Security BOX Enterprise

Cible de Sécurité

Version : **1.5**

Référence : **ARK/TSETA/Cible**

Date : **16/03/2012**

Table des matières

Liste des figures

Liste des tableaux

TERMINOLOGIE ET SIGLES UTILISES

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
Compte	Le compte d'un utilisateur est un ensemble de fichiers assurant le stockage sécurisé de la politique de sécurité et des données sensibles de l'utilisateur.
CRL	Certificate Revocation List (liste de certificats révoqués).
IGC	Infrastructure de Gestion de Clé
PKI	Public Key Infrastructure
Politique de sécurité	Ensemble des paramètres des fonctions de sécurité.
Porte-clés	Conteneur dans lequel les clés privées de l'utilisateur sont stockées. Ce conteneur peut être : - soit logiciel (c'est-à-dire un fichier), - soit matériel (une carte à puce ou un dispositif cryptographique USB).
Règle de sécurité	Attachée à un dossier, la règle de sécurité définit les utilisateurs autorisés à accéder au dossier et que leur rôle.

DOCUMENTS DE REFERENCE

[CC]	Common Criteria for Information Technology Security Evaluation, version 3.1 revision 3 - Part 1: Introduction and general model, ref. CCMB-2009-07-001 - Part 2: Security functional requirements, ref. CCMB-2009-07-002 - Part 3: Security assurance requirements, ref. CCMB-2009-07-003
[QUALIF_STD]	Référentiel général de sécurité - Processus de qualification d'un produit de sécurité – Niveau Standard Version 1.2.
[CRYPTO_STD]	Référentiel général de sécurité (RGS) Annexe B1 Mécanismes cryptographiques Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques Version 1.20 du 26 janvier 2010
[CLES_STD]	Référentiel général de sécurité (RGS) Annexe B2 Gestion des clés cryptographiques Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques Version 1.10 du 24 octobre 2008
[AUTH_STD]	Référentiel général de sécurité (RGS) Annexe B3 Authentification Règles et recommandations concernant les mécanismes d'authentification Version 1.00 du 13 janvier 2010

1. INTRODUCTION DE LA CIBLE DE SECURITE

1.1 Identification de la cible de sécurité

Titre :	Security BOX Enterprise – Cible de Sécurité
Référence :	ARK/TSETA/Cible
Version :	1.5

1.2 Identification de la cible d'évaluation (TOE)

Nom du produit :	Security BOX Enterprise pour poste de travail sous Microsoft Windows XP/Vista/7
Développeur :	Arkoon Network Security
Version :	8.0 (build 8.0.2.0)

1.3 Vue d'ensemble de la TOE

1.3.1 Type de TOE

La cible de l'évaluation est une application de chiffrement transparent de fichiers pour poste Windows.

1.3.2 Présentation de la TOE

1.3.2.1 Security BOX Enterprise

Security BOX *Enterprise* est un produit de sécurité pour poste de travail sous Windows qui préserve la confidentialité des données partagées, stockées ou échangées par voie de messagerie.

Il offre plus précisément les fonctions de sécurité suivantes :

- Le chiffrement en temps réel des fichiers, là où ils se trouvent, et de façon transparente pour l'utilisateur.
- Le chiffrement et la signature des courriers électroniques,
- Le chiffrement à la demande des fichiers, en vue d'un transfert par mail ou d'une sauvegarde sécurisée.
- L'effacement sécurisé et irréversible des données.
- La signature électronique de fichiers et de dossiers.
- Le chiffrement de disques virtuels.

Le produit intègre un outil permettant le paramétrage des fonctions de sécurité et l'administration des utilisateurs et de leurs clés cryptographiques.

La présente cible de sécurité concerne la fonction de chiffrement transparent de fichiers détaillée dans la suite de ce chapitre.

1.3.2.2 Chiffrement transparent de fichier

Security BOX préserve la confidentialité des fichiers sensibles de l'entreprise. Il en assure à cette fin le chiffrement en temps réel et "au fil de l'eau", de façon transparente tant pour l'utilisateur que pour ses applications bureautiques ou métier.

Le chiffrement s'effectue selon des règles définies par dossier : tout fichier créé ou déposé dans un "dossier sécurisé" est automatiquement chiffré sans la moindre interaction nécessaire de la part de l'utilisateur. L'emplacement, le nom et l'extension du fichier restent inchangés.

Security BOX permet également le partage de données confidentielles entre plusieurs collaborateurs. La « règle de sécurité » spécifiée sur le dossier définit alors les utilisateurs autorisés à lire et modifier les fichiers stockés dans le dossier.

Security BOX peut sécuriser :

- Un dossier local à l'ordinateur personnel de l'utilisateur ;
- Un support amovible (une clé USB) en totalité ou partiellement (un ou plusieurs sous-dossiers).
- Un dossier partagé sur un serveur de fichiers.

Quand une règle de sécurité est définie sur un dossier, elle est appliquée de façon récursive à tous ses éventuels sous-dossiers. Il est néanmoins possible de définir une règle différente sur un sous-dossier bien déterminé.

Une fois chiffré, un fichier ne peut être lu, modifié voire effacé que par l'un des utilisateurs autorisés par la règle de sécurité. Quand un utilisateur autorisé ouvre un fichier chiffré :

- Le contenu du fichier est automatiquement déchiffré et fourni « en clair » à l'application ayant ouvert le fichier.
- Les éventuels fichiers temporaires créés dans le dossier sont automatiquement chiffrés.
- Lorsque l'utilisateur enregistre le fichier après l'avoir modifié, la nouvelle version du fichier est automatiquement chiffrée.
- Toutes les lectures/écritures et chiffrement/déchiffrement de donnée s'effectuent au « fil de l'eau » et en mémoire : aucune copie en clair du fichier n'est créée.

Techniquement, chaque fichier est chiffré à l'aide d'une clé de chiffrement symétrique (AES) qui est propre au fichier. Cette clé est elle-même chiffrée avec la clé publique de chiffrement (RSA) de chaque collaborateur autorisé.

Security BOX assure également le chiffrement du fichier d'échange du système (le swap) dans lequel peuvent persister des résidus de données confidentielles.

1.3.2.3 Comment Security BOX fonctionne-t-il ?

Security BOX s'intègre au noyau Windows et s'insère dans l'architecture des systèmes de fichier (« FileSystem ») selon une technique de « filtre » présentée par le schéma suivant :

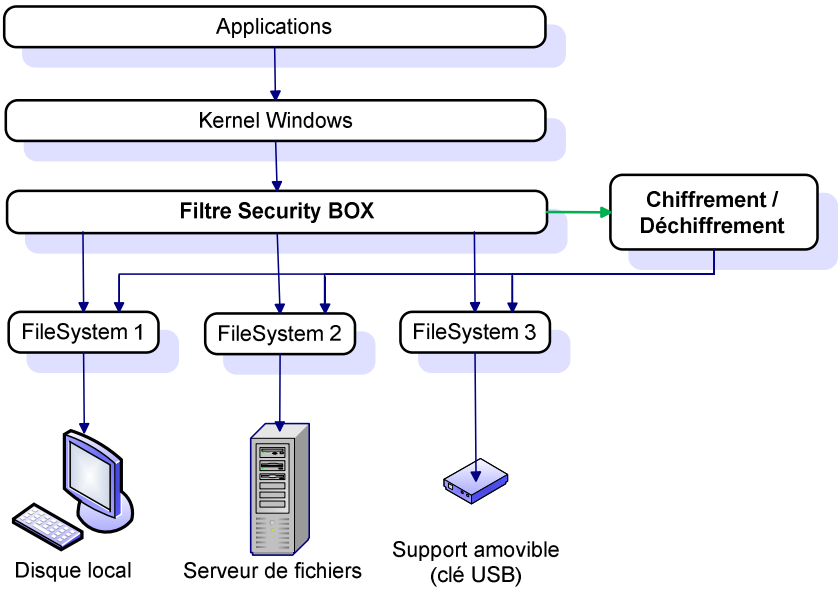

Figure 1 : Fonctionnement de Security BOX

Security BOX intercepte ainsi toutes les requêtes d'ouverture/création/lecture/écriture/effacement de fichier adressées aux systèmes de fichier (« FileSystem ») qu'il filtre.

Avant de retransmettre ces requêtes au système de fichier sous-jacent concerné, Security BOX contrôle les permissions de l'utilisateur sur chaque fichier qu'il ouvre, crée ou efface ;

- Si l'utilisateur n'est pas autorisé : la requête est refusée (avec un code d'erreur « Access Denied »).
- Si l'utilisateur est bien autorisé :
  - Security BOX déchiffre un bloc lu lorsqu'il s'agit d'une lecture d'un fichier chiffré,
  - ou chiffre un bloc écrit lorsqu'il s'agit d'une écriture d'un fichier chiffré.

Les chiffrements et déchiffrements s'effectuent par bloc (cluster) entier correspondant à un bloc lu ou écrit sur le disque par le système de fichier sous-jacent (autrement dit, Security BOX n'induit pas d'accès disque supplémentaire pour la lecture ou l'écriture du contenu d'un fichier).

1.3.3 Concepts de base

Cette section définit les différents éléments concernés par le déploiement du produit : politique de sécurité, règle de sécurité, compte utilisateur.

1.3.3.1 Politique de sécurité

La politique de sécurité est l'ensemble des paramètres nécessaires aux fonctions de sécurité offertes par le produit. Elle comprend essentiellement les paramètres de fonctionnement des différents modules de Security BOX, comme par exemple :

- Les règles de changement du code secret (fréquence, syntaxe).
- Les annuaires LDAP à consulter pour rechercher le certificat d'un collaborateur.
- Les règles de gestion et les points de distribution des listes de révocation.
- Le(s) point(s) de distribution des mises à jour de la politique.
- Les algorithmes de chiffrement.
- L'autorisation éventuellement accordée à l'utilisateur de modifier ces paramètres localement sur son poste de travail, voire le fait de les cacher à l'utilisateur.
- D'éventuels dossiers personnels de l'utilisateur à chiffrer (c'est-à-dire des règles de sécurité dite "personnelles" tel qu'elles sont définies au § 1.3.3.3).

La politique comprend également :

- Les certificats d'autorité de confiance.
- Les certificats de recouvrement.

La politique est définie à l'aide de l'outil d'administration Security BOX Manager. L'administrateur peut décider de la cacher sur le poste de travail, ou d'autoriser l'utilisateur à la consulter, voire à la modifier.

1.3.3.2 Compte utilisateur et mode d'authentification

Chaque utilisateur possède un compte qui est un ensemble de fichiers assurant le stockage de la politique et de ses données sensibles (autorités et certificats de confiance, liste de certificats révoqués, éventuellement des clés privées, etc.).

La façon dont est protégé ce compte dépend du mode d'authentification de l'utilisateur.

Les deux modes d'authentification possibles sont :

1. à l'aide d'un identifiant et d'un mot de passe (login/mot de passe)

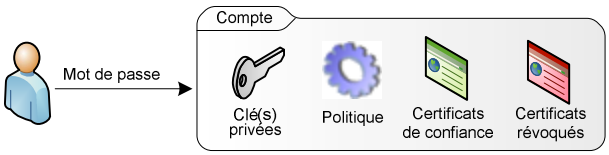

Figure 2 : Compte "mot de passe"

   - o les clés privées de l'utilisateur, ainsi que la politique de sécurité, sont stockées dans le compte de l'utilisateur, lequel est protégé de manière cryptographique par le mot de passe ;
   - o les calculs à clé privée sont effectués de façon logicielle.

2. à l'aide d'une carte à puce (ou d'un dispositif USB) et de son code PIN :

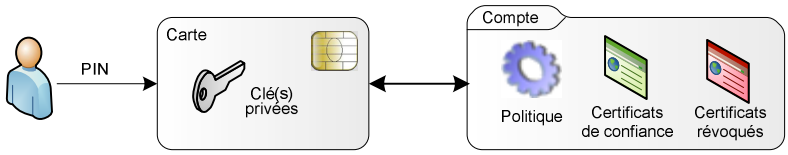

Figure 3 : Compte "carte ou token USB"

   - o les clés privées de l'utilisateur sont stockées dans la carte (ou le dispositif USB) ;
   - o la politique de sécurité est stockée dans le compte de l'utilisateur, qui est protégé de manière cryptographique par la carte ;
   - o les calculs à clé privée sont effectués par la carte.

Sur un poste, il est possible d'autoriser qu'un seul de ces deux modes d'authentification, ou les deux mais si les deux modes cohabitent, ils s'appuient alors sur des comptes, et donc des clés, différentes.

Dans la suite du document, le terme porte-clés désigne le conteneur dans lequel les clés privées de l'utilisateur sont stockées : ce conteneur est le compte de l'utilisateur en cas d'authentification par mot de passe, ou le cas échéant sa carte à puce.

1.3.3.3 Règle de sécurité

Une règle de sécurité s'applique à un dossier et définit les utilisateurs autorisés à accéder à ce dossier.

Le produit propose deux types de règles :

1. La règle « personnelle » concerne uniquement un utilisateur. Elle fait partie de la politique de sécurité (et est donc stockée dans le compte de l'utilisateur). Elle permet de spécifier des dossiers par défaut à sécuriser pour « soi-même », et peut-être être définie à l'aide d'une variable d'environnement ou d'un « CSIDL » s'il s'agit d'un dossier logique géré par Windows tel que le cache d'Internet Explorer.

2. La règle « partagée » s'applique à un dossier partagé. Elle est stockée dans un fichier technique caché dans le dossier en question. En plus de la liste des utilisateurs autorisés, elle précise pour chacun d'entre eux son rôle qui peut être :
   - « propriétaire » : il peut alors modifier la règle et accéder au contenu du dossier.
   - « collaborateur » : il ne peut qu'accéder au contenu du dossier, et ne peut pas modifier la règle.

1.3.3.4 Configuration du poste

En plus de la politique de sécurité, il existe un fichier de configuration du poste de travail. Ce fichier (au format .INI), permet de définir le fonctionnement du produit indépendamment de toute session Security BOX ouverte par un utilisateur.

Ce fichier de configuration comprend par exemple :

- Le ou les modes d'authentification acceptés : carte à puce uniquement, mot de passe uniquement, les deux.
- Pour le mode carte à puce ; la librairie PKCS#11 à utiliser.
- L'interdiction ou l'autorisation de créer un nouveau compte.
- Si la création de compte est autorisée :
  - Politique modèle à appliquer (y compris certificats de confiance).
  - Syntaxe d'un mot de passe.

Ces paramètres peuvent être administrés à l'aide de politique de groupe Windows (GPO).

1.3.3.5 Rôles

Il existe quatre rôles mettant en œuvre les fonctionnalités du produit.

L'administrateur de la sécurité (administrateur Security BOX) définit la politique de sécurité. Si les comptes des utilisateurs sont gérés par Security BOX Manager, l'administrateur de la sécurité créé également ces comptes des utilisateurs.

L'administrateur système (administrateur Windows) se charge de l'installation à partir d'un « master » préparé par l'administrateur de la sécurité. Ce master comprend un fichier de configuration globale. Si les clés des utilisateurs sont fournies par une IGC d'entreprise, le master comprend également une politique "modèle" utilisée pour la création des comptes directement sur le poste de travail.

Un utilisateur est **propriétaire** de la règle de sécurité définie sur un dossier s'il peut la modifier, c'est-à-dire ajouter/supprimer des collaborateurs ou changer leur rôle. Le propriétaire peut naturellement lire, modifier, renommer voire effacer[1] tout fichier ou sous-dossier stocké dans le dossier sécurisé.

Il peut également « désécuriser » le dossier, c'est-à-dire supprimer la règle de sécurité et remettre en clair (déchiffrer) tous les fichiers chiffrés présents dans le dossier.

Un utilisateur est un simple **collaborateur** sur un dossier sécurisé s'il ne peut en modifier la règle de sécurité : il ne peut que la consulter. Un collaborateur peut lire, modifier, renommer et éventuellement effacer[1] tout fichier ou sous-dossier stocké dans le dossier sécurisé.

[1] Un utilisateur peut effacer un fichier sur lequel il n'a pas les autorisations Security BOX via une fonction "avancée" d'effacement, à condition toutefois que l'administrateur de la sécurité lui ait donné accès à cette fonction.

Cette fonction d'effacement doit être réservée à certains utilisateurs dans le but de pouvoir supprimer des vieux fichiers ou dossiers en cas d'absence des utilisateurs historiques autorisés. Elle ne permet en aucun cas d'avoir accès à la donnée confidentielle chiffrée : elle permet uniquement de l'effacer.

1.3.4 Cas d'usage de déploiement

Ce paragraphe décrit les principaux cas d'usage de déploiement de la politique de sécurité, des clés et des comptes utilisateur.

1.3.4.1 Gestion des clés et des cartes à puce par une IGC

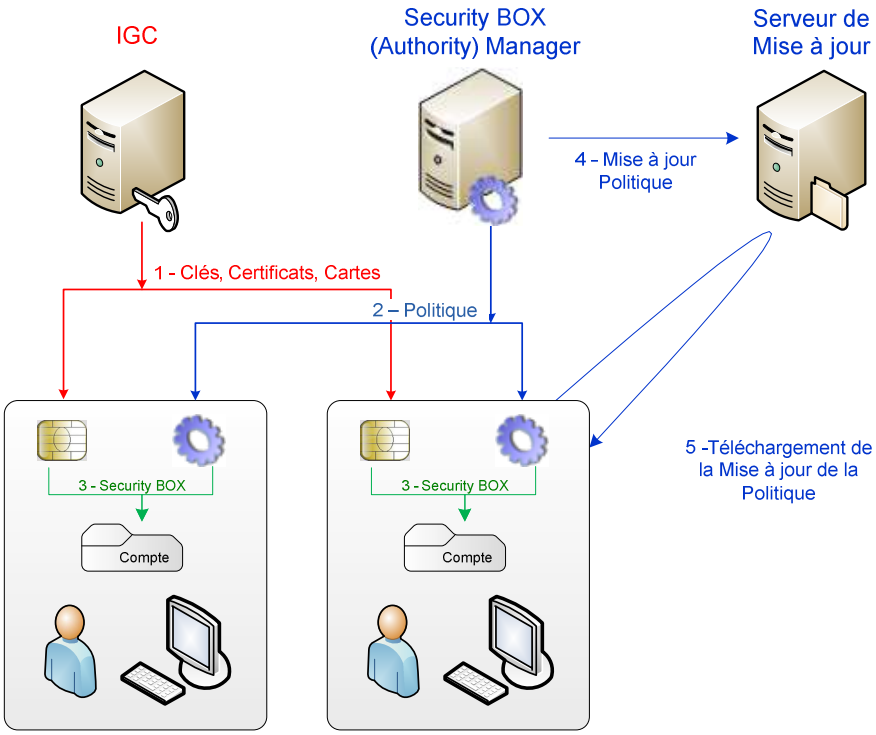

Figure 4 : Clés et cartes fournies par une IGC

1) L'infrastructure de gestion de clé de l'entreprise (IGC) assure :
   - o le tirage et la certification des clés de l'utilisateur (et éventuellement leur recouvrement) ;
   - o et l'installation de ces clés dans une carte à puce.
2) A l'aide de l'outil d'administration Security BOX Manager, l'administrateur définit la politique de sécurité et la déploie sur les postes des utilisateurs (sous la forme d'une politique modèle).
3) L'utilisateur reçoit sa carte à puce (laquelle contient donc déjà les clés), et dès qu'il l'insère sur son poste de travail, son compte Security BOX est automatiquement créé et alimenté avec la politique modèle issue de Security BOX Manager.
4) Quand l'administrateur est amené à modifier la politique de sécurité :
   - o il génère un fichier de mise à jour et le signe afin d'en assurer l'intégrité et l'authenticité ;
   - o et le publie sur un serveur de mise à jour (LDAP, HTT¨P, ou simple serveur de fichiers).
5) Régulièrement, Security BOX interroge le serveur de mise à jour, et si une nouvelle mise à jour est disponible, il la télécharge puis l'applique de façon transparente pour l'utilisateur.

1.3.4.2 Gestion des comptes avec Security BOX Manager

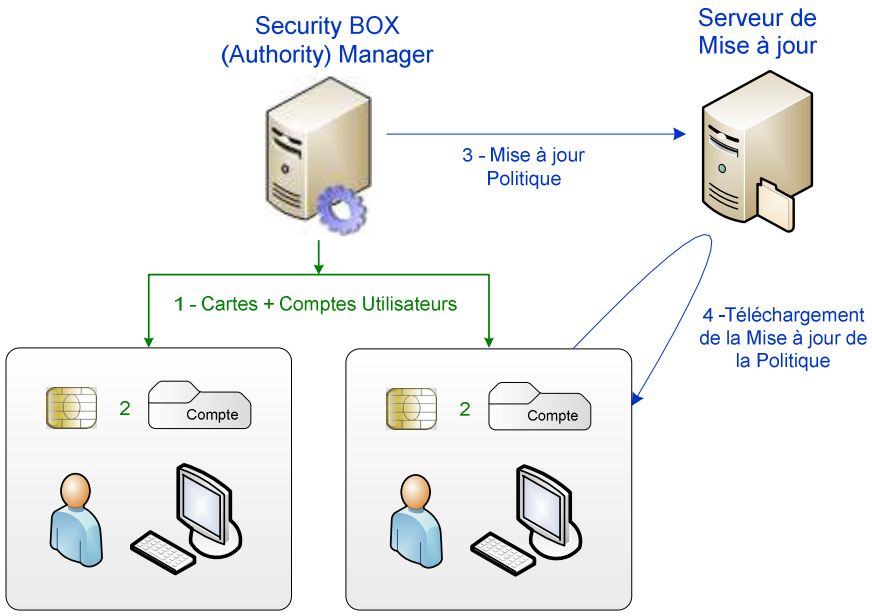

Figure 5 : Clés, cartes et comptes fournis par Security BOX Manager

1) L'outil d'administration Security BOX Manager assure :
   - o le tirage et la certification des clés de l'utilisateur ;
   - o l'installation de ces clés dans une carte à puce ou un dispositif USB ;
   - o la définition de la politique de sécurité ;
   - o la création du compte de l'utilisateur.
2) L'utilisateur reçoit sa carte à puce et son compte Security BOX prêts à l'emploi.
3) La mise à jour de la politique de sécurité s'effectue comme dans le précédent cas d'usage :
   - o L'administrateur génère un fichier de mise à jour et le signe afin d'en assurer l'intégrité et l'authenticité ;
   - o et le publie sur un serveur de mise à jour (LDAP, HTT¨P, ou simple serveur de fichiers).
4) Régulièrement, Security BOX interroge le serveur de mise à jour, et si une nouvelle mise à jour est disponible, il la télécharge puis l'applique de façon transparente pour l'utilisateur.

1.3.4.3 Autres modes de déploiement possibles

Security BOX permet également les modes de déploiement de clé suivants :

- L'IGC de l'entreprise fournit un fichier de clés (format PKCS#12) et Security BOX se charge d'importer la ou clés de ce fichier dans le porte-clés de l'utilisateur (dans le compte ou dans la carte à puce).
- Security BOX tire lui-même les clés de l'utilisateur et l'utilisateur se charge de les faire certifier auprès de son IGC.

Ces deux modes de déploiement ne sont pas dans le périmètre de la cible.

1.3.4.4 Mise à jour du produit

Le produit ne dispose pas de fonctionnalité particulière de mise à jour. Il peut néanmoins être mis à jour avec les mécanismes standards de déploiement de produits.

1.3.5 Schéma de sécurité

1.3.5.1 Répartition des clés

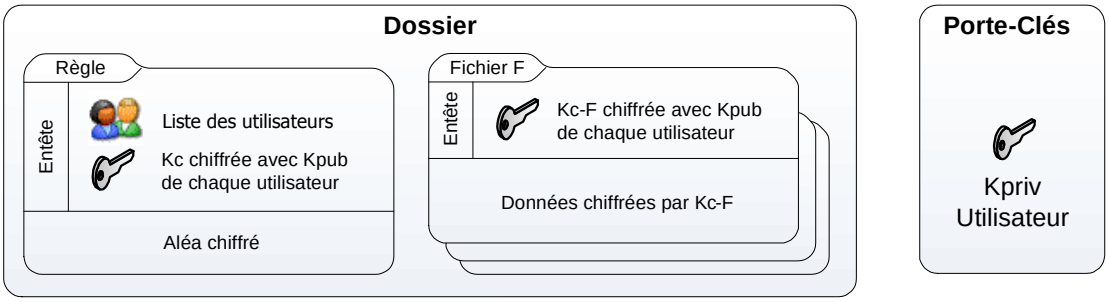

Figure 6 : Schéma de répartition des clés

Le porte-clés de l'utilisateur contient la ou les clés privées de l'utilisateur.

Dans un dossier sécurisé :

- La règle comporte la liste des utilisateurs autorisés. C'est un fichier chiffré à part entière qui comporte un aléa permettant d'assurer l'intégrité de la liste des utilisateurs. La clé de chiffrement Kc de ce fichier est stockée chiffrée avec la clé publique de chaque utilisateur autorisé.
- Chaque fichier est chiffré avec une clé symétrique Kc-F qui lui est propre. Cette clé est stockée chiffrée avec la clé publique de chaque utilisateur autorisé, et le tout est stocké en entête du fichier. La liste de ces utilisateurs est déterminée au moment de la création du fichier. Quand la règle de sécurité du dossier est modifiée :
  - Si un utilisateur est ajouté, alors il est simplement ajouté dans l'entête la clé Kc-F chiffrée avec la clé publique du nouvel utilisateur.
  - Si un utilisateur est retiré de la règle, alors une nouvelle clé de chiffrement est tirée, le fichier est transchiffré avec cette nouvelle clé, laquelle est stockée chiffrée avec la clé publique des utilisateurs de la nouvelle liste.

Notes d'implémentation :

- La clé de chiffrement d'un fichier sécurisé est également chiffrée avec la clé publique des certificats de recouvrement définis dans la politique de sécurité. La génération et la certification des clés de recouvrement sont assurées par l'IGC.
- La non révocation des clés des collaborateurs est contrôlée :
  - lors de la création de tout nouveau fichier dans le dossier sécurisé : le fichier n'est alors pas chiffré pour l'utilisateur révoqué.
  - Lors de l'application d'une règle modifiée : si un utilisateur révoqué était autorisé à déchiffrer un fichier, alors cet utilisateur est supprimé de la liste des utilisateurs autorisés et le fichier est transchiffré.
- Il est impossible par un paramètre de la politique de sécurité d'interdire à un utilisateur dont la clé est révoquée l'ouverture d'un fichier chiffré.

1.3.5.2 Automate d'état

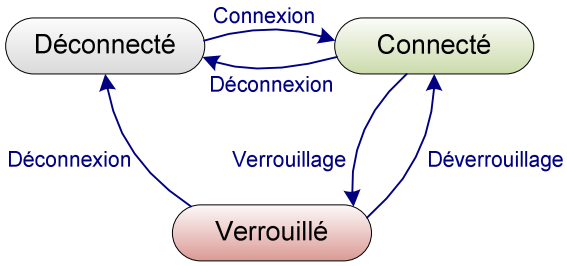

Figure 7 : Automate d'état

Etat	Description
Connecté	Le compte de l'utilisateur est déverrouillé. Ses clés sont disponibles. Ses fichiers confidentiels peuvent être ouverts.
Verrouillé	Le compte de l'utilisateur est verrouillé en lecture seule. Ses clés ne sont plus disponibles. Ses fichiers confidentiels ne peuvent plus être ouverts. Ses fichiers confidentiels qui ont été ouverts avant le verrouillage restent ouverts. Le cache des contextes cryptographiques des règles et des fichiers accédés est conservé dans l'état.
Déconnecté	Le compte de l'utilisateur est fermé. Ses clés ne sont pas/plus disponibles. Ses fichiers confidentiels ne peuvent pas/plus être ouverts. Ses fichiers confidentiels ouverts avant la déconnexion restent ouverts Le cache des contextes cryptographiques des règles et des fichiers accédés est purgé.

Tableau 1 : Description des états de l'automate

1.3.6 Environnement matériel et logiciel de la TOE

Pour que le produit Security BOX puisse fonctionner correctement, l'environnement suivant est requis :

- Un poste de travail utilisateur sous Microsoft Windows XP, Vista ou Seven, sur lequel Security BOX est installé ;
- Un porte-clés matériel offrant une interface PKCS#11 pour le stockage des clés, dans le cas d'utilisation d'un porte-clés matériel ;
- Un poste administrateur sur lequel est installé Security BOX Manager pour la gestion des de la politique de sécurité ;
- Un serveur de fichier disponible en réseau offrant des dossiers partagés (CIFS, DFS, Netware) ;
- Un serveur HTTP(s), LDAP(s) ou de fichier pour la mise à jour de la politique de sécurité
- Une IGC, basée sur Security BOX Manager ou une infrastructure tierce.

1.4 Description de la TOE

1.4.1 Périmètre de la TOE

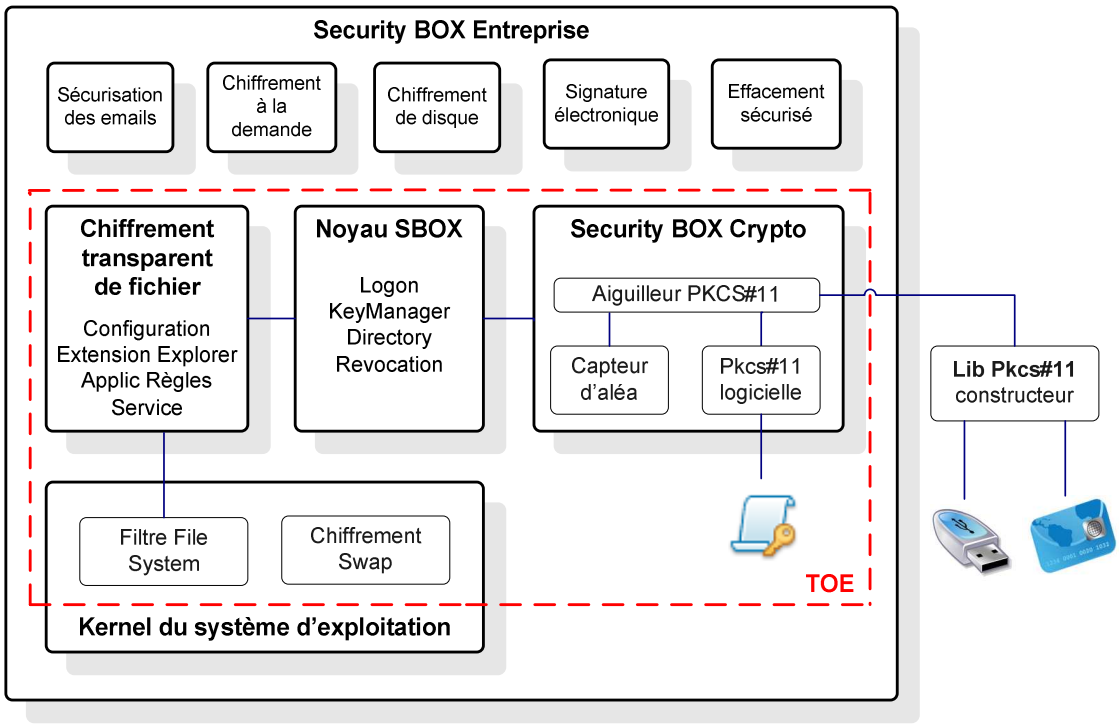

Figure 8 : Périmètre de la TOE

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

- Le module « Security BOX Crypto » est une interface cryptographique conforme au standard Pkcs#11. Les clés de l'utilisateur peuvent être stockées dans un fichier (implémentation logicielle), soit dans une carte à puce ou un dispositif matériel cryptographique.

  Il est à noter qu'une version précédente de ce module a été certifiée EAL4+ en 2004 (certificat numéro 2004/03).

- Le « noyau Security BOX » assure l'authentification de l'utilisateur, surveille l'inactivité du poste, offre des fonctions de haut de niveau d'accès aux clés, contient un annuaire de certificats de confiance, et contrôle la non-révocation des certificats utilisés.

- Le composant « Chiffrement transparent » assure

  o la définition des règles de sécurité (via notamment une extension de l'explorateur)

  o et l'application de ces règles.

- Les composants installés au niveau du noyau du système d'exploitation (mode kernel) assurent le chiffrement proprement-dit des fichiers et du swap.

Les éléments suivants sont hors évaluation :

- La librairie PKCS#11 du constructeur du dispositif matériel ;
- Le système d'exploitation Microsoft Windows.

Le périmètre physique correspond au logiciel fourni sous la forme d'un paquet d'installation auto-extractible.

1.4.2 Interfaces logicielles

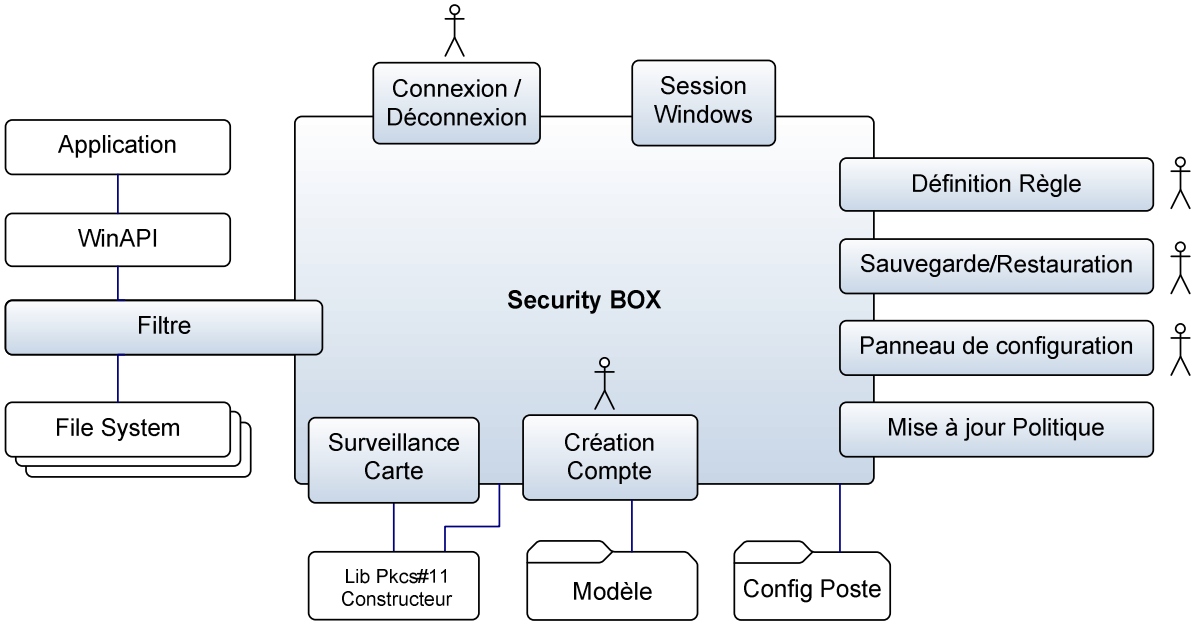

Figure 9 : Interfaces logicielles

Le tableau suivant décrit les interfaces logicielles :

Interface	Description
Filtre	Intercepte et filtre les appels au système de fichier (voir § 1.3.2.3).
Connexion/ Déconnexion	IHM assurant la connexion/déconnexion/verrouillage de la session Security BOX (voir automate d'état au § 1.3.5.1).
Session Windows	Interface permettant d'être notifié des changements d'état de la session Windows : Verrouillage / Déverrouillage / Fermeture de la session Windows ou Activation / Reprise de l'économiseur d'écran.
Définition Règle	IHM intégrée à l'explorateur permettant de définir/modifier/appliquer une règle de sécurité sur un dossier.
Sauvegarde / Restauration	Assure la sauvegarde ou la restauration d'un fichier chiffré. Fonction accessible par l'explorateur ou par un outil en ligne de commande.
Panneau de configuration	IHM permettant de définir/modifier la politique de sécurité, active si l'administrateur l'a autorisée.
Mise à jour Politique	Assure le téléchargement de la politique de sécurité par les protocoles HTTP ou LDAP.
Création compte	IHM assurant la création du compte d'un utilisateur à partir d'un modèle de compte
Surveillance carte	Interface assurant la détection de l'insertion ou de l'arrachage de la carte
Config Poste	Configuration du poste (fichier ou GPO).
Modèle	Modèle utilisé par lors de la création d'un compte
Lib Pkcs#11 constructeur	Librairie d'interface avec l'éventuelle carte à puce ou dispositif cryptographique.

Tableau 2 : Description des interfaces logicielles

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

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

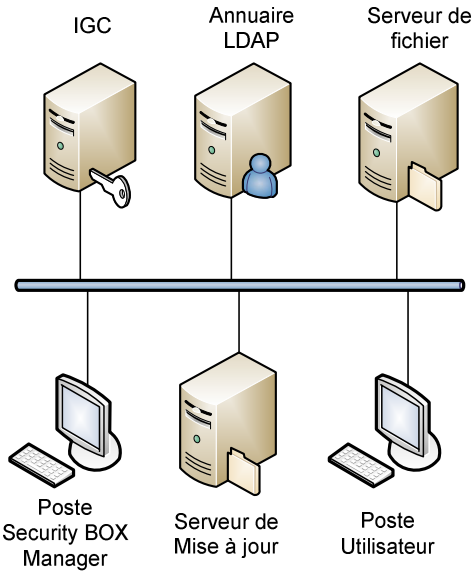

Figure 10 : Plateforme de test pour l'évaluation de la TOE

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

- Un poste utilisateur sous les systèmes d'exploitation Microsoft suivants : Windows XP Professional Service Pack 3, Windows Vista Entreprise Service Pack 2 et Windows Seven Enterprise. Sur ce poste est installé le logiciel Security BOX version 8.0 (build 8.0.2.0).
- Un dispositif matériel Aladdin Pro eToken 64k.
- Un poste d'administration sous le système d'exploitation Microsoft Windows VISTA Service Pack 2. Sur ce poste est installé le logiciel Security BOX Manager version 8.0 (build 8.0.1.0).
- Une IGC, pour la production des clés et des cartes à puce.
- Un serveur de fichier sous le système d'exploitation Microsoft Windows Serveur 2008 Standard Edition Service Pack 2. Ce serveur partage via le protocole CIFS des dossiers hébergés sur une partition NTFS.
- Un annuaire LDAP pour la publication des certificats X.509 des collaborateurs.
- Un serveur pour le déploiement des mises à jour de la politique de sécurité.

2. DECLARATION DE CONFORMITE

2.1 Conformité aux Critères communs

Le présent document est conforme aux exigences des Critères Communs version 3.1 revision 3 [CC].

Toutes les exigences de sécurité présentes dans cette cible sont conformes aux parties 2 et 3 des Critères Communs [CC].

2.2 Conformité à un profil de protection

Cette cible de sécurité ne revendique pas de conformité à un profil de protection.

2.3 Conformité à un paquet d'assurance

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

3. DEFINITION DU PROBLEME DE SECURITE

Ce chapitre précise les aspects de sécurité de l'environnement dans lequel il est prévu d'utiliser la TOE.

3.1 Hypothèses

3.1.1 Hypothèses sur l'environnement physique de la TOE

H.ENV_OPERATIONNEL

L'environnement opérationnel du poste de l'utilisateur ne permet pas à un attaquant d'accéder au poste lorsque la session Security BOX est ouverte par un utilisateur autorisé.

3.1.2 Hypothèses sur l'environnement organisationnel

H.MOT_DE_PASSE

Les mots de passe sont soumis à une politique interdisant l'utilisation de mots de passe faibles.

3.1.3 Hypothèses sur les intervenants

H.ADMIN_SYSTEME_CONFIANCE

L'administrateur système en charge de l'installation et de la maintenance de l'application et du système d'exploitation est considéré de confiance.

H.ADMIN_SECURITE_CONFIANCE

L'administrateur de sécurité en charge de la définition de la politique de sécurité sur le poste ou via l'application Security BOX Manager est considéré de confiance.

3.1.4 Hypothèses sur les systèmes hors-TOE

H.PKI

Les bi-clés et les certificats utilisés sont tous générés par une infrastructure de confiance. Les mécanismes de génération et de distribution des clés sont supposés conformes aux exigences du référentiel [CRYPTO_STD].

H.SECURITY_BOX_MANAGER

Les "modèles" de politiques sont gérés hors de la TOE par l'application Security BOX Manager ou Security BOX Authority Manager qui sont considérées de confiance pour cette évaluation.

H.TOKEN_FIABLE

Dans le mode de déploiement avec porte-clés matériel, il est considéré que ce dispositif assure la protection en confidentialité et en intégrité des bi-clés et des certificats stockés.

H.MACHINE_HOTE_CONFIANCE

La machine hôte sur laquelle la TOE s'exécute est considérée saine.

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

3.2 Menaces

3.2.1 Biens sensibles

3.2.1.1 Données utilisateur protégées par la TOE (User Data)

Le **contenu sensible des fichiers** de l'utilisateur doit être protégé en confidentialité. Ces informations sont stockées soit dans le fichier sur disque ou dans la mémoire vive du poste lors du traitement du fichier.

La **clé privée de l'utilisateur** qui lui permet d'accéder aux clés secrètes de chiffrement des dossiers et ainsi de déchiffrer ses fichiers doit être protégée en confidentialité et intégrité. Dans le cas du porte-clés matériel, cette clé privée est isolée dans le dispositif matériel. Dans le cas du porte-clés logiciel, cette clé est gérée par l'application Security BOX.

3.2.1.2 Données sensibles de la TOE (TSF Data)

Les **comptes utilisateurs** doivent être protégés en intégrité et en confidentialité.

Les **règles de sécurité partagées** sur les dossiers qui permettent de définir les utilisateurs ayant l'autorisation d'accéder au dossier concerné doivent être protégées en intégrité.

Les **clés secrètes AES de chiffrement d'un fichier** doivent être protégées en intégrité et en confidentialité.

La **politique téléchargée** sur un serveur de mise à jour des politiques doit être protégée en intégrité.

3.2.1.3 Synthèse des besoins de sécurité

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

Biens sensibles	Confidentialité	Intégrité
Contenu des fichiers	Oui	
Clé privée de l'utilisateur	Oui	Oui
Compte utilisateur	Oui	Oui
Règle de sécurité partagée		Oui
Clé secrète AES de chiffrement d'un fichier	Oui	Oui
Politique téléchargée		Oui

Tableau 3 : Synthèse des besoins de sécurité

3.2.2 Liste des menaces

Les agents menaçants pour la TOE sont:

- Un **Voleur** qui subtiliserait le poste sur lequel les fichiers à protéger sont stockés,
- Un **Utilisateur non autorisé** qui aurait accès aux fichiers (accès local au disque ou accès au partage) mais qui ne serait pas autorisé à accéder au contenu du fichier,
- Une **Personne malveillante** qui dérouterait le point de distribution d'une mise à jour de la politique de sécurité afin de délivrer une politique illicite.

M.ACCES_ILLICITE_COMPTE_UTILISATEUR

Un attaquant (voleur ou utilisateur non autorisé) réussi à accéder illicitement au contenu d'un compte utilisateur afin d'accéder par la suite aux fichiers de cet utilisateur.

M.ALTERATION_REGLES_PARTAGEES

Un attaquant (voleur ou utilisateur non autorisé) réussit à modifier illicitement une règle partagée au niveau d'un dossier afin de s'octroyer les droits d'accès à un fichier de ce dossier.

M.ACCES_ILLICITE_CLES_CHIFFREMENT_FICHIER

Un attaquant (voleur ou utilisateur non autorisé) réussi à accéder illicitement à la clé de chiffrement d'un fichier afin d'accéder par la suite à ce fichier.

M.ALTERATION_POLITIQUE_TELECHARGEE

Une personne malveillante ayant accès au lien utilisé pour la mise à jour de la politique modifie la politique téléchargée.

3.3 Politique de sécurité de l'organisation (OSP)

3.3.1 Protection des données utilisateurs

P.PROTECTION_FICHIERS

La TOE doit assurer la protection en intégrité et confidentialité des fichiers sécurisés et ne permettre leur chiffrement (pour les opérations d'écriture et de modification) et leur déchiffrement (pour les opérations de lecture) qu'aux utilisateurs (Propriétaires ou Collaborateurs) explicitement autorisés.

P.PROTECTION_SWAP

La TOE doit chiffrer le contenu du fichier d'échange du système (swap).

P.PROTECTION_PORTE-CLES_LOGICIEL

Dans le mode de déploiement porte-clés logiciel, la TOE doit assurer la protection en confidentialité et en intégrité des bi-clés et des certificats stockés.

P.MODE_AUTHENTIFICATION

La TOE doit empêcher l'utilisateur de mettre en œuvre un autre mode d'authentification que celui spécifié par l'administrateur de la sécurité.

P.CLOISONNEMENT_SESSION

La TOE doit cloisonner les sessions Security BOX; c'est-à-dire la portée d'une session Security BOX doit être restreinte à une session Windows.

P.EFF_RESIDUS

La TOE doit effacer les clés stockées en mémoire à la fermeture de la session Security BOX.

3.3.2 Administration de la TOE

P.GESTION_REGLES

La TOE doit offrir aux Propriétaires une interface de gestion des règles de sécurité des fichiers.

P.ROLES

La TOE doit permettre de distinguer le rôle de Propriétaire et de Collaborateur et doit appliquer en conséquence les restrictions d'accès aux règles.

P.JOURNALISATION

La TOE doit générer des journaux d'évènements en rapport avec son fonctionnement dans le journal d'audit du système d'exploitation. Ensuite, ces journaux doivent pouvoir être consultés conformément à la politique de sécurité en vigueur dans l'organisation.

P.SEPARATION_ROLES

L'accès aux fonctions d'administration système de la machine hôte est restreint aux seuls administrateurs de celle-ci (séparation des rôles entre l'utilisateur et l'administrateur).

3.3.3 Cryptographie

P.GENERATION_CLES_CHIFFREMENT_FICHIERS

La TOE doit générer les clés de chiffrement différentes pour chaque fichier contenant des informations sensibles.

P.CRYPTO

Tous les mécanismes cryptographiques présents dans la TOE doivent être conformes aux exigences du référentiel cryptographique de l'ANSSI [CRYPTO_STD]. La gestion des clés cryptographiques présente dans la TOE doit être conforme aux exigences du référentiel cryptographique de l'ANSSI [CLES_STD].

3.3.4 Politique de Sécurité du Système d'Information (PSSI)

P.PSSI

Le responsable sécurité de l'organisme considéré est en charge de définir la politique de sécurité du système d'information en respectant l'état de l'art.

Les administrateurs de l'organisme considéré sont en charge de l'application de cette politique de sécurité.

Cette politique doit notamment prévoir que les postes non équipés de Security BOX n'aient pas accès aux dossiers confidentiels partagés sur un serveur, afin qu'un utilisateur ne puisse pas provoquer un déni de service en altérant, par inadvertance ou par malveillance, les fichiers protégés par le produit.

L'utilisateur suit la politique de sécurité en vigueur dans l'organisme considéré.

4. OBJECTIFS DE SECURITE

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

4.1 Objectifs de sécurité pour la TOE

4.1.1 Protection des données utilisateurs

OT.AUTHENTIFICATION

La TOE doit authentifier les utilisateurs pour leur donner accès à leur compte.

La TOE doit également empêcher l'utilisateur de mettre en œuvre un autre mode d'authentification que celui spécifié par l'administrateur de la sécurité.

OT.PROTECTION_FICHIERS

La TOE doit protéger les fichiers des dossiers sécurisés et ne permettre leur chiffrement (pour les opérations d'écriture et de modification) et leur déchiffrement (pour les opérations de lecture) qu'aux utilisateurs (Propriétaires ou Collaborateurs) explicitement autorisés

OT.PROTECTION_SWAP

La TOE doit chiffrer le contenu du fichier d'échange du système (swap).

OT.PROTECTION_COMPTES_UTILISATEURS

La TOE doit chiffrer et sceller les fichiers contenant les comptes utilisateurs.

OT.PROTECTION_REGLES_PARTAGEES

La TOE doit assurer l'intégrité du contenu des règles de sécurité partagées.

OT.PROTECTION_CLE

La TOE doit protéger les clés de chiffrement des fichiers.

OT.CLOISONNEMENT_SESSION

La TOE doit cloisonner les sessions Security BOX; c'est-à-dire la portée d'une session Security BOX doit être restreinte à une session Windows.

OT.EFF_RESIDUS

La TOE doit effacer les clés stockées en mémoire à la fermeture de la session Security BOX.

4.1.2 Administration de la TOE

OT.GESTION_REGLES

La TOE doit offrir aux Propriétaires une interface de gestion des règles de sécurité.

OT.ROLES

La TOE doit permettre de distinguer le rôle de Propriétaire et de Collaborateur et doit appliquer en conséquence les restrictions d'accès aux règles.

OT.VERIFICATION_POLITIQUE

La TOE doit vérifier l'intégrité et l'authenticité de la politique téléchargée.

OT.JOURNALISATION

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

4.1.3 Génération des clés cryptographiques

OT.GENERATION_CLES_CHIFFREMENT_FICHIERS

La TOE doit générer les clés de chiffrement des fichiers en conformité avec les exigences de référentiel [CRYPTO_STD].

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

4.2.1 Objectifs sur l'environnement physique de la TOE

OE.ENV_OPERATIONNEL

L'environnement opérationnel du poste de l'utilisateur ne doit pas permettre à un attaquant d'accéder au poste lorsque la session Security BOX est ouverte par un utilisateur autorisé.

4.2.2 Objectifs sur les intervenants

OE.ADMIN_SYSTEME_CONFIANCE

L'administrateur système en charge de l'installation de l'application et de ses fichiers de configuration (notamment le fichier de "modèles") est considéré de confiance.

OE.ADMIN_SECURITE_CONFIANCE

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

OE.SEPARATION_ROLES

L'accès aux fonctions d'administration système de la machine hôte est restreint aux seuls administrateurs de celle-ci (séparation des rôles entre l'utilisateur et l'administrateur).

OE.PSSI

Le responsable sécurité de l'organisme considéré est en charge de définir la politique de sécurité du système d'information en respectant l'état de l'art.

Les administrateurs de l'organisme considéré sont en charge de l'application de cette politique de sécurité.

Cette politique doit notamment prévoir que les postes non équipés de Security BOX n'aient pas accès aux dossiers confidentiels partagés sur un serveur, afin qu'un utilisateur ne puisse pas provoquer un déni de service en altérant, par inadvertance ou par malveillance, les fichiers protégés par le produit.

L'utilisateur suit la politique de sécurité en vigueur dans l'organisme considéré.

4.2.3 Objectifs sur les systèmes en relation avec la TOE

OE.PKI

Les bi-clés et les certificats utilisés sont tous générés par une autorité de certification de confiance.

OE.SECURITY_BOX_MANAGER

Les "modèles" de politiques sont gérés hors de la TOE par l'application Security BOX Manager qui est considérée de confiance pour cette évaluation.

OE.TOKEN_FIABLE

Dans le mode de déploiement avec dispositif matériel, il est considéré que ce dispositif assure la protection en confidentialité et en intégrité des clés stockées.

OE.PKCS11_EXTERNE

La librairie PKCS#11 employée sur la machine hôte permet d'accéder de manière certaine à la carte à puce de l'utilisateur, et est réputée de confiance (absence de piégeage). Elle est installée sur le poste par l'administrateur qui en vérifie à l'installation son bon fonctionnement. La politique de sécurité en vigueur sur le système permet de la considérer comme intègre.

OE.MACHINE_HOTE_CONFIANCE

La machine hôte sur laquelle la TOE s'exécute doit être saine.

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

OE.CONFIGURATION_AUTHENTIFICATION

L'authentification de l'utilisateur à son porte-clés est configurée dans l'état de l'art, à la fois pour la configuration du mot de passe et du PIN (notamment en terme de complexité du mot de passe, et de verrouillage du dispositif lors d'échecs consécutifs d'authentification).

OE.AUDIT

Le système d'exploitation sur lequel est installé la TOE doit gérer les journaux d'évènements générés par la TOE en conformité avec la politique de sécurité de l'organisation. Il doit par exemple restreindre l'accès en lecture à ces journaux aux seules personnes explicitement autorisées.

OE.MAJ_POLITIQUES

Les politiques fournies à la TOE doivent être intègres et authentiques. Elles doivent être signées par un administrateur habilité.

4.3 Argumentaire des objectifs de sécurité

4.3.1 Couverture des hypothèses

H.ENV_OPERATIONNEL: *L'hypothèse est directement couverte par [OE.ENV_OPERATIONNEL].*

H.MOT_DE_PASSE: *L'hypothèse est directement couverte par [OE.CONFIGURATION_AUTHENTIFICATION].*

H.ADMIN_SYSTEME_CONFIANCE: *L'hypothèse est directement couverte par [OE.ADMIN_SYSTEME_CONFIANCE].*

H.ADMIN_SECURITE_CONFIANCE: *L'hypothèse est directement couverte par [OE.ADMIN_SECURITE_CONFIANCE].*

H.PKI: *L'hypothèse est directement couverte par [OE.PKI].*

H.SECURITY_BOX_MANAGER: *L'hypothèse est directement couverte par [OE.SECURITY_BOX_MANAGER].*

H.TOKEN_FIABLE: *L'hypothèse est couverte par [OE.TOKEN_FIABLE] et [OE.PKCS11_EXTERNE].*

H.MACHINE_HOTE_CONFIANCE: *L'hypothèse est directement couverte par [OE.MACHINE_HOTE_CONFIANCE].*

4.3.2 Couverture des menaces

M.ACCES_ILLICITE_COMPTE_UTILISATEUR: *La menace est couverte par :*

Objectifs de prévention : les droits d'accès Windows doivent tout d'abord empêcher les accès aux fichiers contenant les comptes utilisateurs [OE.MACHINE_HOTE_CONFIANCE]. Ensuite, l'utilisateur doit s'authentifier pour accéder au contenu du compte [OT.AUTHENTIFICATION] et [OE.CONFIGURATION_AUTHENTIFICATION] pour la configuration suffisante du mot de passe ou du code PIN permettant l'accès.

Objectifs de protection : la TOE doit protéger en intégrité et confidentialité les comptes utilisateurs [OT.PROTECTION_COMPTES_UTILISATEURS].

Objectifs de limitation d'impact : -

M.ALTERATION_REGLES_PARTAGEES: *La menace est couverte par :*

Objectifs de prévention : -

Objectifs de protection : la TOE protège en intégrité et confidentialité les règles partagées [OT.PROTECTION_REGLES_PARTAGEES].

Objectifs de limitation d'impact : -

M.ACCES_ILLICITE_CLES_CHIFFREMENT_FICHIER: *La menace est couverte par :*

Objectifs de prévention : -

Objectifs de protection : La TOE protège en intégrité et confidentialité la clé de chiffrement d'un fichier [OT.PROTECTION_CLE].

Objectifs de limitation d'impact : -

M.ALTERATION_POLITIQUE_TELECHARGEE: *La menace est couverte par :*

Objectifs de prévention : -

Objectifs de protection : -

Objectifs de limitation d'impact : l'administrateur sécurité doit de son côté signer les politiques mises à disposition [OE.MAJ_POLITIQUES] afin que toute altération de la politique téléchargée lors d'une mise à jour puisse être détectée par la TOE [OT.VERIFICATION_POLITIQUE].

Menace	Objectifs pour la TOE	Objectifs pour l'environnement
M.ACCES_ILLICITE_COMPTE_UTILISATEUR	[OT.AUTHENTIFICATION] [OT.PROTECTION_COMPTES_UTILISATEURS]	[OE.MACHINE_HOTE_CONFIANCE] [OE.CONFIGURATION_AUTHENTIFICATION]
M.ALTERATION_REGLES_PARTAGEES	[OT.PROTECTION_REGLES_PARTAGEES]	-
M.ACCES_ILLICITE_CLES_CHIFFREMENT_FICHIER	[OT.PROTECTION_CLE]	-
M.ALTERATION_POLITIQUE_TELECHARGEE	[OT.VERIFICATION_POLITIQUE]	[OE.MAJ_POLITIQUES]

Tableau 4 : Couverture des menaces

4.3.3 Couverture des OSP

P.PROTECTION_FICHIERS: *L'OSP est traduite par l'objectif [OT.PROTECTION_FICHIERS] qui impose le déblocage au préalable du compte de l'utilisateur légitime [OT.AUTHENTIFICATION].*

P.PROTECTION_SWAP: *L'OSP est directement traduite par l'objectif [OT.PROTECTION_SWAP].*

P.PROTECTION_PORTE-CLES_LOGICIEL: *L'OSP est directement traduite par l'objectif [OT.PROTECTION_COMPTES_UTILISATEURS] car dans le mode porte-clés logiciel, le bi-clé et les certificats sont stockés dans le compte de l'utilisateur.*

P.MODE_AUTHENTIFICATION : *L'OSP est directement traduite par l'objectif [OT.AUTHENTIFICATION].*

P.CLOISONNEMENT_SESSION: *L'OSP est directement traduite par l'objectif [OT.CLOISONNEMENT_SESSION].*

P.EFF_RESIDUS: *L'OSP est directement traduite par l'objectif [OT.EFF_RESIDUS].*

P.GESTION_REGLES: *L'OSP est directement traduite par l'objectif [OT.GESTION_REGLES].*

P.ROLES: *L'OSP est directement traduite par l'objectif [OT.ROLES].*

P.JOURNALISATION: *L'OSP est traduite par l'objectif [OT.JOURNALISATION] qui impose à la TOE de générer des journaux d'évènements et par [OE.AUDIT] qui impose au système d'exploitation de bien les gérer.*

P.SEPARATION_ROLES: *L'OSP est traduite par l'objectif [OE.SEPARATION_ROLES]*

P.GENERATION_CLES_CHIFFREMENT_FICHIERS: *L'OSP est directement traduite par l'objectif [OT.GENERATION_CLES_CHIFFREMENT_FICHIERS].*

P.CRYPTO: *L'OSP s'applique aux objectifs [OT.PROTECTION_FICHIER], [OT.PROTECTION_SWAP], [OT.PROTECTION_COMPTES_UTILISATEURS] et [OT.GENERATION_CLES_CHIFFREMENT_FICHIERS] qui mettent en œuvre des mécanismes cryptographiques.*

P.PSSI: *L'OSP est directement traduite par l'objectif [OE.PSSI].*

5. EXIGENCES DE SECURITE

5.1 Exigences de sécurité explicites

La cible de sécurité ne définit pas d'exigences de sécurité explicites. Toutes les exigences de sécurité présentes dans cette cible sont extraites des parties 2 et 3 des Critères Communs [CC].

5.2 Sujets, Objets, Opérations

5.2.1 Liste des sujets

Sujets	Description	Attributs de sécurité
Application	Une application accédant aux fichiers	
Owner	Propriétaire d'une règle	
Coworker	Collaborateur	
Policy Officer	Administrateur de sécurité	
Key Manager	Gestionnaire des clés et des comptes utilisateurs	

Tableau 5 : Liste des sujets

5.2.2 Liste des objets

Objets	Description	Attributs de sécurité
File	Fichier dont le contenu est sensible	• File owner identities • File coworkers identities
User account	Compte utilisateur	• Account owner identity
Security policy	Politique de sécurité	
Shared rules	Règle de sécurité appliquée à un répertoire contenant un fichier dont le contenu est confidentiel	• Shared rules owner identity • Shared rules coworkers identities
User key	Clé utilisateur	
Keystore	Porte-clés matériel ou logiciel	

Tableau 6 : Liste des objets

5.2.3 Liste des opérations

Sujets	Opérations	Objets
Application	Access (Create, open, write, read, delete)	File
Owner	Specify, modify, cancel	Shared rules
Owner. Coworker	Create, open, write, read, delete through the Application	File
Owner. Coworker	Lock, Unlock	Keystore
Owner, Coworker	Backup, restore	File
Policy Officier	Specify, modify	Security policy
Key Manager	Generate, certify, revoke	User key
Key Manager	Create, generate, and deploy	User account

Tableau 7 : Liste des opérations

5.3 Exigences fonctionnelles pour la TOE

Le texte extrait des Critères communs est en caractères normaux. Les attributions (« assignements ») et les sélections (« selections ») sont identifiées par des crochets. Les raffinements (« refinements ») sont en caractères *italiques*.

5.3.1 Synthèse des exigences fonctionnelles

Authentification des utilisateurs

FIA_UAU.1: Timing of authentication

FIA_UID.1: Timing of identification

Protection des fichiers

FDP_ACC.2/files: Complete access control

FDP_ACF.1/files: Security attribute based access control

FCS_COP.1/file_encryption: Cryptographic operation

FCS_CKM.1/file_encryption_keys: Cryptographic key generation

FCS_CKM.4/file_encryption_keys: Cryptographic key destruction

Protection des clés de chiffrement des fichiers

FCS_COP.1/keys_encryption: Cryptographic operation

FDP_ITC.1/user_keys: Import of user data without security attributes

FDP_ITC.1/trusted_third_party_certificate: Import of user data without security attributes

Protection des règles de sécurité partagées

FDP_ACC.2/shared_rules: Complete access control

FDP_ACF.1/shared_rules: Security attribute based access control

FCS_COP.1/shared_rules_encryption: Cryptographic operation

FCS_CKM.1/shared_rules_encryption_keys: Cryptographic key generation

Vérification du statut des certificats

FDP_ACC.1/certificate_revocation_verification: Complete access control

FDP_ACF.1/certificate_revocation_verification: Security attribute based access control

Protection des comptes utilisateurs

FDP_ACC.2/account: Complete access control

FDP_ACF.1/account: Security attribute based access control

FCS_COP.1/account_protection: Cryptographic operation

FCS_CKM.1/account_encryption_keys: Cryptographic key generation

Protection du fichier d'échange

FCS_COP.1/swap_encryption: Cryptographic operation

FCS_CKM.1/swap_encryption_keys: Cryptographic key generation

Protection des informations résiduelles

FDP_RIP.2: Full residual information protection

Génération d'audit

FAU_GEN.1: Audit data generation

FAU_GEN.2: User identity association

Administration des fonctions de sécurité

FMT_SMF.1: Specification of Management Functions

FMT_SMR.1: Security roles

Contrôle de l'intégrité des politiques téléchargées

FDP_ITT.3/policy: Integrity monitoring

FDP_IFF.1/policy: Simple security attributes

FDP_ACC.1/policy: Subset access control

FDP_IFC.1/policy: Subset information flow control

Cloisonnement des sessions

FDP_ACC.2/sessions: Complete access control

FDP_ACF.1/sessions: Security attribute based access control

Sauvegarde et Restauration de fichier

FDP_ETC.2/File : Export of user data with security attributes

FDP_ITC.2/File : Import of user data with security attributes

5.3.2 Détail des exigences fonctionnelles

5.3.2.1 Authentification des utilisateurs

FIA_UAU.1: Timing of authentication

fia_uau.1.1

The TSF shall allow [to list the content of folders and to display file status (encrypted/not encrypted)] on behalf of the user to be performed before the user is authenticated.

fia_uau.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1: Timing of identification

fia_uid.1.1

The TSF shall allow [to list the content of folders and to display file status (encrypted/not encrypted)] on behalf of the user to be performed before the user is identified.

fia_uid.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.3.2.2 Protection des fichiers

FDP_ACC.2/files: Complete access control

fdp_acc.2.1

The TSF shall enforce the [Files access control policy] on [Files] and all operations among subjects and objects covered by the SFP.

fdp_acc.2.2

The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Raffinement : concerne le contrôle d'accès aux fichiers contenant des informations sensibles.

FDP_ACF.1/files: Security attribute based access control

fdp_acf.1.1

The TSF shall enforce the [Files access control policy] to objects based on the following: [Files and theirs security attributes: owner identity and coworkers identities].

fdp_acf.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [an Application can access a File if a user is authenticated and is identified as owner or coworker of the File].

fdp_acf.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [a user is authenticated AND is identified as owner or coworker of the File].

fdp_acf.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [nobody is authenticated OR the authenticated user is not identified as owner or coworker of the File].

Raffinement : concerne le contrôle d'accès aux fichiers contenant des informations sensibles.

FCS_COP.1/file_encryption: Cryptographic operation

fcs_cop.1.1

The TSF shall perform [file encryption] in accordance with a specified cryptographic algorithm [AES for bulk-encryption] and cryptographic key sizes [128, 192, 256 for AES] that meet the following: [ISO 10116, CMS, PKCS#1].

Raffinement : concerne la clé de chiffrement du fichier

FCS_CKM.1/file_encryption_keys: Cryptographic key generation

fcs_ckm.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES] and specified cryptographic key sizes [128, 192, 256] that meet the following: [[CRYPTO_STD]].

Raffinement : concerne la génération de la clé de chiffrement du fichier

FCS_CKM.4/file_encryption_keys: Cryptographic key destruction

fcs_ckm.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [not assigned] that meets the following: [[CLE_STD]].

Raffinement : concerne l'effacement de la clé de chiffrement du fichier

5.3.2.3 Protection des clés de chiffrement des fichiers

FCS_COP.1/keys_encryption: Cryptographic operation

fcs_cop.1.1

The TSF shall perform [encryption keys encryption] in accordance with a specified cryptographic algorithm [RSA] and cryptographic key sizes [2048 for RSA] that meet the following: [CMS, PKCS#1].

Raffinement : concerne le chiffrement/déchiffrement des clés de chiffrement des fichiers

FDP_ITC.1/user_keys: Import of user data without security attributes

fdp_itc.1.1

The TSF shall enforce the [access control] when importing user data, controlled under the SFP, from outside of the TOE.

fdp_itc.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

fdp_itc.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [not assigned].

Raffinement : concerne la clé de l'utilisateur utilisée pour chiffrer et déchiffrer la clé de chiffrement du fichier

FDP_ITC.1/trusted_third_party_certificate: Import of user data without security attributes

fdp_itc.1.1

The TSF shall enforce the [Certificate revocation verification policy] when importing user data, controlled under the SFP, from outside of the TOE.

fdp_itc.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

fdp_itc.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [not assigned].

Raffinement : concerne les certificats des collaborateurs de confiance et également les certificats d'autorité

5.3.2.4 Protection des règles de sécurité partagées

FDP_ACC.2/shared_rules: Complete access control

fdp_acc.2.1

The TSF shall enforce the [shared rules access control policy] on [shared rules] and all operations among subjects and objects covered by the SFP.

fdp_acc.2.2

The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Raffinement : concerne le contrôle d'accès aux règles de sécurité partagées

FDP_ACF.1/shared_rules: Security attribute based access control

fdp_acf.1.1

The TSF shall enforce the [shared rules access control policy] to objects based on the following: [shared rules and theirs security attributes: owner or coworker identities].

fdp_acf.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [an user can access his account if he is authenticated and is identified as owner of theshared rule].

fdp_acf.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [a user is authenticated AND is identified as owner of the shared rule].

fdp_acf.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [the authenticated user is not identified as owner of the shared rule].

Raffinement : concerne le contrôle d'accès aux règles partagées

FCS_COP.1/shared_rules_encryption: Cryptographic operation

fcs_cop.1.1

The TSF shall perform [shared rules encryption] in accordance with a specified cryptographic algorithm [AES for bulk-encryption] and cryptographic key sizes [128, 192, 256 for AES] that meet the following: [ISO 10116, CMS, PKCS#1].

Raffinement : concerne la clé de chiffrement de la règle de sécurité

FCS_CKM.1/shared_rules_encryption_keys: Cryptographic key generation

fcs_ckm.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES] and specified cryptographic key sizes [128, 192, 256] that meet the following: [[CRYPTO_STD]].

Raffinement : concerne la génération de la clé de chiffrement de la règle de sécurité

5.3.2.5 Vérification du statut des certificats

FDP_ACC.1/certificate_revocation_verification: Complete access control

fdp_acc.1.1

The TSF shall enforce the [verification of the certificate revocation status] on [User certificate before an Application can access a File].

Raffinement : concerne le certificat associé au bi-clé utilisé lors du chiffrement ou du déchiffrement d'un fichier

FDP_ACF.1/certificate_revocation_verification: Security attribute based access control

fdp_acf.1.1

The TSF shall enforce the [verification of the certificate revocation status] to objects based on the following: [User certificate and its security attributes: link to download the CRL].

fdp_acf.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [owner is able to authorize file access to Co-worker who has a valid and non revoked certificate].

fdp_acf.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [file access is granted for Co-worker who has a valid and non revoked certificate and when Owner has added the Co-worker certificate is the authorized user list].

fdp_acf.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [file access is automaticaly removed for Co-worker who has a revoked certificate].

Raffinement : concerne le certificat associé au bi-clé utilisé lors du chiffrement ou du déchiffrement d'un fichier

5.3.2.6 Protection des comptes utilisateurs

FDP_ACC.2/account: Complete access control

fdp_acc.2.1

The TSF shall enforce the [account access control policy] on [User accounts] and all operations among subjects and objects covered by the SFP.

fdp_acc.2.2

The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Raffinement : concerne le contrôle d'accès au compte utilisateur

FDP_ACF.1/account: Security attribute based access control

fdp_acf.1.1

The TSF shall enforce the [account access control policy] to objects based on the following: [User accounts and theirs security attributes: owner identity].

fdp_acf.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [an user can access his account if he is authenticated and is identified as owner of the Keystore].

fdp_acf.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [a user is authenticated AND is identified as owner of the account].

fdp_acf.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [the authenticated user is not identified as owner of the account].

Raffinement : concerne le contrôle d'accès au compte utilisateur

FCS_COP.1/account_protection: Cryptographic operation

fcs_cop.1.1

The TSF shall perform [account protection] in accordance with a specified cryptographic algorithm [AES and SHA] and cryptographic key sizes [128, 192, 256 for AES, and 256 for SHA] that meet the following: [CMS, PKCS#1].

Raffinement : concerne la clé de chiffrement du fichier contenant les comptes utilisateur

FCS_CKM.1/account_encryption_keys: Cryptographic key generation

fcs_ckm.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES and SHA] and specified cryptographic key sizes [128, 192, 256 for AES, and 256 for SHA] that meet the following: [[CRYPTO_STD]].

Raffinement : concerne la génération de la clé de chiffrement du compte utilisateur

5.3.2.7 Protection du fichier d'échange

FCS_COP.1/swap_encryption: Cryptographic operation

fcs_cop.1.1

The TSF shall perform [swap encryption] in accordance with a specified cryptographic algorithm [AES for bulk-encryption] and cryptographic key sizes [128, 192, 256 for AES] that meet the following: [ISO 10116].

Raffinement : concerne la clé de chiffrement du swap

FCS_CKM.1/swap_encryption_keys: Cryptographic key generation

fcs_ckm.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [AES] and specified cryptographic key sizes [128, 192, 256] that meet the following: [[CRYPTO_STD]].

Raffinement : concerne la génération de la clé de chiffrement du swap

5.3.2.8 Protection des informations résiduelles

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 [deallocation of the resource from] all objects.

5.3.2.9 Génération d'audit

FAU_GEN.1: Audit data generation

fau_gen.1.1

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

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

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

c) [

- authentication: lock / unlock
- shared rules : specify / modify / cancel
- Personal rules : specify / modify / cancel
- Policy management : Download / Administrated update / Local update / Signatory Key Renewal / Intégrity error
- File backup / restoration].

fau_gen.1.2

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [not assigned].

FAU_GEN.2: User identity association

fau_gen.2.1

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

5.3.2.10 Administration des fonctions de sécurité

FMT_SMF.1: Specification of Management Functions

fmt_smf.1.1

The TSF shall be capable of performing the following management functions: [Specify, modify, and cancel Rule].

Raffinement : concerne les fonctions permettant de gérer les règles de sécurité.

FMT_SMR.1: Security roles

fmt_smr.1.1

The TSF shall maintain the roles [Owner, Coworker].

fmt_smr.1.2

The TSF shall be able to associate users with roles.

Raffinement : concerne les rôles ayant accès à la gestion les règles de sécurité.

5.3.2.11 Contrôle de l'intégrité des politiques téléchargées

FDP_ITT.3/policy: Integrity monitoring

fdp_itt.3.1

The TSF shall enforce the [security policy importation policy] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [integrity or origin errors].

fdp_itt.3.2

Upon detection of a data integrity error, the TSF shall [maintain actual policy and not apply new policy].

Raffinement : concerne le contrôle de l'intégrité des politiques de sécurité téléchargées.

FDP_IFF.1/policy: Simple security attributes

fdp_iff.1.1

The TSF shall enforce the [security policy importation policy] based on the following types of subject and information security attributes: [integrity and origin].

fdp_iff.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [integrity validated and origin proof validated].

fdp_iff.1.3

The TSF shall enforce the [policy integrity and origin proof verification].

fdp_iff.1.4

The TSF shall explicitly authorise an information flow based on the following rules: [integrity verified AND integrity validated AND origin proof verified AND origin proof validated].

fdp_iff.1.5

The TSF shall explicitly deny an information flow based on the following rules: [integrity not verified OR integrity not validated OR origin proof not verified OR or origin proof not validated].

Raffinement : concerne le contrôle d'accès aux politiques de sécurité.

FDP_ACC.1/policy: Subset access control

fdp_acc.1.1

The TSF shall enforce the [access control] on [read or modification of security policy].

Raffinement : concerne le contrôle d'accès aux politiques de sécurité.

FDP_IFC.1/policy: Subset information flow control

fdp_ifc.1.1

The TSF shall enforce the [security policy importation policy] on [imported security policy].

Raffinement : concerne le contrôle d'accès aux politiques de sécurité.

5.3.2.12 Cloisonnement des sessions

FDP_ACC.2/sessions: Complete access control

fdp_acc.2.1

The TSF shall enforce the [Sessions isolation policy] on [User accounts] and all operations among subjects and objects covered by the SFP.

fdp_acc.2.2

The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Raffinement : concerne le contrôle d'accès aux données manipulées au sein d'une session Security BOX

FDP_ACF.1/sessions: Security attribute based access control

fdp_acf.1.1

The TSF shall enforce the [Sessions isolation policy] to objects based on the following: [User account and theirs security attributes: owner identity].

fdp_acf.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [an Application can access a File if a user is authenticated and is identified as owner or coworker of the File].

fdp_acf.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [a user is authenticated AND is identified as owner or coworker of the File].

fdp_acf.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [nobody is authenticated OR the authenticated user is not identified as owner or coworker of the File].

Raffinement : concerne le contrôle d'accès aux données manipulées au sein d'une session Security BOX

5.3.2.13 Sauvegarde/Restauration

FDP_ETC.2/File : Export of user data with security attributes

FDP_ETC.2.1

The TSF shall enforce the [no access control policy] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2

The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3

The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4

The TSF shall enforce the following rules when user data is exported from the TOE: [no rules].

Raffinement : concerne la sauvegarde d'un fichier chiffré.

FDP_ITC.2/File : Import of user data with security attributes

FDP_ITC.2.1

The TSF shall enforce the [Files access control policy] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2

The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3

The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4

The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [the user performing restoration must be an owner or a coworker on the destination folder].

Raffinement : concerne la restauration d'un fichier chiffré.

5.4 Exigences d'assurance pour la TOE

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

ADV : Development

ADV_ARC.1: Security architecture description

ADV_FSP.3: Functional specification with complete summary

ADV_TDS.2: Architectural design

AGD : Guidance documents

AGD_OPE.1: Operational user guidance

AGD_PRE.1: Preparative procedures

ALC : Life-cycle support

ALC_CMC.3: Authorisation controls

ALC_CMS.3: Implementation representation CM coverage

ALC_DEL.1: Delivery procedures

ALC_DVS.1: Identification of security measures

ALC_FLR.3: Systematic flaw remediation

ALC_LCD.1: Developer defined life-cycle model

ASE : Security Target evaluation

ASE_CCL.1 Conformance claims

ASE_ECD.1 Extended components definition

ASE_INT.1 ST introduction

ASE_OBJ.2 Security objectives

ASE_REQ.2 Derived security requirements

ASE_SPD.1 Security problem definition

ASE_TSS.1 TOE summary specification

ATE : Tests

ATE_COV.2: Analysis of coverage

ATE_DPT.1: Testing: basic design

ATE_FUN.1: Functional testing

ATE_IND.2: Independent testing - sample

AVA : Vulnerability assessment

AVA_VAN.3: Focused vulnerability analysis

5.5 Argumentaire des exigences de sécurité

5.5.1 Argumentaire des exigences fonctionnelles de sécurité

5.5.1.1 Couverture des objectifs de sécurité

OT.AUTHENTIFICATION: *L'objectif est directement traduit par les exigences [FIA_UAU.1] et [FIA_UID.1] qui permettent quelques opérations avant authentification.*

OT.PROTECTION_FICHIERS: *L'objectif est traduit par [FDP_ACC.2/files] et [FDP_ACF.1/files] qui permettent de définir les règles d'accès aux fichiers et par [FCS_COP.1/file_encryption] pour l'opération de chiffrement/déchiffrement. Cette dernière exigence nécessite aussi la selection des exigences qui en dépendent: [FDP_ITC.1/user_keys] et [FDP_ITC.1/trusted_third_party_certificate] pour l'importation de la clé utilisateur qui permet de déchiffrer la clé AES de déchiffrement du fichier, qui est elle générée [FCS_CKM.1/file_encryption_keys] par la TOE. Ces clés de chiffrement de fichiers doivent être détruites après emploi: [FCS_CKM.4/file_encryption_keys].*

Par ailleurs, avant utilisation, le statut de révocation des clés des utilisateurs doit être vérifié : [FDP_ACC.1/certificate_revocation_verification] et [FDP_ACF.1/certificate_revocation_verification].

OT.PROTECTION_SWAP: *L'objectif est traduit par [FCS_COP.1/swap_encryption] pour réaliser les opérations cryptographiques selon différents algorithmes. Cette dernière exigence nécessite aussi la sélection des exigences qui en dépendent : la clé de chiffrement est générée [FCS_CKM.1/swap_encryption_keys] par la TOE.*

OT.PROTECTION_COMPTES_UTILISATEURS: *L'objectif est traduit par [FDP_ACC.2/account] et [FDP_ACF.1/account] qui permettent de définir les règles d'accès aux fichiers contenant les comptes utilisateurs et par [FCS_COP.1/account_protection] pour l'opération de chiffrement/déchiffrement. Cette dernière exigence nécessite aussi la selection des exigences qui en dépendent: [FDP_ITC.1/user_keys] pour l'importation de la clé qui permet de déchiffrer la clé AES de déchiffrement du keystore, qui est elle générée [FCS_CKM.1/account_encryption_keys] par la TOE.*

Par ailleurs, avant utilisation, le statut de révocation des clés doit être vérifié: [FDP_ACC.1/certificate_revocation_verification] et [FDP_ACF.1/certificate_revocation_verification].

OT.PROTECTION_REGLES_PARTAGEES: *L'objectif est traduit par [FDP_ACC.2/shared_rules] et [FDP_ACF.1/shared_rules] qui permettent de définir les règles d'accès aux règles de sécurité et par [FCS_COP.1/shared_rules_encryption] pour l'opération de chiffrement/déchiffrement. Cette dernière exigence nécessite aussi la selection des exigences qui en dépendent: la clé AES de déchiffrement de la règle de sécurité est générée [FCS_CKM.1/shared_rules_encryption_keys] par la TOE.*

OT.PROTECTION_CLE: *L'objectif est traduit par [FCS_COP.1/keys_encryption] qui assure le chiffrement des clés symétriques AES de chiffrement des fichiers et des comptes par la clé RSA de l'utilisateur importée de son porte-clés [FDP_ITC.1/user_keys]. Les clés doivent être détruites après emploi: [FCS_CKM.4/file_encryption_keys].*

OT.CLOISONNEMENT_SESSION: *L'objectif est traduit par [FDP_ACC.2/sessions] et [FDP_ACF.1/sessions] qui assurent le contrôle d'accès (et donc le cloisonnement) aux données au sein d'une session Windows.*

OT.EFF_RESIDUS: *L'objectif est traduit par [FDP_RIP.2] qui permet un nettoyage totalement sécurisé des traces dans la mémoire (RAM) ou sur le disque dur (fichier swap ou temporaire).*

OT.GESTION_REGLES: *L'objectif est traduit par [FMT_SMF.1] qui offrent des fonctions d'administration et de gestion des fonctions de sécurité.*

OT.ROLES: *L'objectif est traduit par [FMT_SMR.1] qui permet la gestion et la distinction des rôles de Collaborateur et de Propriétaire.*

OT.VERIFICATION_POLITIQUE: *L'objectif est traduit par l'exigence [FDP_ITT.3/policy] qui s'assure du suivi de l'intégrité de la politique téléchargée. Cette exigence nécessite aussi la sélection des exigences qui en dépendent : [FDP_IFC.1/policy], [FDP_IFF.1/policy] pour la définition des opérations à réaliser à la réception de la politique, notamment la vérification de son intégrité et de l'origine et [FDP_ACC.1/policy] qui s'assure de la prévention de la modification une fois la politique stockée.*

OT.JOURNALISATION: *L'objectif est traduit par [FAU_GEN.1] qui permet la génération des évènements dans le journal d'audit du système d'exploitation et par [FAU_GEN.2] qui associe l'identité de l'utilisateur à chaque évènement inscrit dans ce journal.*

OT.GENERATION_CLES_CHIFFREMENT_FICHIERS: *L'objectif est traduit par [FCS_CKM.1/file_encryption_keys] qui permet de générer les clés cryptographiques.*

5.5.1.2 Dépendances

Exigences	Dépendances CC requises	Dépendances déclarées	Commentaires
FIA_UAU.1	FIA_UID.1	[FIA_UID.1]	OK
FIA_UID.1	-	-	OK
FDP_ACC.2/files	FDP_ACF.1	[FDP_ACF.1/files]	OK
FDP_ACF.1/files	FDP_ACC.1 and FMT_MSA.3	[FDP_ACC.2/files]	La dépendance vers l'exigence FMT_MSA.3 n'est pas exigée car les règles de sécurité par défaut sur un fichier n'ont pas à être configurées. Par défaut (lors de la sécurisation d'un fichier), l'utilisateur authentifié est désigné Propriétaire du fichier.
FCS_COP.1/file_encryption	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	[FDP_ITC.1/user_keys], [FCS_CKM.1/file_encryption_keys], [FCS_CKM.4/file_encryption_keys]	OK
FCS_CKM.1/file_encryption_keys	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	[FCS_COP.1/file_encryption], [FCS_CKM.4/file_encryption_keys]	OK
FCS_CKM.4/file_encryption_keys	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	[FCS_CKM.1/file_encryption_keys]	OK
FCS_COP.1/keys_encryption	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	[FDP_ITC.1/user_keys]	La dépendance vers l'exigence FCS_CKM.4 n'est pas exigée car les clés utilisées pour déchiffrer la clé de chiffrement de la règle sont les clés privées des utilisateurs. La destruction des clés utilisateurs fait partie de l'organisation de l'IGC, qui est hors périmètre de la cible.

Exigences	Dépendances CC requises	Dépendances déclarées	Commentaires
FDP_ITC.1/user_keys	(FDP_ACC.1 or FDP_IFC.1) and FMT_MSA.3	[FDP_ACC.1/certificate_revocation_verification]	La dépendance vers l'exigence FMT_MSA.3 n'est pas exigée car le contrôle d'accès par défaut sur les clés de l'utilisateur n'a pas à être configuré. Par défaut (lors de la sécurisation d'un fichier), l'utilisateur authentifié est désigné Propriétaire de la clé.
FDP_ITC.1/trusted_third_party_certificate	(FDP_ACC.1 or FDP_IFC.1) and FMT_MSA.3	[FDP_ACC.1/certificate_revocation_verification]	La dépendance vers l'exigence FMT_MSA.3 n'est pas exigée car le contrôle d'accès par défaut sur les certificats n'a pas à être configuré.
FDP_ACC.2/shared_rules	FDP_ACF.1	[FDP_ACF.1/shared_rules]	OK
FDP_ACF.1/shared_rules	FDP_ACC.1 and FMT_MSA.3	[FDP_ACC.2/shared_rules]	La dépendance vers l'exigence FMT_MSA.3 n'est pas exigée car le contrôle d'accès aux règles par défaut n'a pas à être configuré. Par défaut, les règles ne sont accessibles qu'au Propriétaire.
FCS_COP.1/shared_rules_encryption	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	[FCS_CKM.1/shared_rules_encryption_keys]	La dépendance vers l'exigence FCS_CKM.4 n'est pas exigée car les clés utilisées pour déchiffrer la clé de chiffrement de la règle sont les clés privées des utilisateurs. La destruction des clés utilisateurs fait partie de l'organisation de l'IGC, qui est hors périmètre de la cible.
FCS_CKM.1/shared_rules_encryption_keys	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	[FCS_COP.1/shared_rules_encryption]	La dépendance vers l'exigence FCS_CKM.4 n'est pas exigée car les clés utilisées pour déchiffrer la clé de chiffrement de la règle sont les clés privées des utilisateurs. La destruction des clés utilisateurs fait partie de l'organisation de l'IGC, qui est hors périmètre de la cible.
FDP_ACC.1/certificate_revocation_verification	FDP_ACF.1	[FDP_ACF.1/certificate_revocation_verification]	OK
FDP_ACF.1/certificate_revocation_verification	FDP_ACC.1 and FMT_MSA.3	[FDP_ACC.1/certificate_revocation_verification]	La dépendance vers l'exigence FMT_MSA.3 n'est pas exigée car le contrôle d'accès la vérification de révocation par défaut n'a pas à être configuré.
FDP_ACC.2/account	FDP_ACF.1	[FDP_ACF.1/account]	OK

Exigences	Dépendances CC requises	Dépendances déclarées	Commentaires
FDP_ACF.1/account	FDP_ACC.1 and FMT_MSA.3	[FDP_ACC.2/account]	La dépendance vers l'exigence FMT_MSA.3 n'est pas exigée car le contrôle d'accès par défaut sur un compte n'a pas à être configuré. Par défaut (lors de la configuration par l'administrateur sécurité), l'utilisateur mentionné par l'administrateur est désigné Propriétaire du compte.
FCS_COP.1/account_protection	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	[FDP_ITC.1/user_keys], [FCS_CKM.1/account_encryption_keys]	La dépendance vers l'exigence FCS_CKM.4 n'est pas exigée car les clés utilisées pour déchiffrer la clé de chiffrement de la règle sont les clés privées des utilisateurs. La destruction des clés utilisateurs fait partie de l'organisation de l'IGC, qui est hors périmètre de la cible.
FCS_CKM.1/account_encryption_keys	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	[FCS_COP.1/account_protection]	La dépendance vers l'exigence FCS_CKM.4 n'est pas exigée car les clés utilisées pour déchiffrer la clé de chiffrement de la règle sont les clés privées des utilisateurs. La destruction des clés utilisateurs fait partie de l'organisation de l'IGC, qui est hors périmètre de la cible.
FCS_COP.1/swap_encryption	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	[FCS_CKM.1/swap_encryption_keys],	OK
FCS_CKM.1/swap_encryption_keys	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	[FCS_COP.1/swap_encryption],	OK
FDP_RIP.2	-	-	OK
FAU_GEN.1	FPT_STM.1	-	La dépendance vers l'exigence FPT_STM.1 n'est pas exigée car la TOE s'appuie sur l'horloge du système d'exploitation, qui est hors périmètre de la TOE.
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	[FAU_GEN.1], [FIA_UID.1]	OK
FMT_SMF.1	-	-	OK
FMT_SMR.1	FIA_UID.1	[FIA_UID.1]	OK

Exigences	Dépendances CC requises	Dépendances déclarées	Commentaires
FDP_ITT.3/policy	(FDP_ACC.1 or FDP_IFC.1) and FDP_ITT.1	[FDP_ACC.1/policy]	La dépendance vers l'exigence FDP_ITT.1 n'est pas exigée car la TOE n'est hébergée sur qu'une seule entité physique.
FDP_IFF.1/policy	FDP_IFC.1 and FMT_MSA.3	[FDP_IFC.1/policy]	La dépendance vers l'exigence FMT_MSA.3 n'est pas exigée car le contrôle d'accès par défaut sur une politique de sécurité n'a pas à être configuré. Par défaut (lors de la configuration par l'utilisateur), l'administrateur sécurité est désigné Propriétaire.
FDP_ACC.1/policy	FDP_ACF.1	-	La dépendance vers l'exigence FDP_ACF.1 n'est pas exigée car le contrôle d'accès par défaut sur une politique de sécurité n'a pas à être configuré. Par défaut (lors de la configuration par l'utilisateur), l'administrateur sécurité est désigné Propriétaire.
FDP_IFC.1/policy	FDP_IFF.1	[FDP_IFF.1/policy]	OK
FDP_ACC.2/sessions	FDP_ACF.1	[FDP_ACF.1/sessions]	OK
FDP_ACF.1/sessions	FDP_ACC.1 and FMT_MSA.3	[FDP_ACC.2/sessions]	La dépendance vers l'exigence FMT_MSA.3 n'est pas exigée car les règles de cloisonnement par défaut n'ont pas à être configurées. Par défaut, les données (et en particulier le compte utilisateur ouvert) sont isolées dans une session Windows unique.
FDP_ETC.2/files	[FDP_ACC.1 or FDP_IFC.1]	-	La dépendance vers FDP_ACC.1 n'est pas exigée car il n'y a pas restriction pour la sauvegarde d'un fichier chiffré car le fichier sauvegardé reste chiffré avec ses attributs.
FDP_ITC.2/files	[FDP_ACC.1 or FDP_IFC.1] and [FTP_ITC.1 or FTP_TRP.1] and FPT_TDC.1	[FDP_ACC.2/files]	Les dépendances vers [FTP_ITC.1 or FTP_TRP.1] and FPT_TDC.1 ne sont pas exigées car le fichier est de toute façon importé chiffré.

Tableau 8 : Dépendances entre exigences fonctionnelles de sécurité

5.5.2 Argumentaire des exigences d'assurance de sécurité

5.5.2.1 Justification du niveau d'évaluation

Le niveau d'évaluation permet de satisfaire les exigences du processus de qualification au niveau « standard » [QS]

5.5.2.2 Dépendances

Exigences	Dépendances requises par les CC	Dépendances déclarées	Commentaires
ADV_ARC.1	ADV_FSP.1 and ADV_TDS.1	[ADV_FSP.3] and [ADV_TDS.2]	
ADV_FSP.3	ADV_TDS.1	[ADV_TDS.2]	
ADV_TDS.2	ADV_FSP.3	[ADV_FSP.3]	
AGD_OPE.1	ADV_FSP.1	[ADV_FSP.3]	
AGD_PRE.1	-	-	
ALC_CMC.3	ALC_CMS.1 and ALC_DVS.1 and ALC_LCD.1	[ALC_CMS.3] and [ALC_DVS.1] and [ALC_LCD.1]	
ALC_CMS.3	-	-	
ALC_DEL.1	-	-	
ALC_DVS.1	-	-	
ALC_FLR.3	-	-	
ALC_LCD.1	-	-	
ASE_CCL.1	ASE_INT.1 and ASE_ECD.1 and ASE_REQ.1	ASE_INT.1 and ASE_ECD.1 and ASE_REQ.2	
ASE_ECD.1	-	-	
ASE_INT.1	-	-	
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	
ASE_REQ.2	ASE_OBJ.2 and ASE_ECD.1	ASE_OBJ.2 and ASE_ECD.1	
ASE_SPD.1	-	-	

Exigences	Dépendances requises par les CC	Dépendances déclarées	Commentaires
ASE_TSS.1	ASE_INT.1 and ASE_REQ.1 and ADV_FSP.1	[ASE_INT.1] and [ASE_REQ.2] and [ADV_FSP.3]	
ATE_COV.2	ADV_FSP.2 and ATE_FUN.1	[ADV_FSP.3] and [ATE_FUN.1]	
ATE_DPT.1	ADV_ARC.1 and ADV_TDS.2 and ATE_FUN.1	[ADV_ARC.1] and [ADV_TDS.2] and [ATE_FUN.1]	
ATE_FUN.1	ATE_COV.1	[ATE_COV.2]	
ATE_IND.2	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1	[ADV_FSP.3] and [AGD_OPE.1] and [AGD_PRE.1] and [ATE_COV.2]and [ATE_FUN.1]	
AVA_VAN.3	ADV_ARC.1 and ADV_FSP.4 and ADV_TDS.3 and ADV_IMP.1 and AGD_OPE.1 and AGD_PRE.1 and ATE_DPT.1	[ADV_ARC.1], [AGD_OPE.1], [AGD_PRE.1], [ATE_DPT.1]	Toutes les dépendances de l'augmentation AVA_VAN.3 ne sont pas formellement satisfaites (il manque ADV_FSP.4, ADV_TDS.3 et ADV_IMP.1) mais l'évaluation est complétée par une expertise de l'implémentation des mécanismes de type cryptographique. A ce titre, l'implémentation complète du produit est fournie à l'évaluateur. Il dispose donc des informations suffisantes pour réaliser les travaux requis par AVA_VAN.3.

Tableau 9 : Dépendances entre exigences fonctionnelles de sécurité

6. RESUME DES SPECIFICATIONS DE LA TOE

6.1 Authentification des utilisateurs

FIA_UAU.1

Les utisateurs doivent s'authentifier pour pouvoir débloquer leur compte. L'utilisateur doit présenter un identifiant et un mot de passe si les clés privées de l'utilisateur sont stockées dans le compte (porte-clés logiciel). L'utilisateur doit présenter un code PIN s'il utilise un dispositif matériel (carte à puce ou clé USB) pour stocker ses clés privées (porte-clés matériel).

FIA_UID.1

Dans le cas du porte-clés logiciel, l'utilisateur doit saisir un identifiant.

Dans le cas du porte-clés matériel, l'utilisateur doit saisir un code PIN.

6.2 Protection des fichiers

FDP_ACC.2/files

La TOE met en oeuvre un système de contrôle d'accès au contenu des fichiers.

FDP_ACF.1/files

Un utilisateur ne peut accéder au contenu d'un fichier via une application que s'il a ouvert son compte Security BOX et s'il est déclaré comme Propriétaire ou Collaborateur pour ce fichier.

FCS_COP.1/file_encryption

Le contrôle d'accès au contenu des fichiers est assuré par des mécanismes de chiffrement : AES 128, 192, 256.

FCS_CKM.1/file_encryption_keys

La TOE génère une clé de chiffrement AES pour chacun des fichiers à protéger.

FCS_CKM.4/file_encryption_keys

A la fermeture de session Security BOX, la TOE parcourt tous les contextes de sécurité ouverts et broie les clés de protection associées.

6.3 Protection des clés de chiffrement des fichiers

FCS_COP.1/keys_encryption

Le contrôle d'accès au contenu de la règle de sécurité est assuré par des mécanismes de chiffrement : RSA 2048, 4096..

FDP_ITC.1/user_keys

La TOE utilise des bi-clés RSA 2048 pour chiffrer et déchiffrer les clés de chiffrement propres à chaque fichier. Ces bi-clés sont également utilisées pour protéger l'accès au compte utilisateur.

Avant leur utilisation, la TOE vérifie si le certificat associé au bi-clé n'a pas été révoqué.

FDP_ITC.1/trusted_third_party_certificate

Avant l'utilisation des bi-clés RSA 2048 pour chiffrer et déchiffrer les clés de chiffrement de fichier, la TOE vérifie si le certificat associé au bi-clé n'a pas été révoqué.

6.4 Protection des règles de sécurité partagées

FDP_ACC.2/shared_rules

Les règles de sécurité sont chiffrées par la clé publique de chaque utilisateur autorisé à les modifier. Ainsi, seuls les utilisateurs autorisés peuvent accéder, avec leur clé privée, aux règles de sécurité.

FDP_ACF.1/shared_rules

Les règles de sécurité sont chiffrées par la clé publique de chaque utilisateur autorisé à les modifier. Ainsi, seuls les utilisateurs autorisés peuvent accéder, avec leur clé privée, aux règles de sécurité.

FCS_COP.1/shared_rules_encryption

Le contrôle d'accès au contenu de la règle de sécurité est assuré par des mécanismes de chiffrement : AES 128, 192, 256.

FCS_CKM.1/shared_rules_encryption_keys

La TOE génère une clé de chiffrement AES pour chacune des règles de sécurité.

6.5 Vérification du statut des certificats

FDP_ACC.1/certificate_revocation_verification

Avant d'utiliser les clés d'un utilisateur pour chiffrer ou déchiffrer un fichier, la TOE vérifie si le certificat associé à ces clés n'a pas été révoqué.

FDP_ACF.1/certificate_revocation_verification

La non-révocation des clés des collaborateurs est contrôlée :

- Lors de la création de tout nouveau fichier dans le dossier sécurisé : le fichier n'est alors pas chiffré pour l'utilisateur révoqué
- Lors de l'application d'une règle modifiée : si un utilisateur révoqué était autorisé à chiffrer un fichier, alors cet utilisateur est supprimé de la liste des utilisateurs autorisés et le fichier est transchiffré.

6.6 Protection des comptes utilisateurs

FDP_ACC.2/account

Le contrôle d'accès au contenu du compte utilisateur est assuré par des mécanismes de chiffrement symétrique.

Le keystore de l'utilisateur est un "token" PKCS#11 et à ce titre peut être ouvert par l'utilisateur lui même (noté U pour user) ou son administrateur (noté SO pour Service Officer).

FDP_ACF.1/account

Le keystore de l'utilisateur est un "token" PKCS#11 et à ce titre peut être ouvert par l'utilisateur lui même (noté U pour user) ou son administrateur (noté SO pour Service Officer).

FCS_COP.1/account_protection

Le contrôle d'accès au contenu du compte utilisateur est assuré par des mécanismes de chiffrement symétrique.

Le keystore de l'utilisateur est un "token" PKCS#11 et à ce titre peut être ouvert par l'utilisateur lui même (noté U pour user) ou son administrateur (noté SO pour Service Officer).

Le compte utilisateur (et les clés privées de l'utilisateur qui y sont stockées dans le mode porte-clés logiciel) est protégé selon deux modes :

- par mot de passe dans le cas du porte-clés logiciel,
- par carte et code PIN dans le cas du porte-clés matériel.

Le compte utilisé est scellé par un mécanisme de chiffrement symétrique.

FCS_CKM.1/account_encryption_keys

La TOE génère une clé de chiffrement AES pour chaque compte utilisateur. Les comptes sont scellés par une clé SHA 256.

6.7 Protection du fichier d'échange

FCS_COP.1/swap_encryption

Le contrôle d'accès au contenu de la zone d'échange est assuré par des mécanismes de chiffrement : AES 128, 192, 256.

FCS_CKM.1/swap_encryption_keys

La TOE génère à chaque démarrage du système une nouvelle clé de chiffrement AES pour le fichier d'échange du système.

6.8 Protection des informations résiduelles

FDP_RIP.2

A la fermeture de session Security BOX, la TOE parcourt tous les contextes de sécurité ouverts et broie les clés de protection associées.

6.9 Génération d'audit

FAU_GEN.1

Les évènements suivants sont enregistrés par la TOE :

- Authentification : connexion / déconnexion / verrouillage / déverrouillage / échec d'authentification
- Gestion des règles partagées : Création / Modification / Désécurisation (remise en clair) / Application
- Gestion des règles peronnelles : Création / Modification / Désécurisation (remise en clair) / Application
- Politique : Téléchargement / Mise à jour administrée ou locale de la politique / changement du certificat signataire de la politique / erreur d'intégrité
- Sauvegarde / Restauration d'un fichier

Les évènements sont enregistrés dans les journaux d'évènements du système d'exploitation.

FAU_GEN.2

Les évènements de la TOE relatifs à une action d'un utilisateur authentifié sont enregistrés avec l'identifiant de l'utilisateur.

6.10 Administration des fonctions de sécurité

FMT_SMF.1

La TSF propose une extension de l'explorateur via un nouvel onglet dans les propriétés du dossier.

Les certificats sont proposés par rapport à l'annuaire de confiance local.

FMT_SMR.1

Les rôles sont configurables dans l'onglet "Security BOX" des propriétés du dossier. Chaque utilisateur se voit attribuer un unique rôle spécique (Owner ou Coworker) associé au dossier.

6.11 Contrôle de l'intégrité des politiques téléchargées

FDP_ITT.3/policy

La mise à jour de la politique est un certificat X.509 d'attributs signé par le signataire des politiques (un administrateur habilité). A la réception de la politique, la TOE vérifie la signature du certificat d'attributs conformément à X.509.

FDP_IFF.1/policy

La mise à jour de la politique est un certificat X.509 d'attributs signé par le signataire des politiques (un administrateur habilité). A la réception de la politique, la TOE vérifie la signature du certificat d'attributs conformément à X.509.

FDP_ACC.1/policy

Une fois téléchargée, et stockée dans le compte utilisateur, l'administrateur de sécurité peut indiquer à l'application que l'utilisateur n'a pas le droit de modifier ou lire la politique appliquée.

FDP_IFC.1/policy

L'intégrité de la politique de sécurité importée est contrôlée par la vérification de sa signature.

6.12 Cloisonnement des sessions

FDP_ACC.2/sessions

Il ne peut y avoir qu'une seule session Security BOX ouverte sur un même poste de travail.

Si une session Security BOX est ouverte, il n'est pas possible, depuis une autre session Windows, ni d'ouvrir une nouvelle connexion Security BOX, ni d'accéder aux fichiers ouverts depuis la session Security BOX.

FDP_ACF.1/sessions

Lorsqu'un utilisateur ouvre un fichier, la TOE s'assure qu'il est authentifié sur sa propre session Security BOX, et avec les droits nécessaires pour l'ouverture du fichier.

6.13 Sauvegarde et restauration de fichiers

FDP_ETC.2/files

Le produit permet de sauvegarder de façon sécurisée un fichier chiffré, par exemple sur une clé USB. Le fichier est alors simplement copié "tel quel", sans déchiffrement.

FDP_ITC.2/files

La fonction de restauration va de pair avec la fonction de sauvegarde : elle permet de copier un fichier chiffré préalablement sauvegardé, le dossier de restauration devant être obligatoirement sécurisé afin de conserver la confidentialité de la donnée restaurée.