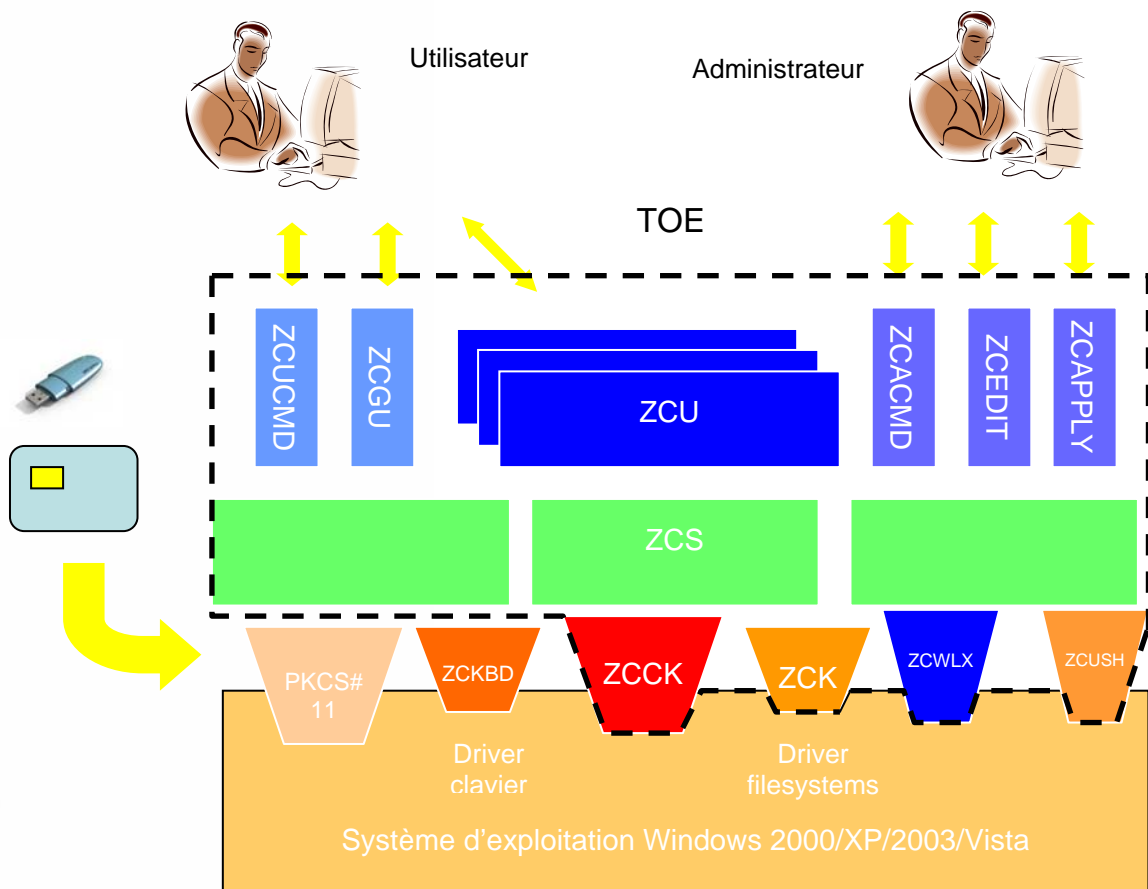


Figure 1 – Périmètre de la TOE

2.3.2.1 Périmètre logique

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

- Les conteneurs (produits « Zed ! » et « Zed ! Edition Limitée ») ;
- Les opérations de transchiffrement des clés de zone et de recouvrement.
- L'utilisation du mode SSO (Single Sign On) qui permet d'ouvrir automatiquement les zones chiffrées lorsque la session Windows est ouverte (mais reporte le niveau de sécurité à celui de Windows ou du composant SSO tiers).

Seuls les aspects logiciels de ZoneCentral seront évalués.

2.3.2.2 Périmètre physique

ZoneCentral sera évalué, en tant que produit, sur une plate-forme PC sous les systèmes d'exploitation de Microsoft suivants : Windows 2000, Windows XP, Windows Vista et Windows 2003.

Le dialogue PKCS#11 entre la TOE et les porte-clés utilisateurs, le dialogue PKCS#12 entre la TOE et les fichiers de clés, le dialogue réseaux entre la TOE et les données utilisateurs stockées sur des médias distants (serveur sur un réseau local ou sur Internet par exemple) seront également évalués.

Les éléments suivants sont hors évaluation :

- Le dialogue clavier entre la TOE et la saisie des mots de passe ;
- Les systèmes d'exploitation Windows, y compris :
 - Les drivers PC/SC ;
 - Le service de gestion des certificats (CMS) ;
 - Le service de gestion des profils utilisateurs (User management) ;
- Les portes clés utilisés (comme les porte-clés de type Token USB, les fichiers de clés ou les containers CSP).

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

2.4. Les biens sensibles

2.4.1. Biens sensibles de l'utilisateur

2.4.1.1 Clés d'accès

Pour ouvrir les zones chiffrées, ZoneCentral met en œuvre les clés d'accès des utilisateurs. En fonction des cas de figure, il peut être amené à manipuler directement soit la clé d'accès elle-même, soit son code confidentiel de protection.

- Accès par mot de passe : ZoneCentral gère la saisie du mot de passe, sa transformation (dérivation) en clé d'accès et effectue des chiffrements et déchiffrements avec cette clé d'accès ;
- Accès par clé RSA hébergée dans un fichier de clés : ZoneCentral gère la saisie du code confidentiel du fichier de clés, lit et déchiffre le fichier de clés avec ce code confidentiel, obtient la clé d'accès RSA et effectue des chiffrements et déchiffrements avec cette clé ;
- 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) : ZoneCentral gère la saisie du code confidentiel du token logique, le remet au composant externe pour le déverrouiller, 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 ;
- 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) : ZoneCentral ne gère pas la saisie du code confidentiel du token logique, c'est le composant externe qui le fait spontanément avec ses propres moyens, 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, ZoneCentral manipule comme biens sensibles un mot de passe ou code confidentiel (en saisie), et une clé d'accès cryptographique. Dans les cas 1 et 2, il manipule les deux éléments, dans le cas 3, il ne manipule que le premier, dans le cas 4, il n'en manipule aucun.

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

2.4.1.2 Fichiers chiffrés

ZoneCentral permet de conserver sous forme chiffrée les fichiers (et dossiers) relatifs à une zone chiffrée. Les biens sensibles sont donc les fichiers et dossiers utilisateurs, de tous types, stockés dans des zones chiffrées.

Les zones chiffrées sont repérables grâce à une icône caractéristique sous Windows et grâce à un onglet dédié «chiffrement» dans les propriétés d'un dossier.

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

2.4.1.3 Fichiers effacés

Que les fichiers soient stockés ou non dans des zones chiffrées, ZoneCentral procède à une surcharge de leur contenu dès lors que ces fichiers sont supprimés, quelle que soit la façon dont ils sont supprimés (action utilisateur ou par programme), ou lorsqu'ils sont redimensionnés (réduction de taille : le résidu est également surchargé avant la réduction).

Note 1 : le fait que les fichiers chiffrés [figurant dans une zone chiffrée] soient traités par surcharge est un paramètre de configuration générale du produit (policy).

Note 2 : ce service d'effacement par surcharge peut être désactivé par un paramètre de configuration générale du produit (policy).

Les fichiers ainsi traités ne sont pas des biens sensibles de l'utilisateur au sens de la TOE pendant leur durée de vie, mais le deviennent dès lors qu'ils font l'objet d'une suppression (fin de vie).

2.4.1.4 Les fichiers d'échange (swap) du système

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

Note : ce service peut être désactivé par un paramètre de configuration générale du produit (policy). De plus, il ne peut être opérationnel que si le volume (C :, D :, etc.) supportant le fichier swap n'est pas exclus de la liste des volumes gérés par ZoneCentral (une policy permet en effet d'exclure des volumes, pour des cas hypothétiques de non-compatibilité).

2.4.2. Biens sensibles de la TOE

2.4.2.1 Les programmes

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

2.4.2.2 La configuration

Pour assurer son fonctionnement, la TOE met en œuvre des politiques (au sens Windows du terme). La sécurité en intégrité de ces politiques est assurée par l'environnement (i.e. le système des politiques 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).

2.4.2.3 Les fichiers de fonctionnement

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

Ils contiennent le libellé de la zone, un identifiant unique, les exceptions applicables à la zone, quelques informations de gestion, et les 'wrappings' d'accès, c'est-à-dire les clés de chiffrement de la zone chiffrées par les clés d'accès des utilisateurs habilités à la zone.

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

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

Chacun de ces fichiers contient une clé RSA, appelée 'clé indirecte d'accès', dédiée au fichier et générée par le produit, chiffrée autant de fois que nécessaire par les différentes clés d'accès des utilisateurs de la liste.

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

2.4.2.4 Remarques

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

Par ailleurs, ZoneCentral n'utilise aucun fichier temporaire en mode de fonctionnement 'utilisateur'. Ce n'est que lorsqu'une opération d'administration de zone est exécutée (création d'une zone chiffrée avec chiffrement initial des fichiers qu'elle contient) que ZoneCentral met en œuvre des fichiers temporaires pour assurer la fiabilité de l'opération (points de reprise sur coupure de courant). Ces fichiers sont situés dans les zones elles-mêmes et sont effacés par surcharge en fin de traitement.

Les «logs» de ZoneCentral ne sont pas considérés comme des biens sensibles de la TOE. Ces logs sont constitués d'«événements» émis dans l'Observateur d'Événements Windows, et, pour certaines opérations d'administration de fichiers logs de déroulement pour analyse en cas de problème technique. Leur rôle est de constituer un «soutien» logistique, mais ils ne sont pas exploités par ZoneCentral.

2.4.3. Synthèse des biens sensibles

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

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

Biens sensibles	Confidentialité	Intégrité
<i>Biens sensibles de l'utilisateur</i>		
Eléments des clés d'accès manipulés par ZoneCentral, 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 ZoneCentral	Forte	Forte
Fichiers et dossiers de l'utilisateur stockés dans des zones chiffrées	Forte	N/A
Fichiers utilisateurs supprimés (pour une confidentialité post-mortem)	Forte	N/A
Fichiers d'échange (SWAP)	Forte	N/A
<i>Biens sensibles de la TOE</i>		
Fichiers de contrôle des « zones » dont : les clés de chiffrement de zones	Faible Forte	Forte
Fichiers d'accès dont : les clés indirectes des fichiers d'accès	Faible Forte	Forte
Configuration de ZoneCentral (policies)	Faible	Forte
Programmes de ZoneCentral	Faible	Forte

Tableau 1 : Synthèse des biens sensibles

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

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



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

3. Environnement de sécurité de la TOE

3.1. Hypothèses

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

- H.NON_OBSERV** L'environnement physique de la TOE permet aux utilisateurs d'entrer leur mot de passe (ou code PIN) sans être observable directement et sans que cela puisse être intercepté (clavier sans fil...) par d'autres utilisateurs ou attaquants potentiels.
- Des mesures organisationnelles adaptées doivent permettre à l'administrateur d'authentifier l'utilisateur distant avant toute transmission du mot de passe de secours.
- H.ENV_OPERATIONNEL** L'environnement opérationnel ne permet pas à un attaquant d'accéder au disque lorsque des données sensibles sont accessibles à un utilisateur légitime sur l'équipement.
- H.CONFIANCE_ADM_TOE** Les administrateurs de la TOE sont des personnes de confiance et sont formés à l'utilisation de la TOE.
- 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 de ses clés.
- 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.ADMIN_WINDOWS** Les administrateurs Windows de plus haut niveau du domaine Windows sont chargés d'interdire aux administrateurs Windows des sous-niveaux (domaines, contrôleurs de domaines, postes de travail) la modification des « politiques » de la TOE. De même, les administrateurs de la TOE ne doivent pas pouvoir modifier les « politiques ».

H.INSTALLATION

L'administrateur de la TOE est chargé d'installer la TOE conformément à son manuel d'installation et de vérifier périodiquement son intégrité (signature authenticode dans les propriétés de l'exécutable).

H.CRYPTO_EXT

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

3.2. 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'attaquant considéré est doté d'un potentiel d'attaque élémentaire (« low » au sens des Critères Communs)..

M.DETOURN_COMPOSANT

Un attaquant met en œuvre, éventuellement à bas niveau, les composants internes de la TOE, pour contourner certaines fonctions de sécurité. Il peut pour cela effectuer du «reverse-ingeniering» sur les programmes, développer des programmes d'appel des fonctions internes de la TOE, ou s'aider d'un debugger. Un bon exemple est le contournement d'une règle de sécurité qui aurait été implémentée dans une IHM et non pas de façon plus interne dans le produit.

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

M.ATTAQUE_FIC_INTERNES

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

Par exemple, il copie les fichiers chiffrés d'une zone, avec les fichiers internes de la TOE et tente à partir de ces éléments de retrouver des informations protégées.

M.MODIF_FIC_INTERNES

Un attaquant modifie les fichiers internes de la TOE pour tenter de retrouver des informations protégées.

3.3. Politiques de sécurité de l'organisation

P.ZONE

La TOE doit offrir un service de protection en confidentialité (chiffrement), automatique et systématique, du stockage des fichiers sensibles des

utilisateurs, ces fichiers ne pouvant être lus (déchiffrés) ou écrits (chiffrés) que par des utilisateurs disposant de clés d'accès valides pour ces fichiers.

Ce service doit opérer sur les volumes de données locaux (disques et partitions), amovibles, et réseau, dès lors que le support est compatible techniquement avec la TOE.

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.

P.ACCE

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

P.ADMIN_ZONES

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

P.ADMIN_ACCES

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

P.EFF_FICHIERS

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

P.SWAP

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

P.CRYPTO

Les mécanismes cryptographiques de la TOE doivent être conformes aux exigences du référentiel cryptographique de la DCSSI pour le niveau de robustesse standard ([CRYPTO_STD]).

4. Objectifs de sécurité

4.1. Objectifs de sécurité pour la TOE

4.1.1. Contrôle d'accès

O.ACCES

La TOE ne doit autoriser l'accès à une zone chiffrée qu'après présentation d'une clé d'accès valide pour la zone.

De plus, la TOE doit permettre de chiffrer conformément à [CRYPTO_STD] les éléments sensibles de ses fichiers de fonctionnement internes (liés à la zone) par les clés d'accès des utilisateurs autorisés.

O.AUTH

La TOE doit permettre d'identifier et authentifier tout utilisateur.

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, plus possibilité d'administrer la zone chiffrée, c'est-à-dire gérer ses accès, la déchiffrer complètement).

Le «pouvoir» d'un utilisateur doté du rôle «administrateur» sur une zone chiffrée peut être restreint globalement par les politiques, qui peuvent lui interdire certaines actions (globalement, toutes zones confondues).

4.1.2. Cryptographie

O.CHIFFREMENT

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

O.ALGO_STD

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

O.CLES_TOKEN

La TOE doit permettre l'emploi de clés d'accès contenues dans un porte-clés comme une carte à puce ou une clé USB. L'utilisation de ces clés d'accès doit être conditionnée par la présentation à la TOE du porte-clés et du code PIN associé.

O.CLES_P12

La TOE doit permettre l'emploi de clés d'accès contenues

dans un fichier au format PKCS#12. L'utilisation de ces clés d'accès doit être conditionnée par la présentation à la TOE du fichier PKCS#12 et du code secret associé.

O.CLES_PWD

La TOE doit permettre l'emploi de clés d'accès obtenues par diversification d'un mot de passe saisi au clavier.

O.ALEAS

La TOE doit implémenter un mécanisme de génération de pseudo-aléas ou d'aléas vrais avec suffisamment d'entropie pour assurer la production d'aléas non prédictibles.

4.1.3. Gestion des zones

O.GEST_SECRETS

La TOE doit utiliser des clés différentes pour protéger les différentes «zones» configurées, même si les utilisateurs sont les mêmes pour ces « zones ».

O.ADM_ZONES

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

O.ADM_ACCES

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

4.1.4. Effacement

O.EFF_RESIDUS

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

O.EFF_FICHIERS

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

4.1.5. Protections lors de l'exécution

O.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. Installation

OE.SOFT_SIGNE

Les composants de la TOE doivent être signés et horodatés par le fournisseur de la TOE pour permettre aux administrateurs de la TOE de vérifier son intégrité.

OE.INSTALLATION

L'installation de la TOE doit être effectuée conformément à son manuel d'installation et son intégrité doit être périodiquement vérifiée.

4.2.2. Utilisation

OE.NON_OBSERV

L'environnement physique d'utilisation de la TOE doit permettre aux utilisateurs et aux administrateurs d'entrer leur mot de passe (ou code PIN) sans être observables directement ou sans que la saisie soit interceptable (clavier sans fil,...) par d'autres utilisateurs ou attaquants potentiels.

Des mesures organisationnelles adaptées doivent permettre à l'administrateur d'authentifier l'utilisateur distant avant toute transmission du mot de passe de secours.

OE.ENV_OPERATIONNEL

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

Note d'application :

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

Les applications installées sur l'équipement ne doivent pas perturber le bon fonctionnement de la TOE. Ainsi, les opérations que peut faire l'utilisateur sur les fichiers protégés par la TOE, surtout au travers de ses applications, ne doivent pas entraîner de copies totales ou partielles de ces fichiers en dehors de la TOE, sauf lorsqu'il l'a clairement demandé ou lorsque c'est une conséquence claire de l'opération demandée.

OE.SO_CONF

Les administrateurs de la TOE doivent être des personnes de confiance.

OE.CONSERV_CLES

Les utilisateurs doivent conserver, dans un lieu sûr, les clés d'accès qui leur ont été transmises par un administrateur de la TOE et empêcher leur divulgation. L'administrateur de la TOE doit conserver ses clés dans un lieu sûr et empêcher leur divulgation.

4.2.3. Formation des utilisateurs

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). Les administrateurs de la TOE doivent recevoir une formation adaptée à cette fonction.

OE.CRYPTO_EXT

Les administrateurs de la TOE doivent être sensibilisés sur la qualité des clés d'accès qu'ils apportent à la TOE afin que ces clés soient conformes à l'état de l'art dans leur implémentation. Ils doivent également être sensibilisés à la qualité du support de ces clés lorsqu'elles sont hébergées par un porte-clés externe.

4.2.4. Administration

OE.CERTIFICATS

L'administrateur de la TOE doit, lors de la fourniture des clés d'accès possédant un certificat X509, vérifier la validité de ces certificats et leur adéquation avec l'usage qui en est fait par la TOE. Cette exigence s'applique en particulier aux certificats racines dits «authenticode» à partir desquels la vérification d'intégrité de la TOE peut être effectuée.

OE.ADM_ROOT_WINDOWS

Les administrateurs de plus haut niveau du domaine Windows doivent interdire aux administrateurs des sous-niveaux (domaines, contrôleurs de domaines, postes de travail) la modification des « polices » de la TOE. De même, les administrateurs de la TOE ne peuvent modifier les « polices ». En conséquence, ces administrateurs de plus haut niveau doivent eux-

OE.ADM_DELEGATION

mêmes être des personnes de confiance.

Quand, pour des raisons pratiques de logistique ou de schéma d'organisation, des fonctions d'administration de la TOE sont déléguées à des utilisateurs particuliers, ces utilisateurs doivent recevoir une formation particulière à ce rôle, et seules les fonctions réellement nécessaires doivent être déléguées.

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, au chapitre 9.1.

5.1.1. Exigences fonctionnelles de sécurité de la TOE

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

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

Tableau 2 : Exigences fonctionnelles de sécurité pour la TOE

5.1.1.1 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	<p>La TSF doit pouvoir générer un enregistrement d'audit des événements auditable suivants :</p> <p>a) démarrage et arrêt des fonctions d'audit ;</p> <p>b) tous les événements auditable pour le niveau d'audit <i>minimum</i> ;</p> <p>c) et :</p> <ul style="list-style-type: none"> - Événements journalisés au titre de la gestion des zones (<i>chiffrement, déchiffrement, détachement, regroupement, création de zone en clair</i>) ; - Événements journalisés au titre de la gestion des accès aux zones (<i>modification ou ajout d'accès sur une zone</i>) ; - Événements journalisés au titre de la gestion des exceptions (<i>création ou suppression de profil d'exception de fichier dans une zone</i>) ; - Événements journalisés au titre de l'utilisation des zones (<i>ouverture ou fermeture d'une zone</i>) ;
FAU_GEN.1.2	<p>La TSF doit enregistrer au minimum les informations suivantes dans chaque enregistrement d'audit :</p> <p>a) date et heure de l'événement, type d'événement, identité du sujet, ainsi que le résultat (succès ou échec) de l'événement ;</p> <p>b) et, pour chaque type d'événement d'audit, sur la base des définitions d'événements auditable contenues dans les composants fonctionnels inclus dans la ST, <i>l'identifiant de l'administrateur</i>.</p>
FAU_GEN.2	Lien entre l'identité de l'utilisateur
FAU_GEN.2.1	La TSF doit pouvoir associer chaque événement auditable avec l'identité de l'utilisateur qui est à l'origine de l'événement.

5.1.1.2 Classe FCS : Support Cryptographique

FCS_CKM	Gestion des clés cryptographiques
FCS_CKM.1	Génération des clés cryptographiques
FCS_CKM.1.1	<p>La TSF doit générer les clés cryptographiques conformément à un algorithme de génération de clés cryptographiques spécifié parmi les suivants <i>génération de nombres pseudo-aléatoires, génération d'exposants Diffie-Hellman et diversification de clés</i> et à des tailles de clés cryptographiques <i>de 128 à 256 bits pour les clés symétriques et de 1024 à 2048 bits pour les clés asymétriques</i> qui satisfont aux standards <i>PKCS #1 v1.5 et PKCS#5 v2.0</i>.</p>

FCS_CKM.3	Accès aux clés cryptographiques
FCS_CKM.3.1	La TSF doit réaliser <i>l'utilisation de clés</i> conformément à une méthode d'accès aux clés cryptographiques spécifiée <i>par déchiffrement (déwrapping) des clés par la clé d'accès</i> .
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 <i>par réécriture de motifs aléatoires</i> .
FCS_COP	Opération cryptographique
FCS_COP.1	Opération cryptographique
FCS_COP.1.1	La TSF doit exécuter le <i>hashage, le chiffrement, le déchiffrement, la génération de clés, le wrapping de clés et la dérivation de clés</i> conformément à un algorithme cryptographique spécifié <i>SHA-1, RSA, 3DES et AES</i> et avec des tailles de clés cryptographiques de <i>128 à 256 bits pour les clés symétriques et de 1024 à 2048 bits pour les clés asymétriques</i> qui satisfont à ce qui suit: <i>RFC 3174 (SHA-1), ANSI X9.52-1998 (3DES), FIPS 197 (AES) et PKCS#1 (RSA)</i> .

5.1.1.3 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 <i>SFP.ACCESS_OBJ</i> aux <i>utilisateurs de la TOE, aux fichiers protégés par la TOE dans une « zone » et aux opérations dans les « zones »</i> .
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 <i>SFP.ACCESS_OBJ</i> aux objets en fonction des <i>identifiants de la « zone » contenant le fichier</i> .
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 : <i>présentation de la clé d'accès associée à la « zone » concernée</i> .
FDP_ACF.1.3	La TSF doit autoriser explicitement l'accès de sujets à des objets en fonction des règles complémentaires suivantes : <i>Aucune</i> .
FDP_ACF.1.4	La TSF doit refuser explicitement l'accès de sujets à des objets en fonction de : <i>Aucune</i> .

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 <i>les politiques de sécurité des fonctions (SFP) SFP.ACCESS_OBJ et SFP.ACCESS_ROLES</i> lors de l'importation de données utilisateur, contrôlées par les SFP, en provenance de l'extérieur du TSC.
FDP_ITC.1.2	La TSF doit ignorer tout attribut de sécurité associé aux données utilisateur lorsqu'elles sont importées depuis l'extérieur du TSC.
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 du TSC : <i>Aucune</i>

FDP_RIP	Protection des informations résiduelles
FDP_RIP.2	Protection totale des informations résiduelles
FDP_RIP.2.1	La TSF doit garantir que toute information contenue précédemment dans une ressource est rendue inaccessible lors de <i>la désallocation de la ressource</i> de tous les objets.

5.1.1.4 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 <i>trois</i> tentatives d'authentification infructueuse ont eu lieu en relation avec <i>l'ouverture d'une « zone »</i> . <u>Note</u> : 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 <i>temporiser l'accès à cette « zone »</i> .

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.

5.1.1.5 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, désactiver, activer ou modifier le comportement* des fonctions de chiffrement des « zones » aux administrateurs de la TOE.

FMT_MSA Administration des attributs de sécurité

FMT_MSA.1 Gestion des attributs de sécurité

FMT_MSA.1.1 La TSF doit mettre en œuvre la *politique SFP.ACCESS_ROLES* pour restreindre aux *administrateurs de la TOE* la possibilité de *changer la valeur par défaut, interroger, modifier ou supprimer* les attributs de sécurité *identifiants de « zone » et rôles*.

FMT_MSA.2 Attributs de sécurité sûrs

FMT_MSA.2.1 La TSF doit garantir que seules des valeurs sûres sont acceptées pour les attributs de sécurité.

FMT_MSA.3 Initialisation statique d'attribut

FMT_MSA.3.1 La TSF doit mettre en œuvre la *politique SFP.ACCESS_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 aux administrateurs de la TOE de spécifier des valeurs initiales alternatives pour remplacer les valeurs par défaut lorsqu'un objet ou une information est créé.

FMT_MTD Gestion des données de la TSF

FMT_MTD.1 Gestion des données de la TSF

FMT_MTD.1.1 La TSF doit restreindre, aux administrateurs de la TOE, la possibilité de *changer la valeur par défaut, interroger, modifier ou supprimer* les stratégies de sécurité.

FMT_SMF Spécification des fonctions d'administration

FMT_SMF.1 Spécification des fonctions d'administration

FMT_SMF.1.1 La TSF doit être capable d'exécuter les fonctions d'administration de la sécurité suivantes :

- *Les fonctions de contrôle d'accès aux opérations d'administration de la sécurité*
 - *Les fonctions de gestion des clés et mots de passe*
 - *Les fonctions de gestion des zones*
 - *Les fonctions d'initialisation des paramètres utilisés par les fonctions de sécurité*
-

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

5.1.1.6 Classe FPT : Protection des fonctions de sécurité de la TOE

FPT_SEP **Séparation de domaines**

FPT_SEP.1 Séparation de domaines pour la TSF

FPT_SEP.1.1 La TSF doit maintenir un domaine de sécurité pour sa propre exécution, qui la protège des interférences et des intrusions par des sujets non sûrs.

FPT_SEP.1.2 La TSF doit appliquer une séparation entre les domaines de sécurité de sujets dans le TSC.

5.1.1.7 Classe FTA : Accès à la TOE

FTA_SSL **Verrouillage de session**

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

FTA_SSL.3.1 La TSF doit clôturer une session interactive *après un délais de 5 secondes d'inactivité de l'utilisateur, comptées à partir du lancement de l'économiseur d'écran Windows*.

5.1.1.8 Classe FTP : Chemins et canaux de confiance

FTP_TRP **Chemin de confiance**

FTP_TRP.1 Chemin de confiance

FTP_TRP.1.1 La TSF doit fournir un chemin de communication entre elle-même et des utilisateurs *locaux* qui soit logiquement distinct des autres chemins de communication et qui garantisse l'identification de ses extrémités et la protection des données transférées contre une modification ou une divulgation.

FTP_TRP.1.2 La TSF doit permettre à *la TSF et aux utilisateurs locaux* d'initier une communication via le chemin de confiance.

FTP_TRP.1.3 La TSF doit exiger l'utilisation du chemin de confiance pour :

- récupérer des clés d'accès localisés dans un « token » ou une carte à puce via l'API PKCS#11 ;
- récupérer des clés d'accès localisés dans un fichier sécurisé au format PKCS#12 ;

5.1.2. Niveau de résistance des exigences fonctionnelles

Le niveau minimal exigé de résistance des exigences fonctionnelles de sécurité FIA_UAU.2 et FIA_UID.2 est « élevé » (SOF-high).

5.1.3. Exigences d'assurance de sécurité de la TOE

Comme indiqué au paragraphe 3.2, la TOE doit être résistante aux attaques de pénétration effectuées par un attaquant ayant un potentiel d'attaque élémentaire.

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

EAL2 augmenté de ALC_FLR.3, AVA_VLA.2, ADV_HLD.2, AVA_MSU.1 et ALC_DVS.1, ainsi que ADV_LLD.1, ALC_TAT.1 et ADV_IMP.1 pour les mécanismes cryptographiques (FCS) avec une résistance SOF-High

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

Composant		Commentaire
ACM_CAP.2	Éléments de configuration	EAL2
ADO_DEL.1	Procédures de livraison	EAL2
ADO_IGS.1	Procédures d'installation, de génération et de démarrage	EAL2
ADV_FSP.1	Spécifications fonctionnelles informelles	EAL2
ADV_HLD.2	Conception de haut niveau de sécurité	+
ADV_IMP.1	Sous-ensemble de l'implémentation de la TSF	+ (FCS)
ADV_LLD.1	Conception de bas niveau descriptive	+ (FCS)
ADV_RCR.1	Démonstration de correspondance informelle	EAL2
AGD_ADM.1	Guide de l'administrateur	EAL2
AGD_USR.1	Guide de l'utilisateur	EAL2
ALC_DVS.1	Identification des mesures de sécurité	+
ALC_FLR.3	Correction d'anomalies systématique	+
ALC_TAT.1	Outils de développement bien définis	+ (FCS)
ATE_COV.1	Éléments de preuve de la couverture	EAL2
ATE_FUN.1	Tests fonctionnels	EAL2
ATE_IND.2	Tests indépendants - par échantillonnage	EAL2
AVA_MSU.1	Examen des guides	+
AVA_SOF.1	Evaluation de la résistance des fonctions de sécurité de la TOE	EAL2
AVA_VLA.2	Analyse de vulnérabilités indépendante	+

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.

Cette section présente les raffinements (notés en **gras**) effectués sur les exigences d'assurance suivantes : ADV_IMP.1, ADV_LLD.1 et ALC_TAT.1.

Pour une meilleure compréhension, les exigences ont été traduites.

Le texte officiel de ces exigences figure dans l'annexe A, chapitre 9.2 de ce présent document.

5.1.3.1 Classe ADV: Développement

ADV_IMP.1 Sous-ensemble de l'implémentation de la TSF

Tâches du développeur :

ADV_IMP.1.1D Le développeur doit fournir la représentation de l'implémentation **des fonctions cryptographiques**.

Contenu et présentation des éléments de preuve :

ADV_IMP.1.1C La représentation de l'implémentation **des fonctions cryptographiques** doit définir **les fonctions cryptographiques** d'une façon non ambiguë avec un niveau de détail suffisant pour qu'elle puisse être générée sans décision de conception supplémentaire.

ADV_IMP.1.2C La représentation de l'implémentation **des fonctions cryptographiques** doit avoir une cohérence interne.

Tâches de l'évaluateur :

ADV_IMP.1.1E L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

ADV_IMP.1.2E L'évaluateur doit déterminer que le plus bas niveau de représentation **des fonctions cryptographiques** fourni est une instanciation correcte et complète des exigences fonctionnelles de sécurité **de la classe FCS** pour la TOE.

ADV_LLD.1 Conception de bas niveau descriptive

Tâches du développeur :

ADV_LLD.1.1D Le développeur doit fournir la conception de bas niveau **des fonctions cryptographiques**

Contenu et présentation des éléments de preuve :

ADV_LLD.1.1C La présentation de la conception de bas niveau **des fonctions cryptographiques** doit être en style informel.

- ADV_LLD.1.2C La conception de bas niveau **des fonctions cryptographiques** doit avoir une cohérence interne.
- ADV_LLD.1.3C La conception de bas niveau **des fonctions cryptographiques** doit décrire **les fonctions cryptographiques** en termes de modules **cryptographiques**.
- ADV_LLD.1.4C La conception de bas niveau **des fonctions cryptographiques** doit décrire le but de chaque module **cryptographique**.
- ADV_LLD.1.5C La conception de bas niveau **des fonctions cryptographiques** doit définir les relations mutuelles entre les modules **cryptographiques** en termes de fonctionnalités de sécurité fournies et de dépendances vis-à-vis des autres modules **cryptographiques**.
- ADV_LLD.1.6C La conception de bas niveau **des fonctions cryptographiques** doit décrire comment chaque **fonction cryptographique** est fournie.
- ADV_LLD.1.7C La conception de bas niveau **des fonctions cryptographiques** doit identifier toutes les interfaces des modules **cryptographiques**.
- ADV_LLD.1.8C La conception de bas niveau **des fonctions cryptographiques** doit identifier les interfaces des modules **cryptographiques** qui sont visibles de l'extérieur.
- ADV_LLD.1.9C La conception de bas niveau **des fonctions cryptographiques** doit décrire le but et le mode d'utilisation de toutes les interfaces des modules **cryptographiques**, en fournissant, lorsque cela est approprié, les détails sur les effets, les exceptions et les messages d'erreur.
- ADV_LLD.1.10C La conception de bas niveau **des fonctions cryptographiques de soutien** doit décrire la séparation de la TOE en **modules cryptographiques** et en autres modules.

Tâches de l'évaluateur :

- ADV_LLD.1.1E L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.
- ADV_LLD.1.1E L'évaluateur doit déterminer que la conception de bas niveau **des fonctions cryptographiques** est une instantiation correcte et complète des exigences fonctionnelles de sécurité **de la classe FCS** pour la TOE.

5.1.3.2 Classe ALC : Support au cycle de vie

ALC_TAT.1 Outils de développement bien définis

Tâches du développeur :

- ALC_TAT.1.1D Le développeur doit identifier les outils de développement utilisés pour **les fonctions cryptographiques** de la TOE.
- ALC_TAT.1.2D Le développeur doit documenter les options dépendant de l'implémentation qui ont été choisies pour les outils de développement **des fonctions cryptographiques**.

Contenu et présentation des éléments de preuve :

- ALC_TAT.1.1C Tous les outils de développement utilisés pour l'implémentation **des fonctions cryptographiques** doivent être bien définis.
- ALC_TAT.1.2C La documentation relative aux outils de développement **des fonctions cryptographiques** doit définir sans ambiguïté la signification de toutes les instructions utilisées dans l'implémentation **des fonctions cryptographiques**.
- ALC_TAT.1.3C La documentation relative aux outils de développement **des fonctions cryptographiques** doit définir sans ambiguïté la signification de toutes les options dépendant de l'implémentation.

Tâches de l'évaluateur :

- ALC_TAT.1.1E L'évaluateur doit confirmer que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve.

5.2. Exigences de sécurité sur la partie TI de l'environnement

Note : dans le cadre des exigences fonctionnelles de sécurité pour la partie TI de l'environnement, le terme « TSF » doit être interprété comme « l'environnement de la TOE ».

5.2.1. Système d'horodatage fiable

FPT_STM Time stamps

FPT_STM.1/ENV Reliable time stamps

FPT_STM.1.1/ENV The TSF shall be able to provide reliable time stamps for its own use.

Note d'application : l'environnement de la TOE doit fournir un système d'horodatage fiable qui permet à la TOE de dater les événements enregistrés dans le journal d'audit.

5.2.2. Signature des composants de la TOE

FCO_NRO Non-repudiation of origin

FCO_NRO.1/ENV Selective proof of origin

FCO_NRO.1.1/ENV The TSF shall be able to generate evidence of origin for transmitted **[TOE Components]** at the request of the **[administrateur]**.

FCO_NRO.1.2/ENV The TSF shall be able to relate the **[identité et la date]** of the originator of the information, and the **[clé certifiée Thawte de type Authenticode]** of the information to which the evidence applies.

FCO_NRO.1.3/ENV The TSF shall provide a capability to verify the evidence of origin of information to **[administrateur]** given **[validité de la clé certifiée Thawte de type Authenticode]**.

Note d'application : l'environnement de la TOE fournit un système de signature des composants de la TOE qui permet à un administrateur de vérifier leur intégrité.

6. Spécifications globales de la TOE

6.1. Fonctions de sécurité de la TOE

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

Note : certaines fonctions d'administration peuvent être déléguées à certains utilisateurs, par configuration.

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

Cette fonction de sécurité couvre l'ensemble des opérations de configuration de la TOE (et assure que seules des valeurs sûres de paramètres de configuration peuvent être utilisées). La TOE ne peut pas fonctionner sans être configurée. Les données de configuration concernent ici les «*«* polices *»* de Windows exploitées par la TOE ;

F.GESTION_OP_ZONE **Gestion des zones**

Cette fonction de sécurité constitue le point d'entrée des opérations sur les zones (déchiffrement, reprise en cas de problème, affichage des informations de zone). Elle assure également le nettoyage des traces de données sensibles (fichiers utilisateurs ou clés d'accès) dans la mémoire (RAM) ou sur le disque dur (fichier SWAP ou temporaire), dès la fin des opérations réalisées.

F.OPERATIONS_CRYPTO **Implémentation des opérations cryptographiques**

Cette fonction de sécurité couvre l'ensemble des opérations cryptographiques mises au service des autres fonctions de sécurité et assure que ces opérations sont réalisées en utilisant des zones mémoires dédiées.

F.GESTION_CLES **Gestion des clés**

Cette fonction de sécurité réalise les opérations de création, de suppression des clés de zone ainsi que les opérations d'accès à ces clés.

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).

F.GESTION_DROITS **Gestion des droits**

Cette fonction de sécurité gère les utilisateurs et les droits 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.

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

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

F.CONFIGURE_ZONE

Configuration des zones

Cette fonction de sécurité couvre les opérations de configuration des descripteurs de zone. Elle réalise le chiffrement initial de la zone. Elle assure également que les données de configurations utilisées ne peuvent prendre que des valeurs sûres.

F.AUDIT

Audit

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

6.2. Niveau de résistance des fonctions

Le niveau minimal exigé de résistance des fonctions de sécurité de la TOE est « élevé » (SOF-high). Ceci concerne 2 fonctions de sécurité de la TOE qui implémentent des mécanismes de sécurité non cryptographiques et de nature combinatoire ou permutationnelle basés sur des mots de passe:

- La fonction F.GESTION_CLES qui assure la protection de l'accès aux clés de zone est SOF-high. Cet accès aux clés requiert l'entrée d'une clé (RSA) ou d'un mot de passe fort.
- La fonction F.CONTROLE_ACCES_ZONE qui assure le contrôle d'accès utilisateur aux zones est SOF-high. L'accès aux zones protégées requiert l'entrée d'une clé (RSA) ou d'un mot de passe fort.

Le tableau suivant réprécise les mécanismes de sécurité non cryptographiques de nature combinatoire ou permutationnelle qui sont impliqués dans la mise en œuvre des fonctions de sécurité.

Mécanismes de sécurité non cryptographiques	F.CONFIGURATION_TOE	F.GESTION_OP_ZONE	F.OPERATIONS_CRYPTO	F.GESTION_CLES	F.ENTREE_SECURISEE	F.GESTION_DROITS	F.CONTROLE_ACCES_ZONE	F.CONFIGURE_ZONE	F.AUDIT
Evaluation des mots de passe				X			X		

Tableau 4 : Mécanismes de sécurité non cryptographiques

6.3. Mesures d'assurance

Cette section décrit les mesures d'assurance qui sont mises en œuvre afin de satisfaire aux exigences d'assurance visées par l'évaluation de la TOE.

6.3.1. Mesures de l'environnement de développement

6.3.1.1 MA.ENV_CONF : Méthodes et outils de gestion de configuration

Le système de gestion de configuration couvre la gestion et le contrôle du développement, de la production et de la maintenance du logiciel ZoneCentral. Son application permet d'affecter un identifiant unique à chaque version de la TOE et d'établir une liste des versions des composants qui constituent une version donnée.

Les procédures du système de gestion de configuration sont documentées et fournissent une liste de configuration pour la TOE.

Références des fournitures :

- PRIMX ZoneCentral 3.1 ZEBRA2 ACM (PX81121) v1r1
- PRIMX-ZoneCentral 3.1 Infrastructure de Développement (PX82131) v1r2
- PRIMX-Gestion des documents (PX82127) v1r1
- PRIMX-ZoneCentral 3.1 Liste de configuration (PX81112) v1r4

Argumentaire : ces procédures satisfont de manière directe à l'exigence ACM_CAP.2.

6.3.1.2 MA.ENV_SEC : Sécurité de l'environnement de développement

Les mesures de sécurité appliquées pour le développement et la maintenance du logiciel ZoneCentral garantissent l'intégrité du code exécutable de la TOE et la confidentialité des documents de développement associés.

Les mesures de sécurité de l'environnement de développement sont documentées, elles identifient précisément le périmètre de cet environnement et fournissent des traces de l'application de ces mesures.

Références des fournitures :

- PRIMX ZoneCentral 3.1 ZEBRA2 ALC (PX81123) v1r1
- PRIMX-Sécurité Développements (PX82129) v1r2

Argumentaire : ces procédures satisfont de manière directe à l'exigence ALC_DVS.1.

6.3.1.3 MA.ENV_LIV : Procédures de livraison

Les procédures et mesures mises en place pour transférer le logiciel ZoneCentral du développeur chez l'utilisateur final garantissent l'authenticité et l'intégrité de la TOE lors du transfert.

Les procédures de livraison sont documentées.

Références des fournitures :

- PRIMX ZoneCentral 3.1 ZEBRA2 ADO (PX81122) v1r1

- PRIMX-ZoneCentral 3.1 Infrastructure de Développement (PX82131) v1r2
- PRIMX-Génération de versions (PX82128) v1r1
- PRIMX-Emission d'une version (PX82126) v1r2

Argumentaire : ces procédures satisfont de manière directe à l'exigence ADO_DEL.1.

6.3.1.4 MA.ENV_SUP : Procédures de correction des anomalies

Des procédures de correction des anomalies sont mises en place au niveau du laboratoire et du service support pour assurer une gestion et un contrôle des anomalies de sécurité découvertes en interne ou soumises par les exploitants, ainsi que la distribution des correctifs associés, une fois les anomalies résolues.

Les procédures visant à la correction des anomalies sont documentées, et les documents donnant des lignes directrices aux exploitants pour soumettre les anomalies sont fournis.

Références des fournitures :

- PRIMX ZoneCentral 3.1 ZEBRA2 ALC (PX81123) v1r1
- PRIMX-Support & Corrections (PX82130) v1r2

Argumentaire : ces procédures satisfont de manière directe à l'exigence ALC_FLR.3.

6.3.2. MA.DEV : Documentation et outils de développement des fonctions de sécurité

Les documents permettant d'assurer un niveau de qualité compatible avec les exigences liées au paquet d'assurance sécurité sont fournis : spécifications fonctionnelles, conception de haut niveau et, uniquement pour les fonctions cryptographiques, conception de bas niveau, documentation des outils et techniques de développement (compilateurs, makefiles, ...) et code source. Ces documents forment les niveaux successifs de représentation de la fonctionnalité de sécurité.

Des correspondances entre ces niveaux sont établies, en commençant par les fonctions de sécurité des TI spécifiées de manière abrégée dans ce document.

Références des fournitures :

- PRIMX-ZoneCentral 3.1 Spécifications fonctionnelles (PX81115) v1r3
- PRIMX-ZoneCentral 3.1 Conception de haut niveau (PX81116) v1r3
- PRIMX-ZoneCentral 3.1 Conception de bas niveau (PX81117) v1r5
- PRIMX ZoneCentral 3.1 ZEBRA2 ALC (PX81123) v1r1
- PRIMX-ZoneCentral 3.1 Infrastructure de Développement (PX82131) v1r2

Argumentaire : ces mesures satisfont de manière directe aux exigences ADV_FSP.1, ADV_HLD.2, ADV_LLD.1, ALC_TAT.1, ADV_IMP.1 et ADV_RCR.1.

6.3.3. Test des fonctions de sécurité

6.3.3.1 MA.TEST_DEV : Procédure de test du développeur

Les documents produits à l'occasion des tests effectués sur la TOE sont fournis. Ces documents doivent décrire le plan et les procédures de tests suivies et montrer le degré de couverture des spécifications fonctionnelles par les tests. Ils doivent inclure les résultats effectifs des tests et démontrer que les fonctions de sécurité se comportent bien de la manière spécifiée dans les spécifications fonctionnelles.

Une TOE se prêtant au repassage des tests effectués est mise à disposition de l'évaluateur.

Références des fournitures :

- PRIMX-ZoneCentral 3.1 documentation de test (PX81120) v1r1

Argumentaire : ces procédures satisfont de manière directe aux exigences ATE_FUN.1, ATE_COV.1 et à une partie d'ATE_IND.2 (repassage des tests).

6.3.3.2 MA.TEST_EVAL : Test indépendant

Le commanditaire met à disposition de l'évaluateur une TOE se prêtant à l'exécution de tests indépendants.

Références des fournitures : sans objet.

Argumentaire : ces mesures satisfont de manière directe à l'exigence ATE_IND.2 (test indépendant).

6.3.4. Documentation d'exploitation

6.3.4.1 MA.GUIDE_INST : Procédures d'installation et de démarrage

Ces procédures permettent l'installation et le démarrage de la TOE dans des conditions qui garantissent une exécution satisfaisante de ses fonctions de sécurité.

Afin de prévenir les risques d'utilisation impropre, la documentation d'installation et de démarrage doit spécifiquement identifier tous les modes d'exécution possibles de la TOE ainsi que leur impact sur la sécurité. Elle doit être claire, complète, cohérente, et accessible à l'audience visée. Elle doit enfin énumérer toutes les hypothèses relatives à l'environnement d'exploitation prévu et les exigences sur les mesures de sécurité (TI ou non-TI) qui doivent être présentes dans l'environnement.

Les procédures d'installation et de démarrage sûrs de la TOE sont documentées.

Références des fournitures :

- PRIMX ZoneCentral 3.1 ZEBRA2 ADO (PX81122) v1r1
- ZoneCentral 3.1 Manuel Technique FR (PX81098) r5

Argumentaire : ces procédures satisfont de manière directe aux exigences ADO_IGS.1 et AVA_MSU.1 (concernant la documentation d'installation et de démarrage).

6.3.4.2 MA.GUIDE_ADMIN : Documentation d'administration

La documentation d'exploitation à destination des administrateurs doit décrire le comportement des fonctions de sécurité et refléter les hypothèses sur l'environnement d'exploitation, dans une optique de configuration, de maintenance et de maintien en condition opérationnelle corrects des fonctions de sécurité. Elle doit également décrire les différents types d'événements relatifs à la sécurité susceptibles de survenir, et fournir des lignes directrices sur la manière de les prendre en compte.

Des exigences spécifiques à la prévention de l'utilisation impropre, similaires à celles sur la documentation d'installation et de démarrage, pèsent également sur la documentation d'administration. La documentation d'administration est fournie.

Références des fournitures :

- ZoneCentral 3.1 Manuel Technique FR (PX81098) r5

Argumentaire : ces mesures satisfont de manière directe aux exigences AGD_ADM.1 et AVA_MSU.1 (concernant la documentation d'administration).

6.3.4.3 MA.GUIDE_UTILIS : Documentation utilisateur

La documentation d'exploitation à destination des utilisateurs doit décrire le comportement des fonctions de sécurité qu'ils ont besoin de connaître, et refléter les hypothèses sur l'environnement d'exploitation et les responsabilités qui les concernent (et notamment les situations qui nécessitent d'en référer à l'administrateur).

Des exigences spécifiques à la prévention de l'utilisation impropre, similaires à celles sur la documentation d'installation et de démarrage et d'administration, peuvent également peser sur la documentation utilisateur, sous réserve de leur pertinence et de leur applicabilité aux utilisateurs.

La documentation utilisateur est fournie.

Références des fournitures :

- ZoneCentral 3.1 Guide FR (PX81092) r3

Argumentaire : ces mesures satisfont de manière directe aux exigences AGD_USR.1 et AVA_MSU.1 (concernant la documentation utilisateur).

6.3.5. MA.VUL : Estimation de la vulnérabilité

Cette tâche s'appuie sur les résultats de toutes les tâches précédentes et sur des sources publiques pour identifier les faits techniques (vulnérabilités) susceptibles de causer la réalisation de menaces identifiées dans la présente cible de sécurité ou des infractions aux règles de politiques de sécurité de l'organisation de la présente cible de sécurité. La résistance des mécanismes de sécurité de nature combinatoire ou probabiliste aux attaques directes est également estimée.

Une analyse de vulnérabilités est fournie, énonçant toutes les vulnérabilités décelées au cours du développement, montrant qu'elles ne sont pas exploitables et justifiant que la cible d'évaluation résiste aux attaques de pénétration requérant une compréhension minimale de son fonctionnement.

Une analyse de la résistance des mécanismes pour lesquels une annonce de résistance des fonctions a été faite dans la présente cible de sécurité est également fournie.

Références des fournitures :

- PRIMX-ZoneCentral 3.1 analyse de vulnérabilités (PX82129) v1r2

Argumentaire : ces mesures satisfont de manière directe aux exigences AVA_SOF.1 et AVA_VLA.2.

7. Annonces de conformité à un PP

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

8. Argumentaire

8.1. Argumentaire pour les objectifs de sécurité

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

8.1.1. Hypothèses

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

		Objectifs de sécurité pour l'environnement de la TOE											
		OE.SOFT_SIGNE	OE.NON_OBSERV	OE.ENV_OPERATIONNEL	OE.SO_CONF	OE.CONSERV_CLES	OE.CERTIFICATS	OE.ADM_ROOT_WINDOWS	OE.ADM_DELEGATION	OE.INSTALLATION	OE.FORMATION	OE.CRYPTO_EXT	
Hypothèses	H.NON_OBSERV		X										
	H.ENV_OPERATIONNEL			X									
	H.CONFIANCE_ADM_TOE				X						X		
	H.CONSERVATION_CLES					X					X		
	H.CERTIFICATS						X						
	H.ADMIN_WINDOWS							X	X		X		
	H.INSTALLATION	X					X			X	X		
	H.CRYPTO_EXT											X	

Tableau 5 : Couverture des hypothèses par les objectifs de sécurité

H.NON_OBSERV

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

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

H.ENV_OPERATIONNEL

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

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

H.CONFIANCE_ADM_TOE

Les administrateurs de la TOE sont des personnes de confiance et sont formés à l'utilisation de la TOE.

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

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 de ses clés.

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

H.CERTIFICATS

L'administrateur de la TOE est chargé, lors de la fourniture des clés d'accès possédant un certificat X509, de vérifier la validité de ces certificats et leur adéquation avec l'usage qui en est fait par la TOE.

L'objectif OE.CERTIFICATS couvre directement cette hypothèse.

H.ADMIN_WINDOWS

Les administrateurs Windows de plus haut niveau du domaine Windows sont chargés d'interdire aux administrateurs Windows des sous-niveaux (domaines, contrôleurs de domaines, postes de travail) la modification des « polices » de la TOE.

Les objectifs OE.ADM_ROOT_WINDOWS, OE.ADM_DELEGATION et OE.FORMATION couvrent cette hypothèse en séparant les rôles et en formant les administrateurs.

H.INSTALLATION

L'administrateur de la TOE est chargé d'installer la TOE conformément à son manuel d'installation et de vérifier périodiquement son intégrité (signature authenticode dans les propriétés de l'exécutable).

Les objectifs OE.INSTALLATION et OE.FORMATION couvrent directement la partie relative à l'installation de la TOE de cette hypothèse, et les objectifs OE.SOFT_SIGNE et OE.CERTIFICATS couvrent les aspects liés à la vérification de l'intégrité.

H.CRYPTO_EXT

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

L'objectif OE.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 :

Menaces	Objectifs de sécurité pour la TOE	Objectifs de sécurité pour l'environnement de la TOE
M.DETOURN_COMPOSANT	O.ACCES, O.ALGO_STD, O.EFF_RESIDUS, O.AUTH	OE.SOFT_SIGNE
M.ATTAQUE_FIC_INTERNES	O.ACCES, O.ALGO_STD, O.ALEAS	
M.MODIF_FIC_INTERNES	O.ACCES, O.ALGO_STD	

Tableau 6 : Couverture des menaces par les objectifs de sécurité

M.DETOURN_COMPOSANT

Un attaquant met en œuvre, éventuellement à bas niveau, les composants internes de la TOE, pour contourner certaines fonctions de sécurité. Il peut pour cela effectuer du «reverse-ingeniering» sur les programmes, développer des programmes d'appel des fonctions internes de la TOE, ou s'aider d'un debugger. Un bon exemple est le contournement d'une règle de sécurité qui aurait été implémentée dans une IHM et non pas de façon plus interne dans le produit.

→ Pour prévenir cette menace, la TOE doit :

- Garantir le fait qu'il n'est pas possible, cryptographiquement, de retrouver les clés de chiffrement de zones sans fournir une clé d'accès valide : 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.ACCES et O.ALGO_STD),
- Garantir le fait qu'avant toute opération sur la TOE, une authentification est nécessaire (O.AUTH),
- Garantir que les composants de la TOE sont intègres (OE.SOFT_SIGNE) et ce, grâce aux mécanismes Authenticode de Windows :

Signatures : clé certifiée Thawte type Authenticode, validation Kbis,

Horodatage : horodatage signé en ligne à la génération par Verisign.

→ Pour se protéger, la TOE doit :

- Garantir le fait qu'un composant détourné ne conserve pas de résidus permettant de présenter un chemin pour une attaque (O.EFF_RESIDUS).

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

rien

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

Rien

M.ATTAQUE_FIC_INTERNES Un attaquant récupère des fichiers internes de la TOE pour pénétrer dans une zone chiffrée.

→ Pour prévenir cette menace, la TOE doit :

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

→ Pour se protéger, la TOE doit :

■ Garantir le fait que les fichiers internes des différentes zones sont rendus «cryptographiquement différents» par l'utilisation d'aléas ne permettant pas de tirer des enseignements d'un fichier interne (ou zone) pour en attaquer un autre (O.ALEAS).

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

rien

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

Rien

M.MODIF_FIC_INTERNES Un attaquant modifie les fichiers internes de la TOE pour tenter de retrouver des informations protégées.

→ Pour prévenir cette menace, la TOE doit :

■ Garantir le fait qu'il n'est pas possible, cryptographiquement, de retrouver les clés de chiffrement de zones sans fournir une clé d'accès valide (O.ACCES) en utilisant des algorithmes standards (O.ALGO_STD), et par le fait que les fichiers internes de la TOE respectent également ce principe (O.ACCES).

→ Pour se protéger, la TOE doit :

rien

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

rien

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

rien

8.1.3. Politiques de sécurité de l'organisation

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

	O.CHIFFREMENT	O.ACCES	O.ALGO STD	O.CLES TOKEN	O.CLES P12	O.CLES PWD	O.ROLES	O.GEST SECRETS	O.EFF RESIDUS	O.ALEAS	O.EFF FICHIERS	O.ADM ZONES	O.ADM ACCES	O.AUTH	O.AUDIT
P.ZONE	X							X	X					X	X
P.ACCES		X		X	X	X			X					X	X
P.ADMIN_ZONES	X						X		X	X		X		X	X
P.ADMIN_ACCES							X		X	X			X	X	X
P.EFF_FICHIERS											X				
P.SWAP	X								X	X					
P.CRYPTO			X						X	X					

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

P.ZONE

La TOE doit offrir un service de protection en confidentialité (chiffrement), automatique et systématique, du stockage des fichiers sensibles des utilisateurs, ces fichiers ne pouvant être lus (déchiffrés) ou écrits (chiffrés) que par des utilisateurs disposant de clés d'accès valides pour ces fichiers.

Note: cette politique ne concerne pas la création initiale de la zone (avec le chiffrement de son contenu initial), qui relève de P.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 P.ACCES (et P.ADMIN_ACCES). De plus, O.ALEAS n'intervient pas ici, car cette politique s'applique à une zone chiffrée existante, dont les clés existent déjà.

→ Pour mettre en œuvre la politique, la TOE :

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

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

- Efface les traces mémoire liées aux clés de chiffrement des zones (O.EFF_RESIDUS) ;
- ➔ Pour contrôler la mise en œuvre de la politique, la TOE :
- Enregistre les événements relatifs au traitement de la zone (O.AUDIT).

P.ACCES

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

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

- ➔ Pour mettre en œuvre la politique, la TOE :
- Demande une authentification avant tout accès à une zone chiffrée et attribue un rôle à l'utilisateur (O.AUTH);
- Fait en sorte que seule une clé d'accès valide puisse permettre de retrouver les clés de chiffrement d'une zone, et que les fichiers ou informations internes de la TOE ne permettent pas de faire autrement (O.ACCES).
- ➔ Pour garantir la mise en œuvre de la politique, la TOE :
- Définit les supports ou moyens avec lesquels les utilisateurs peuvent fournir leur(s) clé(s) d'accès (O.CLES_TOKEN, O.CLES_P12 et O.CLES_PWD).
- Efface les traces mémoire liées aux éventuels calculs cryptographiques intermédiaires (dérivation de mots de passe) ou au transport des valeurs de clés de chiffrement lorsqu'elles sont calculées par un dispositif cryptographique externe (token) (O.EFF_RESIDUS) ;
- ➔ Pour contrôler la mise en œuvre de la politique, la TOE :
- Enregistre les événements en relation avec l'utilisation (ouverture ou fermeture) d'une zone (O.AUDIT).

P.ADMIN_ZONES

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

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_ACCES.

- Pour mettre en œuvre la politique, la TOE :
 - Demande une authentification avant de permettre la gestion des zones (O.AUTH) ;
 - Offre une interface à l'administrateur, lui permettant de visualiser et gérer le chiffrement et le déchiffrement des « zones » (O.ADM_ZONES).
- Pour garantir la mise en œuvre de la politique, la TOE :
 - Chiffre les fichiers quand on crée une zone chiffrée (chiffrement initial des fichiers qu'elle contient), déchiffre les fichiers quand on crée une zone en clair (déchiffrement quand les fichiers étaient initialement chiffrés) (O.CHIFFREMENT) ;
 - Génère, lors d'un chiffrement des aléas pour la création des clés de chiffrement des zones (O.ALEAS) ;
 - Efface les traces mémoires des clés de chiffrement manipulées, mais intervient également plus fortement pour l'effacement de la version «en clair» des fichiers lorsqu'on crée une zone chiffrée (effacement de l'original) (O.EFF_RESIDUS).
- Pour contrôler la mise en œuvre de la politique, la TOE :
 - Contrôle que seul un utilisateur disposant du rôle 'administrateur' dans une zone chiffrée existante a le droit d'intervenir sur cette zone (la déchiffrer, ...) (O.ROLES) ;
 - Enregistre les événements en relation avec la gestion d'une zone (O.AUDIT).

P.ADMIN_ACCES

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

- Pour mettre en œuvre la politique, la TOE :
 - Demande une authentification avant de permettre la gestion des accès aux zones chiffrées (O.AUTH) ;
 - Offre une interface à l'administrateur, comme à l'utilisateur, lui permettant de visualiser et gérer les clés d'accès aux « zones » (O.ADM_ACCES).
- Pour garantir la mise en œuvre de la politique, la TOE :
 - Fait intervenir un ingrédient aléatoire (qui n'est pas une clé) dans la dérivation de clé à partir d'un mot de passe, quand un accès de type 'mot de passe' est ajouté (O.ALEAS) ;
 - Efface les traces mémoires des clés de chiffrement manipulées (O.EFF_RESIDUS).
- Pour contrôler la mise en œuvre de la politique, la TOE :
 - Contrôle que seul un utilisateur disposant du rôle 'administrateur' dans une zone chiffrée existante a le droit d'intervenir sur cette zone (la déchiffrer, ...) (O.ROLES) ;
 - Enregistre les événements en relation avec la gestion des accès à une zone (O.AUDIT).

P.EFF_FICHIERS

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

→ Pour mettre en œuvre la politique, la TOE :

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

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

rien

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

Rien

P.SWAP

La TOE doit offrir un service de chiffrement, transparent pour les utilisateurs, des fichiers d'échanges de la mémoire virtuelle (swap) de Windows.

→ Pour mettre en œuvre la politique, la TOE :

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

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

- Génère lors d'un chiffrement ou d'un déchiffrement, des aléas pour la création des clés de chiffrement du swap (O.ALEAS) ;
- Efface les traces mémoires des clés de chiffrement manipulées (O.EFF_RESIDUS) ;

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

Rien

P.CRYPTO

Les mécanismes cryptographiques de la TOE doivent être conformes aux exigences du référentiel cryptographique de la DCSSI pour le niveau de robustesse standard ([CRYPTO_STD]).

→ Pour mettre en œuvre la politique, la TOE :

- Fournit un choix d'algorithmes cryptographiques et de tailles de clés conformes à l'état de l'art et aux standards de ce domaine, prévus dans [CRYPTO_STD] (O.ALGO_STD),
- Génère lors d'un chiffrement ou d'un déchiffrement, des aléas pour la création des clés de chiffrement du swap (O.ALEAS),
- Efface les traces mémoires des clés de chiffrement manipulées (O.EFF_RESIDUS).

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

rien

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

rien

8.2. Argumentaire pour les exigences de sécurité

8.2.1. Dépendances entre exigences fonctionnelles de sécurité

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

Composant	Dépendances	Dépendances satisfaites
FAU_GEN.1	FPT_STM.1	FPT_STM.1/ENV
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, FMT_MSA.2	FCS_COP.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.3	[FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FDP_ITC.1, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	[FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FMT_MSA.2	FDP_ITC.1, FCS_CKM.1, FMT_MSA.2
FCS_COP.1	[FDP_ITC.1 ou FDP_ITC.2 ou FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FDP_ITC.1, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FDP_ITC.1	[FDP_ACC.1 ou FDP_IFC.1], FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FDP_RIP.2	Aucune	Aucune
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	Aucune	Aucune
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 ou FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	FDP_ACC.1, FMT_SMF.1, FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 ou FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_ACC.1, FMT_MSA.1, FMT_SMR.1 ADV_SPM.1 : non satisfaite
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	Aucune	Aucune
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_SEP.1	Aucune	Aucune
FTA_SSL.3	Aucune	Aucune
FTP_TRP.1	Aucune	Aucune
FPT_STM.1/ENV	Aucune	Aucune
FCO_NRO.1/ENV	FIA_UID.1	FIA_UID.1 non satisfaite

Tableau 8 : Satisfaction des dépendances entre exigences fonctionnelles de sécurité

8.2.2. Argumentaire pour les dépendances non satisfaites

Dépendance de FMT_MSA.2 sur ADV_SPM.1 : ADV_SPM.1 n'est pas justifié pour le niveau d'assurance visé conformément au document de référence [QUALIF_STD] qui décrit la sélection des composants d'assurance pour le niveau « qualification standard ».

Dépendance de FCO_NRO.1/ENV sur FIA_UID.1 : l'exigence FCO_NRO.1/ENV est utilisée pour décrire le fait que l'environnement fournit, sur la base de clé certifiée Thawte de type Authenticode, un moyen de signer les composants de la TOE. La dépendance sur FIA_UID.1 sera implicitement satisfaite par l'environnement d'exploitation utilisé pour produire ces clés certifiées. Il n'a pas été jugé pertinent d'inclure cette exigence fonctionnelle car, du fait des affectations à réaliser (identifier l'ensemble des opérations réalisables dans l'environnement sans que l'utilisateur soit identifié), il n'est pas réaliste d'en donner une définition correcte.

8.3. 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 l'environnement	FPT_STM.1/ENV	FCO_NRO.1/ENV
OE.SOFT_SIGNE	X	X

Tableau 9 : Couverture des objectifs de sécurité sur l'environnement par les exigences fonctionnelles de sécurité sur l'environnement

Objectifs de sécurité de la TOE	FAU_GEN.1	FAU_GEN.2	FCS_CKM.1	FCS_CKM.3	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_ITC.1	FDP_RIP.2	FIA_AFL.1	FIA_UAU.2	FIA_UID.2	FMT_MOF.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_SEP.1	FTA_SSL.3	FTP_TRP.1	
O.CHIFFREMENT			X	X		X																		
O.ACCES							X	X	X														X	
O.ALGO_STD			X	X	X	X																		
O.CLES_TOKEN									X															X
O.CLES_P12									X															X
O.CLES_PWD			X																					
O.ROLES							X	X						X				X	X	X				
O.GEST_SECRETS			X				X	X													X			
O.EFF_RESIDUS									X															
O.ALEAS			X			X																		
O.EFF_FICHIERS									X															
O.ADM_ZONES														X	X	X	X							
O.ADM_ACCES																			X	X				
O.AUTH											X	X	X											
O.AUDIT	X	X																						

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

8.3.1. Contrôle d'accès

O.ACCES

La TOE ne doit autoriser l'accès à une zone chiffrée qu'après présentation d'une clé d'accès valide pour la zone.

De plus, la TOE doit permettre de chiffrer conformément à [CRYPTO_STD] les éléments sensibles de ses fichiers de fonctionnement internes (liés à la zone) par les clés d'accès des utilisateurs autorisés.

Afin de remplir cet objectif :

- Pour que la TOE donne l'accès à une zone chiffrée, l'utilisateur doit présenter sa clé d'accès (token USB par exemple) en vue de son authentification (FDP_ITC.1). La TOE applique ensuite une politique de contrôle d'accès aux « zones » (FDP_ACC.1) et aux objets de la « zones » basé sur les attributs de sécurité (FDP_ACF.1).

- La TOE peut ensuite, à l'activation de l'économiseur d'écran, fermer la session de l'utilisateur (FTA_SSL.3) pour forcer la présentation d'une clé d'accès valide en cas d'absence momentanée de l'utilisateur.

O.AUTH

La TOE doit permettre d'identifier et authentifier tout utilisateur.

Afin de remplir cet objectif :

- La TOE identifie et authentifie chaque utilisateur avant de permettre toute opérations (FIA_UID.2 et FIA_UAU.2) et applique une règle de ralentissement d'affichage de la mire de connexion à un utilisateur, suite à plusieurs essais d'authentification infructueux (FIA_AFL.1).

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, plus possibilité d'administrer la zone chiffrée, c'est-à-dire gérer ses accès, la déchiffrer complètement).

Le «pouvoir» d'un utilisateur doté du rôle «administrateur» sur une zone chiffrée peut être restreint globalement par les politiques, qui peuvent lui interdire certaines actions (globalement, toutes zones confondues).

Afin de remplir cet objectif :

- La TOE doit gérer et distinguer les rôles d'administrateur de la TOE et d'utilisateur de la TOE (FMT_SMR.1) et restreindre certaines fonctions aux utilisateurs (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 aux administrateurs les fonctions d'administration de la sécurité (FMT_SMF.1) et la gestion des « politiques » (FMT_MTD.1).

8.3.2. Cryptographie

O.CHIFFREMENT La TOE doit chiffrer les « zones » configurées et les fichiers swap par l'emploi de clés cryptographiques.

Afin de remplir cet objectif :

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

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

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).

O.CLES_TOKEN La TOE doit permettre l'emploi de clés d'accès contenues dans un porte-clés comme une carte à puce ou une clé USB. L'utilisation de ces clés d'accès doit être conditionnée par la présentation à la TOE du porte-clés et du code PIN associé.

Afin de remplir cet objectif :

- La TOE doit récupérer des clés d'accès localisées dans un « token » ou une carte à puce (FTP_TRP.1) de manière sécurisée et les importer dans le périmètre sous son contrôle de manière à pouvoir les utiliser (FDP_ITC.1).

O.CLES_P12

La TOE doit permettre l'emploi de clés d'accès contenues dans un fichier au format PKCS#12. L'utilisation de ces clés d'accès doit être conditionnée par la présentation à la TOE du fichier PKCS#12 et du code secret associé.

Afin de remplir cet objectif :

- La TOE doit récupérer des clés d'accès localisées dans un fichier sécurisé (FTP_TRP.1) et les importer dans le périmètre sous son contrôle de manière à pouvoir les utiliser (FDP_ITC.1).

O.CLES_PWD

La TOE doit permettre l'emploi de clés d'accès obtenues par diversification d'un mot de passe saisi au clavier.

Afin de remplir cet objectif :

- La TOE doit diversifier les mots de passe saisi au clavier en utilisant un algorithme de diversification standard (FCS_CKM.1).

O.ALEAS

La TOE doit implémenter un mécanisme de génération de pseudo-aléas ou d'aléas vrais avec suffisamment d'entropie pour assurer la production d'aléas non prédictibles.

Afin de remplir cet objectif :

- La TOE permet de générer des pseudo-aléas ou des aléas vrais selon des algorithmes (FCS_CKM.1) et d'effectuer des opérations cryptographiques sur ceux-ci (FCS_COP.1).

8.3.3. Gestion des zones

O.GEST_SECRETS

La TOE doit utiliser des clés différentes pour protéger les différentes «zones» configurées, même si les utilisateurs sont les mêmes pour ces « zones ».

Afin de remplir cet objectif :

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

- Elle doit ensuite appliquer une politique de contrôle d'accès aux « zones » (FDP_ACC.1) et aux objets dans la « zone », basé sur des attributs de sécurité (FDP_ACF.1).
- La TOE met en place une séparation entre les domaines de sécurité des utilisateurs (FPT_SEP.1) afin de prévenir des interférences entre clés lors des opérations cryptographiques.

O.ADM_ZONES

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

Afin de remplir cet objectif :

- La TOE assure que seuls les administrateurs de la TOE peuvent gérer le comportement de chiffrement des « zones » (FMT_MOF.1) et les attributs de sécurité des objets stockés (FMT_MSA.1).
- L'administrateur peut aussi définir les données statiques d'une zone, tel que le type d'algorithme de chiffrement et la longueur des clés à utiliser (FMT_MSA.3).
- La TOE garantit, de plus, que seuls des valeurs sûres sont acceptées pour les attributs de sécurité (FMT_MSA.2).

O.ADM_ACCES

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

Afin de remplir cet objectif :

- La TOE offre des fonctions d'administration et de gestions (FMT_SMF.1) des zones
- La TOE limite les accès à ces fonctions d'administration et de gestion en fonction du rôle associé aux utilisateurs (FMT_SMR.1).

8.3.4. Effacement

O.EFF_RESIDUS

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

Afin de remplir cet objectif :

- La TOE permet un nettoyage totalement sécurisé des traces dans la mémoire (RAM) ou sur le disque dur (FDP_RIP.2).

O.EFF_FICHIERS

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

Afin de remplir cet objectif :

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

8.3.5. Protections lors de l'exécution

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).
- L'environnement de la TOE fournit un système d'horodatage fiable qui permet à la TOE de dater précisément les événements enregistrés dans le journal (FPT_STM.1/ENV)

8.3.6. Objectifs sur l'environnement

OE.SOFT_SIGNE

Les composants de la TOE doivent être signés et horodatés par le fournisseur de la TOE pour permettre aux administrateurs de la TOE de vérifier son intégrité.

Afin de remplir cet objectif :

- L'environnement de la TOE fournit un système d'horodatage fiable qui permet au fournisseur de la TOE de dater précisément les composants de la TOE (FPT_STM.1/ENV).
- L'environnement de la TOE fournit un système de vérification de l'intégrité de la TOE à base de certificats racines dits «authenticode» (FCO_NRO.1/ENV).

8.3.7. Argumentaire pour le support mutuel des exigences fonctionnelles

Comme démontré par l'argumentaire précédent, ainsi que par le respect des dépendances entre exigences fonctionnelles, les exigences fonctionnelles contribuent ensemble à satisfaire les objectifs de sécurité pour la TOE. De plus il n'existe aucun conflit entre les exigences fonctionnelles sélectionnée et définies dans cette cible de sécurité.

8.4. Argumentaire pour les spécifications globales de la TOE

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

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

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

FAU_GEN.1 Génération de données d'audit

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

- Les opérations d'administration de la TOE : commandes d'administration réussies ou en échec (F.CONFIGURATION_TOE),
- Les opérations de configuration des zones : création, suppression ou modification de zone, création de profil d'exception de fichier dans une zone, modification ou ajout de clé d'accès sur une zone (F.CONFIGURE_ZONE),
- Les opérations de gestion des clés d'accès : création, suppression, ouverture ou fermeture (F.GESTION_CLES),
- Les opérations diverses sur les zones : chiffrement, déchiffrement, reprise de chiffrement ou déchiffrement d'une zone (F.GESTION_OP_ZONE),
- Les opérations de contrôle d'accès : ouverture, fermeture de zone (F.CONTROLE_ACCES_ZONE, F.GESTION_DROITS).
- Les opérations d'accès aux clés, succès ou échec (F.ENTREE_SECURISEE)
- Les opérations cryptographiques nécessaires au fonctionnement de ZoneCentral (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 :

- Les opérations d'administration de la TOE : commandes d'administration réussies ou en échec (F.CONFIGURATION_TOE),
- Les opérations de configuration des zones : création, suppression ou modification de zone, création de profil d'exception de fichier dans une zone, modification ou ajout de clé d'accès sur une zone (F.CONFIGURE_ZONE),
- Les opérations de gestion des clés d'accès : création, suppression, ouverture ou fermeture (F.GESTION_CLES),
- Les opérations diverses sur les zones : chiffrement, déchiffrement, reprise de chiffrement ou déchiffrement d'une zone (F.GESTION_OP_ZONE),
- Les opérations de contrôle d'accès : ouverture, fermeture de zone (F.CONTROLE_ACCES_ZONE, F.GESTION_DROITS).
- Les opérations d'accès aux clés, succès ou échec (F.ENTREE_SECURISEE)
- Les opérations cryptographiques nécessaires au fonctionnement de ZoneCentral (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 politiques. Par défaut, c'est une clé AES de 256 bits.

A chaque clé d'accès créée, une clé cryptographique est générée par la TOE.

La fonction de sécurité F.GESTION_CLES 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.

Cette fonction est utilisée lorsque la TOE :

- Récupère une clé d'accès avant de pouvoir créer une clé de zone,
- Récupère une clé d'accès pour accéder à la clé de la zone avant de pouvoir créer une nouvelle clé d'accès,
- Récupère une clé d'accès avant de pouvoir utiliser la clé de zone et déchiffrer la zone,
- Récupère une clé d'accès avant de pouvoir utiliser la clé de zone et déchiffrer les fichiers répondant à l'exception,
- Récupère la clé de zone afin de pouvoir terminer les chiffrements inachevés,
- Récupère une clé d'accès avant de pouvoir utiliser une clé de zone,
- Récupère une clé d'accès avant de pouvoir utiliser une clé de zone.

FCS_CKM.4 Destruction de clés cryptographiques

Lorsqu'une zone est supprimée, les clés cryptographiques relatives à la zone sont détruites. De même lorsqu'une des clés d'accès à la zone d'un utilisateur est supprimée, la clé d'accès à la zone associée est détruite.

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

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 et chiffrer la zone,
- Récupère une clé d'accès pour déchiffrer la clé de la zone avant de pouvoir créer une nouvelle clé d'accès en dérivant la clé de zone,
- Récupère une clé d'accès avant de pouvoir déchiffrer la clé de zone, afin de pouvoir déchiffrer la zone,
- Récupère une clé d'accès avant de pouvoir utiliser la clé de zone et déchiffrer les fichiers répondant à l'exception,
- Récupère la clé de zone afin de pouvoir terminer les chiffrements inachevés,
- Récupère une clé d'accès avant de pouvoir déchiffrer une clé de zone et ainsi pouvoir déchiffrer la zone,
- Récupère une clé d'accès avant de pouvoir déchiffrer une clé de zone et ainsi pouvoir déchiffrer la ou les zones.
- Récupère un mot de passe afin d'en dériver une clé d'accès qui va chiffrer ou déchiffrer la clé de zone.
- Transmet la clé de zone chiffrée au porte-clés puis récupère la clé de zone déchiffrée par le porte-clés afin de pouvoir déchiffrer la zone,

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

Les fonctions F.GESTION_CLES (création de la clé d'accès) 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_DROITS pour la configuration des accès aux zones par l'administrateur
- F.CONTROLE_ACCES_ZONE pour le contrôle d'accès aux zones
- F.CONFIGURE_ZONE et F.GESTION_OP_ZONE pour le contrôle d'accès aux opérations sur les 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_DROITS),
- et l'accès aux zones est donc contrôlé (F.CONTROLE_ACCES_ZONE, F.GESTION_OP_ZONE et F.CONFIGURE_ZONE).

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

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

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

FDP_RIP.2 Protection totale des informations résiduelles

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

Cette exigence fonctionnelle est mise en œuvre par la fonction de sécurité F.GESTION_OP_ZONE qui est le point d'entrée des opérations sur les zones ainsi que par F.GESTION_CLES qui gère l'effacement sécurisé des clés d'accès et des clés de zone.

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

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

Après une tentative d'ouverture de zone, si cette ouverture n'a pas été effectuée parce que l'utilisateur a annulé la demande ou parce qu'il n'y a pas eu de réponse dans les délais impartis, toute nouvelle ouverture de la même zone est automatiquement rejetée si elle intervient dans un délai court après ce premier refus. Ce délai est paramétrable (par défaut cinq secondes) et permet de renforcer la sécurité lorsque quelqu'un tente de multiples essais de mots de passe ou de codes : il sera ralenti par ce délai entre ses différents essais.

Les fonctions de sécurité faisant intervenir un contrôle d'accès F.CONTROLE_ACCES_ZONE, F.GESTION_DROITS, F.GESTION_OP_ZONE et F.CONFIGURE_ZONE couvrent ces fonctionnalités et la configuration de ces options est assurée par la fonction de sécurité F.CONFIGURATION_TOE.

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

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

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

Cette exigence fonctionnelle est implémentée par :

- F.CONFIGURE_ZONE et F.GESTION_OP_ZONE pour la gestion des zones,
- F.GESTION_DROITS pour la gestion des utilisateurs et leurs droits associés,
- F.GESTION_CLES et 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.

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

Cette exigence fonctionnelle est implémentée par :

- F.CONFIGURE_ZONE pour le fait que les accès aux zones sont configurés,
- F.GESTION_DROITS pour la gestion des utilisateurs et leurs droits associés,
- F.GESTION_CLES et 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

Seuls les administrateurs de la TOE peuvent déterminer le comportement, activer/désactiver, modifier le comportement des fonctions de chiffrement de zones.

Ils ont par exemple la possibilité de choisir l'algorithme de chiffrement des zones lors de leur création (AES, 3DES, avec longueurs de clés de 128, 192 ou 256 bits) ou d'activer la génération de données d'audit.

La fonction de sécurité F.CONFIGURATION_TOE implémente cette exigence.

FMT_MSA.1 Gestion des attributs de sécurité

Seuls les administrateurs ont la possibilité de modifier la valeur par défaut, interroger, modifier ou supprimer l'attribut de sécurité « identifiants de zone ».

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

Les fonctions de sécurité F.GESTION_OP_ZONE , F.CONFIGURATION_TOE et F.CONFIGURE_ZONE implémentent cette exigence.

FMT_MSA.2 Attributs de sécurité sûrs

Les fonctions de sécurité F.GESTION_OP_ZONE, F.CONFIGURATION_TOE et F.CONFIGURE_ZONE permettent de garantir que l'unique attribut de sécurité « identifiant de zone » est sûr.

FMT_MSA.3 Initialisation statique d'attribut

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

Les fonctions de sécurité F.GESTION_OP_ZONE, F.CONFIGURATION_TOE et F.CONFIGURE_ZONE mettent en œuvre cette exigence.

FMT_MTD.1 Administration des données de la TSF

Seuls les administrateurs ont la possibilité de gérer les stratégies de sécurité (ou « politiques»). Cette exigence est implémentée par la fonction de sécurité F.CONFIGURATION_TOE.

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 et mots de passe
- Les fonctions de gestion des zones
- Les fonctions d'initialisation des paramètres utilisés par les fonctions de sécurité

Cette exigence fonctionnelle est implémentée par les fonctions de sécurité :

- F.CONFIGURATION_TOE (configuration des politiques)
- F. CONFIGURE_ZONE et F.GESTION_OP_ZONE (gestions des zones)
- F. GESTION-DROITS (gestion des clés et mots de passe)

FMT_SMR.1 Rôles de sécurité

La TOE supporte les rôles utilisateur et administrateur.

Cette exigence est implémentée par F.CONFIGURATION_TOE qui fixe les droits administrateur et utilisateur par l'intermédiaire des politiques et par F.GESTION_DROITS pour la gestion des utilisateurs et de leurs droits associés.

FPT_SEP.1 Séparation de domaines pour la TSF

La fonction de sécurité F.OPERATIONS_CRYPTO implique que les opérations cryptographiques doivent être réalisées en utilisant des zones mémoire dédiées, ce qui contribue directement à assurer une séparation de domaines au sein de la TSF.

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

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

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

FTP_TRP.1 Chemin de confiance

A chaque fois qu'un utilisateur utilise une clé d'accès ou un code confidentiel, celui-ci transite via des chemins de confiance. Cette exigence est implémentée par la fonction de sécurité F.ENTREE_SECURISEE qui assure la communication de données fournies en entrée vers la TOE.

8.5. Argumentaire pour les mesures d'assurance

Le tableau ci-dessous justifie la nécessité des mesures d'assurance par rapport aux composants d'assurance Critères Communs sélectionnés. L'argumentaire détaillé est fourni au chapitre 6.3

Mesures d'assurance		MA_ENV_CONE	MA_ENV_SEC	MA_ENV_LIV	MA_ENV_SUP	MA_DEV	MA_TEST_DEV	MA_TEST_EVAL	MA_GUIDE_INST	MA_GUIDE_ADMIN	MA_GUIDE_UTILIS	MA_VUL
ACM_CAP.2	Éléments de configuration	X										
ADO_DEL.1	Procédures de livraison			X								
ADO_IGS.1	Procédures d'installation, de génération et de démarrage								X			
ADV_FSP.1	Spécifications fonctionnelles informelles					X						
ADV_HLD.2	Conception de haut niveau de sécurité					X						
ADV_IMP.1	Sous-ensemble de l'implémentation de la TSF					X						
ADV_LLD.1	Conception de bas niveau descriptive					X						
ADV_RCR.1	Démonstration de correspondance informelle					X						
AGD_ADM.1	Guide de l'administrateur									X		
AGD_USR.1	Guide de l'utilisateur										X	
ALC_DVS.1	Identification des mesures de sécurité		X									
ALC_FLR.3	Correction d'anomalies systématique				X							
ALC_TAT.1	Outils de développement bien définis					X						
ATE_COV.1	Éléments de preuve de la couverture						X					
ATE_FUN.1	Tests fonctionnels						X					
ATE_IND.2	Tests indépendants - par échantillonnage						X	X				
AVA_MSU.1	Examen des guides								X	X	X	
AVA_SOF.1	Evaluation de la résistance des fonctions de sécurité de la TOE											X
AVA_VLA.2	Analyse de vulnérabilités indépendante											X

Tableau 12 : Couverture des exigences d'assurance sécurité par les mesures d'assurance

8.6. 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.

8.7. Pertinence du niveau d'assurance

Le niveau d'assurance EAL2 augmenté de ALC_FLR.3, AVA_VLA.2, ADV_HLD.2, AVA_MSU.1 et ALC_DVS.1, ainsi que ADV_LLD.1, ALC_TAT.1 et ADV_IMP.1 pour les mécanismes cryptographiques (FCS) a été choisi pour assurer la conformité au processus de qualification de niveau standard défini par la DCSSI dans [QUALIF_STD]. Ce niveau d'assurance impose:

- Des tests indépendants effectués par l'évaluateur (l'utilisateur final est alors assuré que les fonctions de sécurité de la TOE sont implémentées comme spécifié)
- Une analyse de vulnérabilité indépendante effectuée par l'évaluateur (l'utilisateur final est alors assuré que la TOE est résistante à des attaques de pénétration effectuées par des attaquants possédant un faible potentiel d'attaque).
- L'évaluation de l'architecture de haut niveau et de bas niveau incluant l'analyse de l'implémentation (fonctions cryptographiques seulement) pour vérifier qu'il n'y a pas de défaut de sécurité
- De bonnes pratiques en matière de développement (l'utilisateur final est alors assuré que le produit a été correctement et sécuritairement conçu et développé et que tous les éventuels défauts de sécurité ont été tracés, analysés et corrigés).

8.8. Pertinence du niveau de résistance des fonctions exigées

Le niveau de résistance des fonctions exigées est SOF-high et se justifie par le niveau des informations traitées par le produit et par les exigences du référentiel cryptographique de la DCSSI [CRYPTO_STD].

9. Annexe A : Exigences de sécurité de la TOE

Cette annexe contient les textes officiels de la partie 2 des Critères Communs en version 2.3 d'Août 2005 avec l'ensemble des opérations réalisées pour la TOE.

9.1. Exigences fonctionnelles de sécurité de la TOE

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

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

Tableau 13 : Exigences fonctionnelles de sécurité pour la TOE

9.1.1. Class FAU : Security audit

FAU_GEN	Security audit data generation
FAU_GEN.1	Audit data generation
FAU_GEN.1.1	<p>The TSF shall be able to generate an audit record of the following auditable events:</p> <ul style="list-style-type: none"> a) Start-up and shutdown of the audit functions; b) All auditable events for the [<i>minimum</i>] level of audit; and c) [<ul style="list-style-type: none"> - Evénements journalisés au titre de la gestion des zones (chiffrement, déchiffrement, détachement, regroupement, création de zone en clair) ; - 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 gestion des exceptions (création ou suppression de profil d'exception de fichier dans une zone) ; - Evénements journalisés au titre de l'utilisation des zones (ouverture ou fermeture d'une zone) ;]
FAU_GEN.1.2	<p>The TSF shall record within each audit record at least the following information:</p> <ul style="list-style-type: none"> a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [<i>l'identifiant de l'administrateur</i>] .
FAU_GEN.2	User identity association
FAU_GEN.2.1	The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

9.1.2. 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 à 256 bits pour les clés symétriques et de 1024 à 2048 bits pour les clés asymétriques] that meet the following: [PKCS #1 v1.5 et PKCS#5 v2.0].
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 [déchiffrement (déwrapping) des clés par la clé d'accès] that meets the following: [Aucun].
FCS_CKM.4	Cryptographic key destruction
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [réécriture de motifs aléatoires] that meets the following: [Aucun].
FCS_COP	Cryptographic operation
FCS_COP.1	Cryptographic operation
FCS_COP.1.1	The TSF shall perform [le hashage, le chiffrement, le déchiffrement, la génération de clés, le wrapping de clés et la dérivation de clés] in accordance with a specified cryptographic algorithm [SHA-1, RSA, 3DES et AES] and cryptographic key sizes [de 128 à 256 bits pour les clés symétriques et de 1024 à 2048 bits pour les clés asymétriques] that meet the following: [RFC 3174 (SHA-1), ANSI X9.52-1998 (3DES), FIPS 197 (AES) et PKCS#1 (RSA)].

9.1.3. 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 [utilisateurs de la TOE, aux fichiers protégés par la TOE dans une « zone » et aux opérations dans les « zones »].

FDP_ACF	Access control functions
FDP_ACF.1	Security attribute based access control
FDP_ACF.1.1	The TSF shall enforce the [<i>SFP.ACCESS_OBJ</i>] to objects based on the following: [identifiant de la « zone » contenant le fichier].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [présentation de la clé d'accès associée à la « zone » concernée].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [Aucune].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the [Aucune].
FDP_ITC	Import from outside TSF control
FDP_ITC.1	Import of user data without security attributes
FDP_ITC.1.1	The TSF shall enforce the [<i>SFP.ACCESS_OBJ</i> et <i>SFP.ACCESS_ROLES</i>] when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [Aucune].
FDP_RIP	Residual information protection
FDP_RIP.2	Full residual information protection
FDP_RIP.2.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [désallocation de la ressource de] all objects.

9.1.4. 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 identify itself before allowing any other TSF-mediated actions on behalf of that user.

9.1.5. 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, désactiver, activer ou modifier le comportement de] the functions [de chiffrement des « zones »] to [administrateurs de la TOE] .

FMT_MSA	Management of security attributes
FMT_MSA.1	Management of security attributes
FMT_MSA.1.1	The TSF shall enforce the [SFP.ACCESS_ROLES] to restrict the ability to [changer la valeur par défaut, interroger, modifier ou supprimer] the security attributes [identifiants de « zone »] to [administrateurs] .
FMT_MSA.2	Secure security attributes
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.

FMT_MSA.3	Static attribute initialisation
FMT_MSA.3.1	The TSF shall enforce the [<i>SFP.ACCESS_ROLES</i>] to provide [<i>restrictive</i>] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [administrateurs de la TOE] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD Management of TSF data

FMT_MTD.1	Management of TSF data
FMT_MTD.1.1	The TSF shall restrict the ability to [changer la valeur par défaut, interroger, modifier ou supprimer] the [stratégies de sécurité] to [administrateurs de la TOE].

FMT_SMF Specification of Management Functions

FMT_SMF.1	Specification of Management Functions
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [<ul style="list-style-type: none"> - <i>Les fonctions de contrôle d'accès aux opérations d'administration de la sécurité</i> - <i>Les fonctions de gestion des clés et mots de passe</i> - <i>Les fonctions de gestion des zones</i> - <i>Les fonction d'initialisation des parametres utilisés par les fonctions de sécurité</i>

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.

9.1.6. Class FPT : Protection of the TSF

FPT_SEP Domain separation

FPT_SEP.1	TSF domain separation
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.

9.1.7. Class FTA : TOE access

FTA_SSL Session locking

FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [délais de 5 secondes] of user inactivity, [comptées à partir du lancement de l'économiseur d'écran Windows].

Raffinement : ajout de "comptées à partir du lancement de l'économiseur d'écran Windows"

9.1.8. Class FTP : Trusted path/channels

FTP_TRP Trusted path

FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [*local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit [*the TSF, local users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [récupérer des clés d'accès localisés dans un « token » ou une carte à puce via l'API PKCS#11 ; récupérer des clés d'accès localisés dans un fichier sécurisé au format PKCS#12].

9.2. Exigences d'assurance de sécurité de la TOE.

9.2.1. Class ADV : Développement

ADV_IMP.1 Subset of the implementation of the TSF

Developer action elements :

ADV_IMP.1.1D The developer shall provide the implementation representation [refinement: **des fonctions cryptographiques**.]

Content and presentation of evidence elements :

ADV_IMP.1.1C The implementation representation [refinement: **des fonctions cryptographiques**] shall unambiguously define [refinement: **les fonctions cryptographiques**] to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2C The implementation representation [refinement: **des fonctions**

cryptographiques] shall be internally consistent.

Evaluator action elements :

- ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADV_IMP.1.2E The evaluator shall determine that the least abstract [refinement: TSF = **des fonctions cryptographiques]** representation provided is an accurate and complete instantiation of the TOE security functional requirements [refinement: **de la classe FCS.**]

ADV_LLD.1 Descriptive low-level design

Developer action elements :

- ADV_LLD.1.1D The developer shall provide the low-level design [refinement: of the TSF = **des fonctions cryptographiques.**]

Content and presentation of evidence elements :

- ADV_LLD.1.1C The presentation of the low-level design [refinement: **des fonctions cryptographiques]** shall be informal.
- ADV_LLD.1.2C The low-level design [refinement: **des fonctions cryptographiques]** shall be internally consistent.
- ADV_LLD.1.3C The low-level design [refinement: **des fonctions cryptographiques]** shall describe [refinement: the TSF => **les fonctions cryptographiques]** in terms of modules [refinement: **cryptographiques.**]
- ADV_LLD.1.4C The low-level design [refinement: **des fonctions cryptographiques]** shall describe the purpose of each module [refinement: **cryptographique.**]
- ADV_LLD.1.5C The low-level design [refinement: **des fonctions cryptographiques]** shall define the interrelationships between the modules [refinement: **cryptographique]** in terms of provided security functionality and dependencies on other modules [refinement: **cryptographique.**]
- ADV_LLD.1.6C The low-level design [refinement: **des fonctions cryptographiques]** shall describe how each [refinement: TSP-enforcing function => **fonction cryptographique]** is provided.
- ADV_LLD.1.7C The low-level design [refinement: **des fonctions cryptographiques]** shall identify all interfaces to the modules [refinement: of the TSF => **cryptographiques.**]

- ADV_LLD.1.8C The low-level design [refinement: **des fonctions cryptographiques**] shall identify which of the interfaces to the modules [refinement: of the TSF => **cryptographiques**] are externally visible.
- ADV_LLD.1.9C The low-level design [refinement: **des fonctions cryptographiques**] shall describe the purpose and method of use of all interfaces to the modules [refinement: of the TSF => **cryptographiques**], providing details of effects, exceptions and error messages, as appropriate.
- ADV_LLD.1.10C The low-level design [refinement: **des fonctions cryptographiques de soutien**] shall describe the separation of the TOE into [refinement: TSP-enforcing => **modules cryptographiques**] and other modules.

Evaluator action elements :

- ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADV_LLD.1.1E The evaluator shall determine that the low-level design [refinement: **des fonctions cryptographiques**] is an accurate and complete instantiation of the TOE security functional requirements [refinement: **de la classe FCS.**]

9.2.2. Class ALC : Life cycle support

ALC_TAT.1 Well-defined development tools

Developer action elements :

- ALC_TAT.1.1D The developer shall identify the development tools being used for [refinement: **les fonctions cryptographiques de**] the TOE.
- ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools [refinement: **des fonctions cryptographiques.**]

Content and presentation of evidence elements :

- ALC_TAT.1.1C All development tools used for implementation [refinement: **des fonctions cryptographiques**] shall be well-defined.
- ALC_TAT.1.2C The documentation of the development tools [refinement: **des fonctions cryptographiques**] shall unambiguously define the meaning of all statements used in the implementation [refinement: **des fonctions cryptographiques.**]

ALC_TAT.1.3C The documentation of the development tools [refinement: **des fonctions cryptographiques**] shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements :

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Copyright © Prim'X Technologies 2003, 2008.