PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification 2004/03

Librairie Security BOX® Crypto 6.0

Paris, le 10 mai 2004

Le Directeur central de la sécurité des systèmes d'information

Henri Serres

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 terme d'objectifs de sécurité.
Toutefois, la certification ne constitue pas en soi une recommandation du produit par le centre de certification, et ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables.

Table des matières

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 selon les ITSEC et les Critères Communs[1] sont publiques et disponibles en français sur le site Internet :

www.ssi.gouv.fr

Accords de reconnaissance des certificats

L'**accord de reconnaissance** européen du SOG-IS de 1999 permet la reconnaissance entre les Etats signataires de l'accord[2], des certificats délivrés par leur autorité de certification. La reconnaissance mutuelle européenne s'applique jusqu'au niveau ITSEC E6 et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

La direction centrale de la sécurité des systèmes d'information passe aussi des **accords de reconnaissance** avec des organismes étrangers homologues ayant leur siège en dehors des Etats membres de l'Union européenne. Ces accords peuvent prévoir que les certificats délivrés par la France sont reconnus par les Etats signataires. Ils peuvent prévoir aussi que les certificats délivrés par chaque partie sont reconnus par toutes les parties.

[1] La version 2.1 des Critères Communs est conforme à la norme internationale ISO/IEC 15408 :1999.
[2] En avril 1999, les pays signataires de l'accord SOG-IS sont : le Royaume-Uni, l'Allemagne, la France, l'Espagne, l'Italie, la Suisse, les Pays-Bas, la Finlande, la Norvège, la Suède et le Portugal.

L'accord du Common Criteria Recognition Arrangement permet la reconnaissance, par les pays signataires de l'accord[1], des certificats délivrés dans le cadre du schéma Critères Communs. La reconnaissance mutuelle s'applique au niveau EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque :

Les sites des organismes nationaux de certification des pays signataires de l'accord Common Criteria Recognition Arrangement sont :

Pays	Organisme certificateur	Site web
France	DCSSI	www.ssi.gouv.fr
Royaume-Uni	CESG	www.cesg.gov.uk
Allemagne	BSI	www.bsi.bund.de
Canada	CSE	www.cse-cst.gc.ca
Australie-Nouvelle Zélande	AISEP	www.dsd.gov.au/infosec
Etats-Unis	NIAP	www.niap.nist.gov
Japon	NITE	www.nite.go.jp

[1] En novembre 2003, les pays émetteurs de certificats signataires de l'accord sont : la France, l'Allemagne, le Royaume-Uni, les Etats-Unis, le Canada, l'Australie-Nouvelle Zélande et le Japon ; les pays signataires de l'accord qui n'émettent pas de certificats sont : l'Autriche, l'Espagne, la Finlande, la Grèce, la Hongrie, Israël, l'Italie, la Norvège, les Pays-Bas, la Suède et la Turquie.

1. Le produit évalué

1.1. Identification du produit

Le produit évalué est la librairie Security BOX® Crypto 6.0 développée par la société Méthode et Solution Informatique S.A.. Cette librairie est utilisée comme module cryptographique dans tous les produits de la gamme Security BOX®.

1.2. Le développeur

Méthode et Solution Informatique S.A.

7 rue Jean Mermoz
78000 Versailles
France

www.securitybox.net

1.3. Description du produit évalué

La librairie Security BOX® Crypto 6.0 est une librairie conforme au standard Pkcs#11 qui assure :

- le tirage et le stockage des clés privées d'un utilisateur ;
- le stockage des données sensibles de l'utilisateur ;
- le tirage d'aléa (clés de session) ;
- les calculs cryptographiques (chiffrement/déchiffrement de données ou de clés, signature, vérification de signature, calcul de condensats).

Les données sensibles de l'utilisateur sont stockées dans un fichier dit "coffre fort individuel", dont l'ouverture nécessite l'authentification préalable de l'utilisateur.
Deux modes d'authentification sont possibles :

1. sans dispositif matériel (mode "mot de passe") :
   - l'utilisateur est authentifié avec un identifiant et un mot de passe (login/password) ;
   - les clés privées de l'utilisateur sont stockées dans le "coffre fort" ;
   - les calculs à clé privée sont effectués de façon logicielle ;

2. avec un dispositif matériel (mode "carte ou clé USB") :
   - l'utilisateur est authentifié avec une carte à puce (ou une clé USB) et un code "PIN";
   - les clés privées sont stockées dans la carte ;
   - les calculs à clé privée sont effectués par la carte.

1.3.1. Architecture

La librairie Security BOX® Crypto 6.0 est constituée des trois fichiers suivants :

Nom	Version	Description
sbp11.dll	6.0.2.0	intègre la librairie Pkcs#11 logicielle, les fonctions

		d'accès au « coffre-fort » et le générateur d'aléa.
sbp11ka.dll	6.0.2.0	nécessaire uniquement en mode "carte ou clé USB" : assure l'interface avec la librairie Pkcs#11 de la carte utilisée.
p11msidll.lib	6.0.2.0	librairie Pkcs#11 logicielle, incluse dans **sbp11.dll** et dans certains composants de Security BOX® Suite.

1.3.2. Périmètre et limites du produit évalué

La librairie Security BOX® Crypto est évaluée, en tant que produit, sur une plate-forme PC sous les systèmes d'exploitation de Microsoft Windows 95/98/Me/NT/2000/XP.

L'évaluation a porté sur le fonctionnement complet de la librairie quand elle est utilisée en mode "mot de passe" et la mise en œuvre du dispositif cryptographique matériel quand elle est utilisée en mode "carte ou clé USB". La protection des données stockées sur ces dispositifs matériels n'a pas été évaluée.

1.4. Utilisation et administration

1.4.1. Utilisation

Les utilisateurs de la librairie sont les développeurs des produits de la suite Security BOX®. Les utilisateurs finaux n'interagissent pas directement avec la librairie évaluée.

1.4.2. Administration

La librairie n'est pas administrée, elle est utilisée telle qu'elle par les développeurs des produits (voir chapitre précédent).

2. L'évaluation

2.1. Centre d'évaluation

OPPIDA

13, route de la minière – Bât. 134
78000 Versailles Satory
France

Téléphone : +33 (0)1 30 83 27 95

Adresse électronique : contact@oppida.fr

L'évaluation s'est déroulée de décembre 2002 à janvier 2004.

2.2. Commanditaire

Méthode et Solution Informatique S.A.

7 rue Jean Mermoz
78000 Versailles
France

www.securitybox.net

2.3. Référentiels d'évaluation

L'évaluation a été menée conformément à la norme internationale ISO/IEC 15408 [IS 15408], à la méthodologie d'évaluation définie dans le manuel CEM [CEM], et à l'ensemble des interprétations finales listées dans les rapports d'évaluation.

2.4. Evaluation de la cible de sécurité

La cible de sécurité [ST] définit le produit évalué et son environnement d'exploitation.
Toutes les exigences fonctionnelles et d'assurance de la cible de sécurité sont extraites respectivement de la partie 2 et de la partie 3 de l'IS 15408 [IS 15408].
La cible de sécurité répond aux exigences de la classe ASE.

2.5. Evaluation du produit

L'évaluation consiste à vérifier que le produit et sa documentation respectent les exigences fonctionnelles et d'assurance définies dans la cible de sécurité [ST].

2.5.1. Développement du produit

La classe d'assurance ADV – développement – définit les exigences de raffinement pas à pas des fonctions de sécurité du produit depuis ses spécifications globales dans la cible de sécurité [ST] jusqu'à l'implémentation. Chacune des représentations des fonctions de sécurité du

produit qui résultent de ce processus fournit des informations qui aident l'évaluateur à déterminer si les exigences fonctionnelles du produit ont été satisfaites.
L'analyse des documents associés à la classe ADV montre que les exigences fonctionnelles sont correctement et complètement raffinées dans les différents niveaux de représentation du produit (spécifications fonctionnelles (FSP), sous-systèmes (HLD), modules (LLD) et implémentation (IMP)), jusqu'à l'implémentation de ses fonctions de sécurité.
Les documents fournis pour la classe ADV – développement – répondent aux exigences de la partie 3 de l'IS 15408 [IS 15408] en terme de contenu et de présentation des éléments de preuve.

2.5.2. Documentation

Du point de vue de l'évaluation, les utilisateurs sont les développeurs des applications de la suite Security BOX® qui utilisent la librairie évaluée. Les utilisateurs finaux de ces applications n'interagissent pas directement avec les interfaces de la librairie évaluée.
Du point de vue de l'évaluation, il n'y a pas d'administrateur de la librairie.
Les guides utilisateur fournis [USR] répondent aux exigences de la partie 3 de l'IS 15408 [IS 15408] en terme de contenu et de présentation des éléments de preuve.

2.5.3. Livraison et installation

La livraison est considérée juste après le développement du produit. L'application développée est livrée aux développeurs des produits de la suite Security BOX® qui intègrent la librairie évaluée. La librairie et son sceau sont disponibles en téléchargement sur le site intranet de MSI. Ce sceau permet de vérifier l'intégrité des fichiers téléchargés.
Cette procédure de livraison [DEL] est suffisante pour répondre aux exigences demandées : elle permet de détecter une modification du produit qui aurait pu avoir lieu pendant sa livraison.
L'installation du produit correspond à la phase d'installation de ces librairies dans l'environnement de développement des produits de la suite Security BOX®. Les procédures d'installation, de génération et de démarrage [IGS] permettent d'obtenir une configuration sûre.
Les documents fournis pour la classe ADO – livraison et opération – répondent aux exigences de la partie 3 de l'IS 15408 [IS 15408] en termes de contenu et de présentation des éléments de preuve.

2.5.4. L'environnement de développement

MSI utilise un système de gestion de configuration automatisé pour gérer le code source du produit et la documentation associée. Les erreurs détectées ainsi que toutes les demandes d'évolution du logiciel sont également suivies. Le système de gestion de configuration mis en place par MSI permet également de soutenir la génération du produit (compilation). Enfin, il a été vérifié que ce système est utilisé conformément au plan de gestion de configuration fourni.
Les procédures de gestion de configuration et de génération de l'application sont efficaces pour s'assurer de l'intégrité du produit généré ; c'est-à-dire que les bons éléments du code source ont été utilisés pour compiler l'application.

Le produit est développé sur le site de MSI situé :

3, place de Renaudel
69003 Lyon
France

Les mesures de sécurité décrites dans les procédures fournissent le niveau nécessaire de protection pour maintenir la confidentialité et l'intégrité du produit évalué et de sa documentation.
La vérification de la mise en œuvre des procédures de développement et de gestion de configuration a été effectuée par une visite du site de MSI Lyon (cf Annexe 1). Le rapport de visite se trouve sous la référence [Visite].
Les documents fournis pour la classe ACM – gestion de la configuration – et ALC – support au cycle de vie – répondent aux exigences de la partie 3 de l'IS 15408 [IS 15408] en termes de contenu et de présentation des éléments de preuve.

2.5.5. Tests fonctionnels

MSI a fourni sa documentation de test qui identifie toutes les fonctionnalités testées. L'évaluateur a vérifié que toutes les fonctions de sécurité et les interfaces de la spécification fonctionnelle du produit sont reliées à au moins un test fonctionnel. Il a également vérifié que les interfaces des sous-systèmes du produit décrits dans la conception de haut niveau, sont couvertes par des tests du développeur.
L'évaluateur a également développé ses propres tests fonctionnels qui ont été réalisés sur les plate-formes Microsoft Windows 95/98/Me/NT/2000/XP. Ces tests complémentaires ont démontré que le produit réalise bien les fonctions de sécurité identifiées dans les spécifications fonctionnelles.

2.5.6. Estimation des vulnérabilités

Toutes les vulnérabilités identifiées par le développeur ont été vérifiées par une analyse complétée de tests. L'évaluateur conclut que les vulnérabilités identifiées par le développeur ont été correctement prises en compte dans la conception du produit.
L'évaluateur a également réalisé une analyse de vulnérabilité indépendante, dont les résultats ne montrent pas de vulnérabilités exploitables au niveau d'évaluation considéré.
Le produit dans son environnement d'exploitation est résistant à des attaquants disposant d'un potentiel d'attaque **moyen**.

3. Conclusions de l'évaluation

3.1. Rapport technique d'évaluation

Le rapport technique d'évaluation [RTE] décrit les résultats de l'évaluation de la librairie Security BOX® Crypto 6.0.

3.2. Niveau d'évaluation

La librairie Security BOX® Crypto 6.0e a été évaluée selon la norme internationale ISO/IEC 15408 [IS 15408] et sa méthodologie [CEM] au niveau **EAL4**[1] **augmenté des composants d'assurance suivants**, conformes à la partie 3 de l'IS 15408 [IS 15408] :

Composants	Descriptions
AVA_VLA.3	Moderatly resistant

Tableau 1 - Augmentations

Pour tous les composants, les verdicts suivants ont été émis :

Class ASE	Security Target evaluation	
ASE_DES.1	TOE description	Réussite
ASE_ENV.1	Security environment	Réussite
ASE_INT.1	ST introduction	Réussite
ASE_OBJ.1	Security objectives	Réussite
ASE_PPC.1	PP claims	Réussite
ASE_REQ.1	IT security requirements	Réussite
ASE_SRE.1	Explicitly stated IT security requirements	Réussite
ASE_TSS.1	Security Target, TOE summary specification	Réussite
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	Réussite
ACM_CAP.4	Generation support and acceptance procedures	Réussite
ACM_SCP.2	Problem tracking CM coverage	Réussite
Class ADO	**Delivery and operation**	
ADO_DEL.2	Detection of modification	Réussite
ADO_IGS.1	Installation, generation, and start-up procedures	Réussite
Class ADV	**Development**	

[1] Annexe 4: tableau des différents niveaux d'assurance d'évaluation (EAL – Evaluation Assurance Level) prédéfinis dans l'IS 15408 [IS 15408].

ADV_FSP.2	Fully defined external interfaces	Réussite
ADV_HLD.2	Security enforcing high-level design	Réussite
ADV_IMP.1	Subset of the implementation of the TSF	Réussite
ADV_LLD.1	Descriptive low-level design	Réussite
ADV_RCR.1	Informal correspondence demonstration	Réussite
ADV_SPM.1	Informal TOE security policy model	Réussite
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Réussite
AGD_USR.1	User guidance	Réussite
Class ALC	**Life cycle support**	
ALC_DVS.1	Identification of security measures	Réussite
ALC_LCD.1	Developer defined life-cycle model	Réussite
ALC_TAT.1	Well-defined development tools	Réussite
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	Réussite
ATE_DPT.1	Testing: high-level design	Réussite
ATE_FUN.1	Functional testing	Réussite
ATE_IND.2	Independent testing - sample	Réussite
Class AVA	**Vulnerability assessment**	
AVA_MSU.2	Validation of analysis	Réussite
AVA_SOF.1	Strength of TOE security function evaluation	Réussite
AVA_VLA.3	Moderatly resistant	Réussite

Tableau 2 - Composants et verdicts associés

3.3. Exigences fonctionnelles

Le produit répond aux **exigences fonctionnelles de sécurité** suivantes[1]. Les opérations sur ces exigences sont décrites dans la cible de sécurité [ST].

- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.3 Cryptographic key access
- FCS_CKM.4 Cryptographic key destruction
- FCS_COP.1 Cryptographic operation
- FDP_ACC.2 Complete access control
- FDP_ACF.1 Security attribute based access control
- FDP_ETC.1 Export of user data without security attributes
- FDP_ITC.1 Import of user data without security attributes
- FDP_RIP.2 Full residual information protection
- FDP_SDI.2 Stored data integrity monitoring and action
- FIA_UAU.2 User authentication before any action
- FIA_UID.2 User identification before any action

[1] Annexe 3 : tableau des exigences fonctionnelles de sécurité du produit évalué.

- FMT_MSA.1 Management of security attributes
- FMT_MSA.2 Secure security attributes
- FMT_MSA.3 Static attribute initialisation
- FMT_SMR.1 Security roles
- FPT_FLS.1 Failure with preservation of secure state
- FTA_SSL.2 User-initiated locking

3.4. Résistance des fonctions

Les fonctions d'authentification des utilisateurs (pour les fonctions TransKeyStore, Login et SetPIN) ont fait l'objet d'une estimation du niveau de résistance. Il est conseillé dans les guides d'utilisation [USR] d'utiliser des mots de passe d'une taille supérieure à 8 caractères.
Le niveau de résistance de ces fonctions est par conséquent jugé **élevé** (**SOF-high**).

3.5. Analyse des mécanismes cryptographiques

Les mécanismes cryptographiques ont été analysés dans le cadre de l'évaluation (cf Annexe 2).

3.6. Conformité à un profil de protection

(Sans objet)[1]

3.7. Reconnaissance européenne (SOG-IS)

Ce certificat a été émis dans les conditions de l'accord du SOG-IS. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].

3.8. Reconnaissance internationale (CC RA)

Ce certificat a été émis dans les conditions de l'accord du CC RA. Les dispositions de cet accord nécessitent la fourniture de la cible de sécurité [ST].
Les augmentations suivantes ne sont par reconnues dans le cadre du CC RA [CC RA] : AVA_VLA.3 (Tableau 1).

3.9. Restrictions d'usage

L'environnement d'exploitation doit respecter les objectifs de sécurité sur l'environnement (§ 3.10) ainsi que les recommandations se trouvant dans les guides d'utilisation du produit [USR et IGS]. Il faut notamment respecter les recommandations issues de l'analyse des mécanismes cryptographiques (voir Annexe 2).

Les résultats de l'évaluation ne sont valables que dans la configuration spécifiée dans le présent rapport de certification.

[1] La cible de sécurité [ST] du produit ne revendique pas de conformité à un profil de protection.

3.10. Objectifs de sécurité sur l'environnement

Les objectifs de sécurité suivants sont extraits de la cible de sécurité du produit [ST § 4.2] :

- l'environnement physique de la librairie doit permettre aux utilisateurs d'entrer leur mot de passe (ou code PIN) sans être observable directement ou interceptable (clavier sans fil,…) par d'autres utilisateurs ou attaquants potentiels ;
- le PC de l'utilisateur doit être périodiquement inspecté physiquement et doit posséder un logiciel anti-virus à jour ;
- les applications s'appuyant sur la librairie doivent sélectionner des algorithmes cryptographiques pour lesquels aucune vulnérabilité n'est connue et des tailles de clés suffisamment longues pour rendre impossible toute attaque par force brute (essais exhaustifs de toutes les clés possibles) ;
- les applications s'appuyant sur la librairie doivent proposer à l'utilisateur une aide pour la création de mots de passe, lui permettant d'estimer la robustesse de son mot de passe se basant sur sa longueur, sa non trivialité, le nombre de caractères alphanumériques et spéciaux qu'il contient ;
- l'utilisateur doit s'assurer de la non divulgation de son mot de passe (ou code PIN) et de son renouvellement périodique ;
- l'utilisateur doit conserver le mot de passe de l'officier de sécurité associé à son "coffre-fort individuel" dans une enveloppe scellée placée dans une armoire fermant à clé ;
- les applications s'appuyant sur la librairie doivent proposer à l'utilisateur la possibilité de vérifier l'intégrité de la librairie, par exemple par l'utilisation d'un outil de contrôle de scellement (type MD5) ;
- les applications s'appuyant sur la librairie doivent fournir un mécanisme permettant de déclencher le verrouillage par la librairie du « coffre-fort » individuel d'un utilisateur connecté, en cas d'inactivité prolongée dont la durée est paramétrable par l'utilisateur et/ou en cas de lancement du verrouillage d'écran du PC ;
- l'utilisateur doit sauvegarder, à chaque modification, le fichier contenant son "coffre-fort individuel" (fichier .usr) et placer le support de sauvegarde dans une armoire fermant à clé ;
- l'utilisateur doit générer suffisamment de bruit lors de la création des aléas (mouvement de la souris, frappe de touches au clavier) pour assurer une bonne qualité d'aléas.

3.11. Synthèse des résultats

L'ensemble des travaux réalisés par le centre d'évaluation est accepté par le centre de certification qui atteste que la librairie Security BOX® Crypto 6.0 identifiée au paragraphe 1.1 et décrit au paragraphe 1.3 du présent rapport **est conforme** aux exigences spécifiées dans la cible de sécurité [ST]. L'ensemble des travaux d'évaluation et les résultats de ces travaux sont décrits dans le rapport technique d'évaluation [RTE].

Annexe 1. Rapport de visite du site MSI Lyon

Le site de développement de MSI situé à Lyon, 3 place Renaudel, 69003 Lyon, France, a fait l'objet, dans le cadre de l'évaluation de la librairie Security BOX® Crypto 6.0, d'une visite sur site pour vérifier la conformité aux critères d'évaluation et aux documents fournis pour ce qui concerne :

- la gestion de configuration : **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- la livraison du produit évalué : **ADO** (ADO_DEL.2) ;
- le support au cycle de vie : **ALC** (ALC_DVS.1).

La visite par le centre d'évaluation, accompagné d'un représentant de la DCSSI, a permis de conclure que les critères sont satisfaits sur ce site.

Annexe 2. Analyse des mécanismes cryptographiques

Les mécanismes de nature cryptographiques suivants ont été analysés :

- les mécanismes directement utilisés par la librairie pour protéger les informations stockées dans le « coffre-fort » ;
- les fonctions PKCS#11 offertes par la librairie ;
- le générateur d'aléas.

Les mécanismes de protection du « coffre-fort » atteignent un niveau de résistance élevé si :

- les clés utilisées ont une taille strictement supérieure à 64 bits ;
- l'algorithme DES simple n'est pas employé pour le chiffrement des champs « private » ;
- l'intégrité est contrôlée en utilisant l'algorithme HMAC dans les versions utilisant des clés d'au moins 128 bits et les algorithmes SHA-1 ou MD5 (l'algorithme MD2 ne doit pas être utilisé).

Pour les fonctions offertes par la librairie, il est conseillé pour atteindre un niveau de résistance élevé :

- de ne pas utiliser l'algorithme MD2 ;
- de ne pas utiliser l'algorithme de signature RSA ISO 9796 ;
- de ne pas utiliser la méthode de padding PKCS#7 au sein des protocoles SSL/TLS, IPSEC, WTLS et d'analyser avec soin toute autre utilisation.

Le générateur d'aléas utilise un mécanisme de retraitement de niveau élevé.

Annexe 3. Exigences fonctionnelles de sécurité du produit évalué

Attention : les descriptions des composants fonctionnels suivants sont données à titre indicatif. Seule une lecture attentive de la cible de sécurité ([ST]) peut apporter la description exacte des exigences fonctionnelles du produit.

Class FCS	**Cryptographic support**
Cryptographic key management	
FCS_CKM.1	*Cryptographic key generation* Le produit doit générer des clés cryptographiques conformément à un algorithme et des tailles de clés spécifiées qui peuvent être basées sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.3	*Cryptographic key access* Les accès aux clés cryptographiques doivent être effectués conformément à une méthode d'accès spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
FCS_CKM.4	*Cryptographic key destruction* Le produit doit détruire les clés cryptographiques conformément à une méthode de destruction spécifiée qui peut être basée sur une norme identifiée. Les paramètres de cette exigence sont spécifiés dans la cible de sécurité [ST].
Cryptographic operation	
FCS_COP.1	*Cryptographic operation* Le produit doit exécuter des opérations cryptographiques conformément à un algorithme spécifié et des clés cryptographiques dont les tailles peuvent prendre plusieurs valeurs spécifiées. L'algorithme et les tailles des clés cryptographiques spécifiés peuvent être basés sur une norme identifiée (spécifiés dans la cible de sécurité [ST]).
Class FDP	**User data protection**
Access control policy	
FDP_ACC.2	*Complete access control* Chaque règle de contrôle d'accès identifiée doit s'appliquer à toutes les opérations sur les sujets et objets couverts par cette règle. De plus tous les objets et toutes les opérations doivent être couverts par au moins une règle de contrôle d'accès identifiée.
Access control functions	
FDP_ACF.1	*Security attribute based access control* Le produit doit mettre en œuvre des accès basés sur des attributs de sécurité et des groupes d'attributs désignés. Il peut aussi offrir l'aptitude d'autoriser ou de refuser explicitement l'accès à un objet sur la base d'attributs de sécurité.
Export to outside TSF control	
FDP_ETC.1	*Export of user data without security attributes* Le produit doit appliquer les règles de sécurité appropriées lors de l'exportation de données de l'utilisateur à l'extérieur. Les données de l'utilisateur exportées par cette fonction le sont sans les attributs de sécurité qui leur sont associés.
Import from outside TSF control	
FDP_ITC.1	*Import of user data without security attributes* Les attributs de sécurité doivent représenter correctement les données de

	l'utilisateur et doivent être fournis séparément de l'objet.
Residual information protection	
FDP_RIP.2	*Full residual information protection* Le produit doit garantir que toutes les informations résiduelles contenues dans n'importe quelle ressource ne sont pas disponibles pour tous les objets du TSC lors de l'allocation ou de la désallocation de la ressource.
Stored data integrity	
FDP_SDI.2	*Stored data integrity monitoring and action* Le produit doit contrôler les données des utilisateurs stockées pour rechercher des erreurs d'intégrité identifiées et entreprendre des actions (spécifiées dans la cible de sécurité [ST]) suite à une détection d'erreur.
Class FIA	**Identification and authentication**
User authentication	
FIA_UAU.2	*User authentication before any action* Les utilisateurs doivent s'authentifier avant que toute action ne soit autorisée.
User identification	
FIA_UID.2	*User identification before any action* Les utilisateurs doivent s'identifier avant que toute action ne soit autorisée.
Class FMT	**Security management**
Management of security attributes	
FMT_MSA.1	*Management of security attributes* Les utilisateurs autorisés doivent pouvoir gérer les attributs de sécurité spécifiés.
FMT_MSA.2	*Secure security attributes* Le produit doit garantir que les valeurs assignées aux attributs de sécurité sont valides par rapport à l'état sûr.
FMT_MSA.3	*Static attribute initialisation* Le produit doit garantir que les valeurs par défaut des attributs de sécurité sont soit de nature permissive soit de nature restrictive.
Security management roles	
FMT_SMR.1	*Security roles* Les rôles relatifs à la sécurité que le produit reconnaît doivent être identifiés et associés à des utilisateurs (spécifiés dans la cible de sécurité [ST]).
Class FPT	**Protection of the TSF**
Fail secure	
FPT_FLS.1	*Failure with preservation of secure state* Le produit doit préserver un état sûr dans le cas de défaillances identifiées.
Class FTA	**TOE access**
Session locking	
FTA_SSL.2	*User-initiated locking* Ce composant offre des capacités pour que l'utilisateur verrouille et déverrouille ses propres sessions interactives.

Annexe 4. Niveaux d'assurance prédéfinis IS 15408 ou CC

Classe	Famille	Composants par niveau d'assurance						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Classe ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Classe ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Classe ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Classe AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Classe ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Classe ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Classe AVA Estimation des vulnérabilités	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Annexe 5. Références documentaires du produit évalué

[ST]	Security BOX® Crypto 6.0 - Cible de sécurité CC niveau EAL4+ - v2.6 du 09/01/2004
[USR]	Security BOX® Crypto 6.0 - Guide utilisateur v1.3 du 04/12/2003
[DEL]	Security BOX® Crypto 6.0 - Procédure de livraison de la cible v1-0 du 08/10/2003
[IGS]	Security BOX® Crypto 6.0 - Procédure de génération de la cible v1-0 du 22/08/2003 Security BOX® Crypto 6.0 – Guide administrateur v1-0 du 07/07/2003
[Visite]	Compte-rendu visite sur site v1.0, réf OPPIDA/CESTI/TANGO/CRR.000/1, 18 juin 2003. Compte-rendu suivi visite sur site v1.0, réf OPPIDA/CESTI/TANGO/CRP.004/1, 11 septembre 2003
[RTE]	Rapport technique d'évaluation, réf. OPPIDA/CESTI/TANGO/RTE/1.2, 10/02/2004

Annexe 6. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[IS 15408]	Norme Internationale ISO/IEC 15408:1999, comportant 3 documents : ▪ ISO/IEC 15408-1: Part 1 Introduction and general model; ▪ ISO/IEC 15408–2: Part 2 Security functional requirements; ▪ ISO/IEC 15408–3: Part 3 Security assurance requirements.
[CEM]	Méthodologie d'évaluation de la sécurité des technologies de l'information: ▪ Part 2: Evaluation Methodology, august 1999, version 1.0, ref CEM- 99/045.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, may 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Bureau certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr