PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2011/71

Security BOX Enterprise 8.0 - Fonctionnalité de chiffrement transparent de fichiers

build 8.0.2.0

Paris, le 4 AVR 2012

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2011/71

Nom du produit

Security BOX Enterprise 8.0 - Fonctionnalité de chiffrement transparent de fichiers

Référence/version du produit

build 8.0.2.0

Conformité à un profil de protection

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 3 augmenté

ALC_FLR.3, AVA_VAN.3

Développeur(s)

ARKOON Network Security
1 Place Verrazzano
69009 LYON

Commanditaire

ARKOON Network Security
1 Place Verrazzano
69009 LYON

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Tél : +33 (0)1 30 14 19 00

Accords de reconnaissance applicables

CCRA

SOG-IS

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

L'application « **Security BOX Enterprise 8.0 - Fonctionnalité de chiffrement transparent de fichiers »** fait partie du produit « Security BOX Enterprise» développé par ARKOON Network Security.
Le produit « Security BOX Enterprise » comporte un ensemble de modules pour poste de travail sous Windows qui préserve la confidentialité des données partagées, stockées ou échangées par voie de messagerie.
Les applications faisant l'objet de la présente certification assurent la fonctionnalité de chiffrement en temps réel des fichiers, là où ils se trouvent, et de façon transparente pour l'utilisateur (module TEAM). Cette fonctionnalité assure en particulier :

- que 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 ;
- 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.

Le produit « Security BOX Enterprise » comporte d'autres modules ne faisant pas partie du périmètre de l'évaluation et qui sont listés ci-après pour mémoire :

- un module de chiffrement et de signature des courriers électroniques (module MAIL) ;
- un module de chiffrement à la demande de fichiers, en vue d'un transfert par mail ou d'une sauvegarde sécurisée (module FILE) ;
- l'effacement sécurisé et irréversible des données (module SHREDDER) ;
- la signature électronique de fichiers et de dossiers (module SIGN) ;
- le chiffrement de disques virtuels (module DISK).

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du produit est identifiable en allant dans le répertoire d'installation du produit Security Box Enterprise:

- la version du fichier *build* installée est visible en regardant les propriétés d'un fichier exécutable comme présenté ci-dessous : **version 8.0.2.0.**

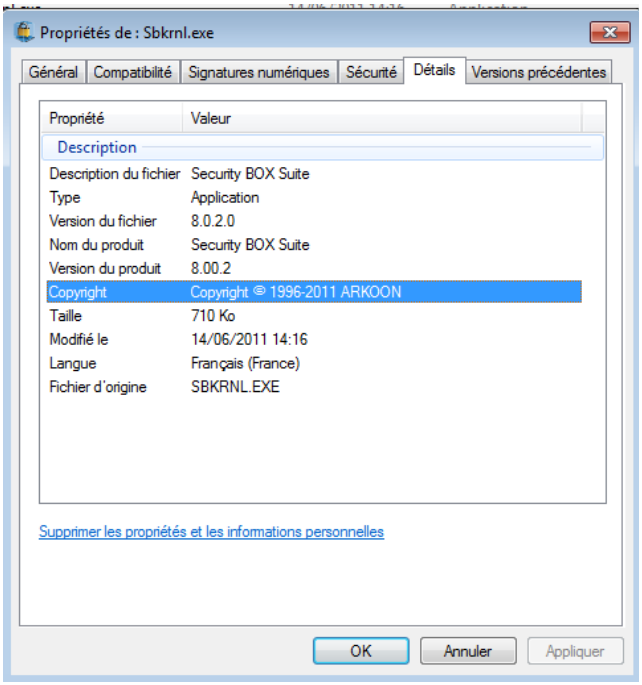

Figure 1 : Version *build* installée

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- authentification des utilisateurs ;
- protection des fichiers ;
- protection des clés de chiffrement ;
- protection des règles de sécurité partagées ;
- vérification du statut des certificats ;
- protection des comptes utilisateurs ;
- protection du fichier d'échange ;
- protection des informations résiduelles ;
- génération d'audit ;
- administration des fonctions de sécurité ;
- contrôle de l'intégrité des politiques téléchargées;
- cloisonnement des sessions.

1.2.3. Architecture

Une représentation de l'architecture de fonctionnement Security BOX Enterprise :

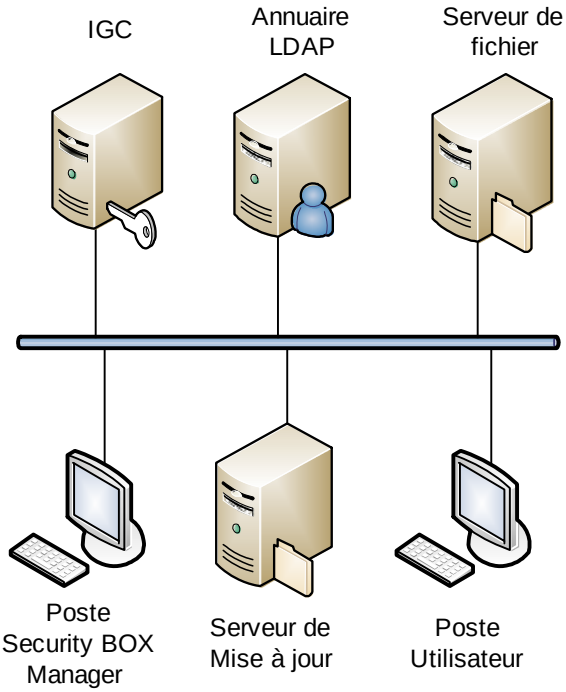

Figure 2 : Architecture de fonctionnement Security BOX Enterprise

Security BOX Enterprise réalise le chiffrement transparent en s'intégrant au noyau Windows et en s'insérant dans l'architecture des systèmes de fichier selon une technique de filtre tel que représenté ci-dessous :

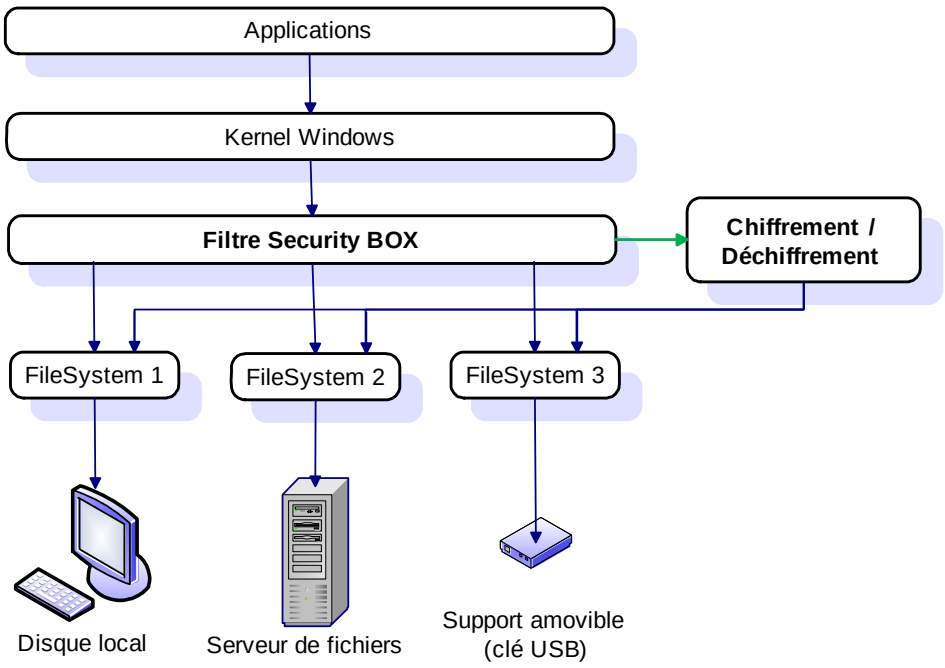

Figure 3 : Fonctionnement de Security BOX Enterprise

La cible d'évaluation (TOE[1]) est ainsi la fonctionnalité de chiffrement transparent de fichiers comprenant les modules suivants et tels que représentés ci-après :

- le module de chiffrement transparent de fichier (TEAM) ;
- le noyau Security BOX, commun à l'ensemble de la gamme, qui assure l'authentification de l'utilisateur, surveille l'inactivité du poste, gère un annuaire de certificats de confiance, et contrôle la non-révocation des certificats utilisés ;
- le noyau Security BOX Crypto qui gère les clés de l'utilisateur, qu'elles soient stockées dans un fichier (implémentation logicielle) ou dans une carte à puce.

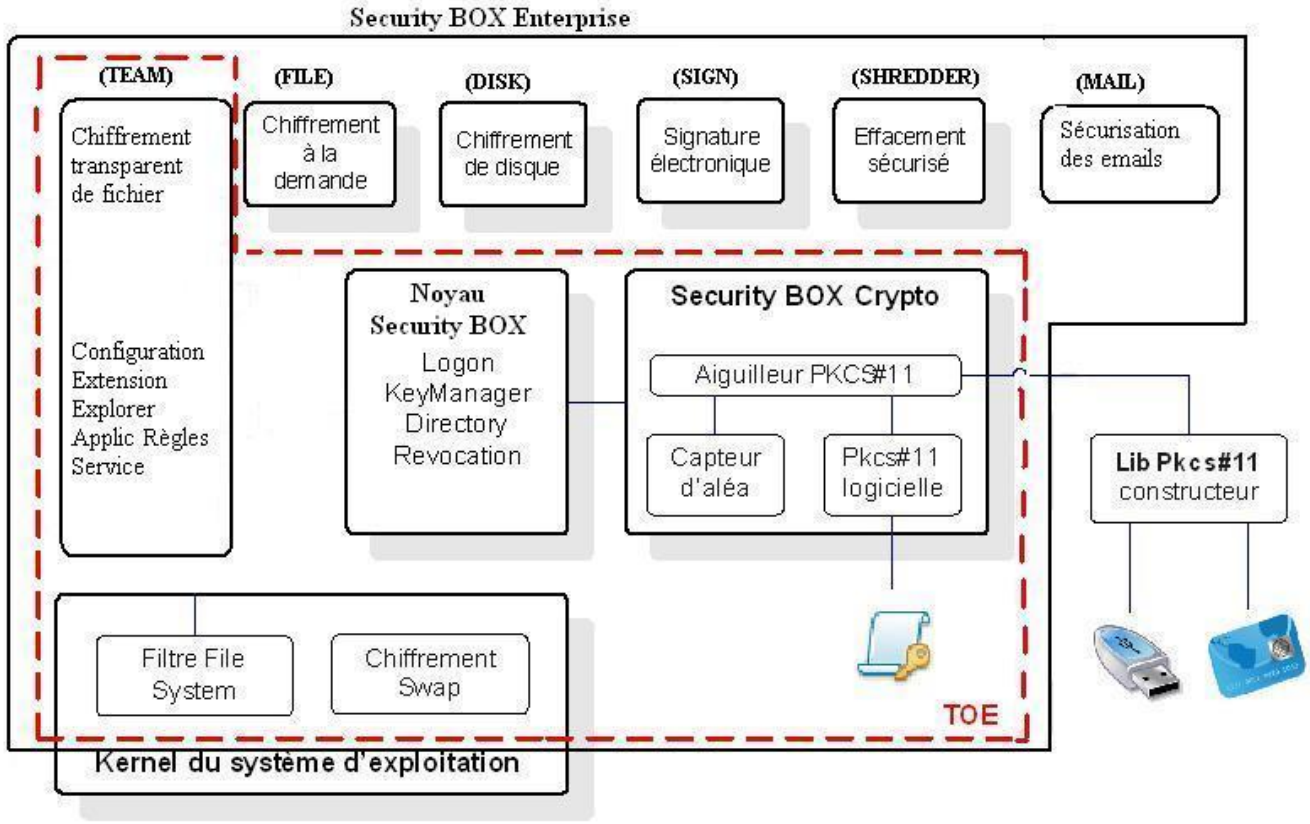

Figure 4 : TOE

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

- le développement et la livraison du produit sont réalisés sur le site d'Arkoon à Lyon ;
- l'installation, l'administration et l'utilisation du produit correspondent au déploiement du produit par le client.

Le produit a été développé sur le site suivant :

Arkoon Network Security

1 place Verrazzano
69009 LYON
France

[1] *Target Of Evaluation*

Pour l'évaluation, l'évaluateur a considéré les rôles suivants définis dans la cible de sécurité :

- l'administrateur de la sécurité (administrateur Security Box) qui est en charge de définir la politique de sécurité. Si les comptes des utilisateurs sont gérés par Security BOX Manager, l'administrateur de la sécurité crée également les comptes des utilisateurs ;
- l'administrateur système (administrateur Windows) qui est en 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 ;
- l'utilisateur qui est propriétaire de la règle de sécurité définie sur un dossier. Le propriétaire peut lire, modifier, renommer voire effacer tout fichier ou sous-dossier stocké dans le dossier sécurisé.

1.2.5. Configuration évaluée

Le certificat porte sur le module logiciel de chiffrement TEAM de Security BOX Enterprise, *build* 8.0.2.0.

Le certificat porte sur l'environnement d'exploitation suivant :

- système d'exploitation : *Microsoft Windows XP Pro 32 bits SP3* et *Microsoft Windows Seven Enterprise 32 bits* de base et SP1 ;
- un lecteur de cartes à puce de type *Omnikey Cardman 2020* avec le *middleware* Oberthur AWP 4.0.18 et une carte Oberthur Cosmo64 RSA v5.1 contenant les bi-clés et certificat d'un utilisateur légitime ;
- une infrastructure de gestion de clés (IGC) ;
- un annuaire LDAP[2] ;
- un serveur de fichiers ;
- un serveur de mise à jour de politiques de sécurité Security BOX ;
- un poste *Security BOX Authority Manager 8.0.*

[2] *Lightweight Directory Access Protocol*

La plate-forme de tests mise en œuvre par le CESTI correspond à la configuration suivante:

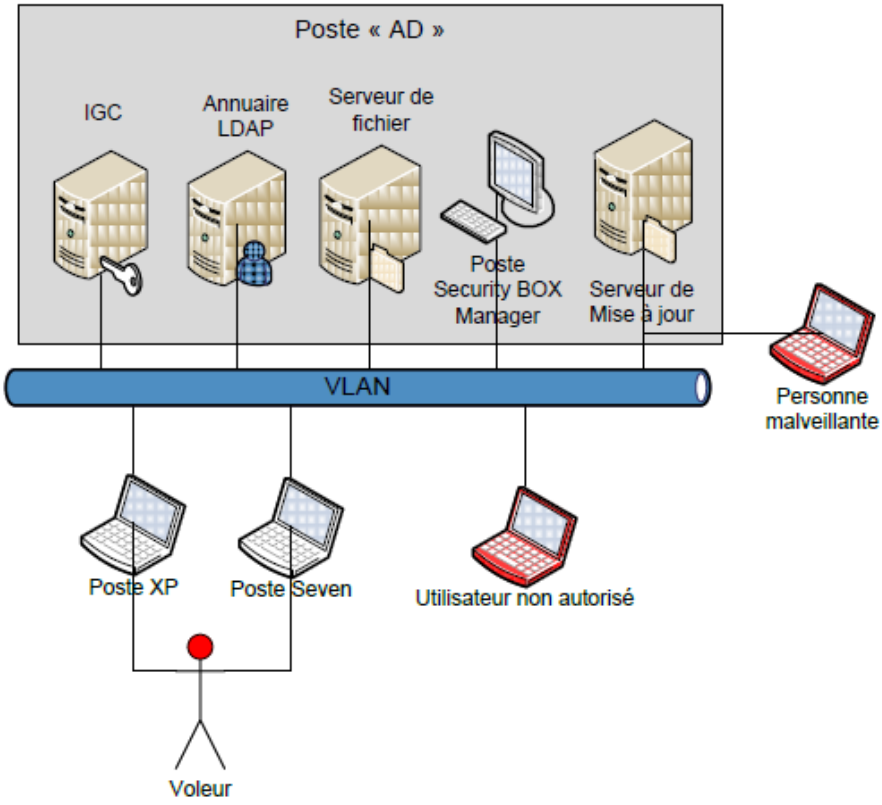

Figure 5 : Plate-forme de tests

Cette plate-forme de tests disposait de systèmes d'exploitation virtualisés et gérés par VMware Workstation 7.1. Ce choix est jugé sans conséquence sur l'évaluation de ce produit.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 21 mars 2012, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques

La cotation des mécanismes cryptographiques a été réalisée conformément aux référentiels techniques de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes utilisés ne sont pas tous conformes aux référentiels cités ci-dessus.
Cependant, les résultats de l'expertise de l'implémentation de la cryptographie, réalisée par le CESTI [EXP-CRY], ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le produit comporte un générateur d'aléas reconnu conforme aux référentiels techniques [REF] de l'ANSSI.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que l'application « Security BOX Enterprise 8.0 - Fonctionnalité de chiffrement transparent de fichiers » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- 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 (OE.ENV_OPERATIONNEL) ;
- 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_SYSTEME_CONFIANCE) ;
- l'administrateur de sécurité, en charge de la définition de la politique de sécurité, est considéré de confiance (OE.ADMIN_SECURITE_CONFIANCE) ;
- 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.SEPARATION_ROLES) ;
- 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 (OE.PSSI) ;
- les bi-clés et les certificats utilisés sont tous générés par une autorité de certification de confiance (OE.PKI) ;
- 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.SECURITY_BOX_MANAGER) ;

- 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.TOKEN_FIABLE) ;
- 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.PKCS11_EXTERNE) ;
- 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.MACHINE_HOTE_CONFIANCE) ;
- 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.CONFIGURATION_AUTHENTIFICATION) ;
- 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.AUDIT) ;
- les politiques fournies à la TOE doivent être intègres et authentiques. Elles doivent être signées par un administrateur habilité (OE.MAJ_POLITIQUES).

Enfin, afin de garantir une utilisation sécurisée du produit, les administrateurs système et de sécurité de Security BOX Enterprise, devront :

- s'assurer que les recommandations indiquées dans le guide d'Administration de Security BOX Suite et du module *Authority BOX Manager* sont bien suivies ;
- avoir pleinement conscience que les paramétrages de ces politiques ont des conséquences directes sur le bon fonctionnement du produit.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[3], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4.

[3] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[4], des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[4] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**3**	Functional specification with complete summary
	ADV_IMP				**1**	1	**2**	2		
	ADV_INT					**2**	**3**	3		
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**2**	Architectural design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**3**	Authorisation controls
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5		Implementation representation CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3		
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**		Testing: basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**3**	Focused vulnerability analysis

Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Security BOX Enterprise* – Cible de Sécurité, référence ARK/TSETA/Cible, version 1.5 du 16 mars 2012, Arkoon Network Security.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation, Projet TSETA, référence OPPIDA/CESTI/TSETA/RTE/4.0 du 21 mars 2012, OPPIDA.
[ANA-CRY]	Cotation de mécanismes cryptographiques Qualification TSETA, référence : 525/ANSSI/ACE du 3 mars 2011, ANSSI.
[EXP-CRY]	Rapport d'expertise de l'implémentation de la cryptographie TSETA, référence OPPIDA/CESTI/TSETA/CRYPTO/2.0 du 22 août 2011, OPPIDA.
[CONF]	- Security BOX – Liste des documents - trunk, référence ARK/SBE/DEV/ListeFichiersSource, version SBE trunk du 5 juillet 2011, Arkoon Network Security. - Security BOX – Liste des documents de la version v8.0 major RC-2, référence ARK/SBE/DEV/ListeFichiersSource, version SBE v8.0 major RC-2 du 14 juin 2011, Arkoon Network Security.
[GUIDES]	- Security BOX Team Chiffrement transparent et partagé, Security_BOX_Team_8_0_FR.pdf, Version 8.0 pour Windows, mars 2012, Arkoon Network Security ; - Security BOX Authority Manager, *Security_BOX_Authority_Manager_8_0.pdf*, Version 8.0 pour Windows, mars *2012*, Arkoon Network Security ; - Security BOX Suite 8.0 Guide Administration, Security_BOX_Guide_Administration_8_0_FR.pdf, Version 8.0 pour Windows, mars 2012, Arkoon Network Security ; - Security BOX Suite 8.0 Guide d'installation et de mise en œuvre, Security_BOX_Guide_Installation_8_0_fr.pdf, Version 8.0 pour Windows, mars 2012, Arkoon Network Security.

Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, RGS_B1, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, RGS_B2, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, RGS_B3, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr