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-2012/07

ZoneCentral, version 5.0, build 960

Paris, le 13 février 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-2012/07**
Nom du produit **ZoneCentral**
Référence/version du produit **version 5.0, build 960**
Conformité à un profil de protection **Néant**
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 **Prim'X Technologies SA** **10 place Charles Béraudier, 69428 Lyon Cedex 03, France**
Commanditaire **Prim'X Technologies SA** **10 place Charles Béraudier, 69428 Lyon Cedex 03, France**
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, mél : cesti@oppida.fr**
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

Le produit évalué est « ZoneCentral, version 5.0, build 960» développé par Prim'X Technologies.

Ce produit est utilisé pour assurer la confidentialité de fichiers manipulés par des utilisateurs sur des postes isolés, des ordinateurs portables, ou des postes de travail connectés à un réseau d'entreprise. Il permet de chiffrer des fichiers, sans modifier leurs caractéristiques (emplacement, nom, date, taille). Ce chiffrement est réalisé de la façon la plus transparente possible pour les utilisateurs : en effet, le chiffrement et le déchiffrement des fichiers s'effectuent « *in-place* » (là où résident les fichiers, donc sans impact sur l'organisation des données de l'utilisateur) et « *à la volée* » (à la demande de l'utilisateur, sans manipulation particulière en dehors de la saisie des codes d'accès aux clés nécessaires).

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].

Le numéro de la version du produit est intégré au nom des fichiers exécutables :

- pour Windows Seven 32 bits : « Setup ZoneCentral 5.0 x86(960).exe »,
- pour Windows Seven 64 bits : « Setup ZoneCentral 5.0 x64(960).exe ».

Une fois le produit installé, la version certifiée du produit (« 5.0.0960 » ou « version 5.0, build 960 ») est identifiable par les moyens suivants

- en consultant les propriétés des binaires installés ;
- en lançant l'outil « zcacmd.exe » ;
- en consultant la fenêtre « A propos ».

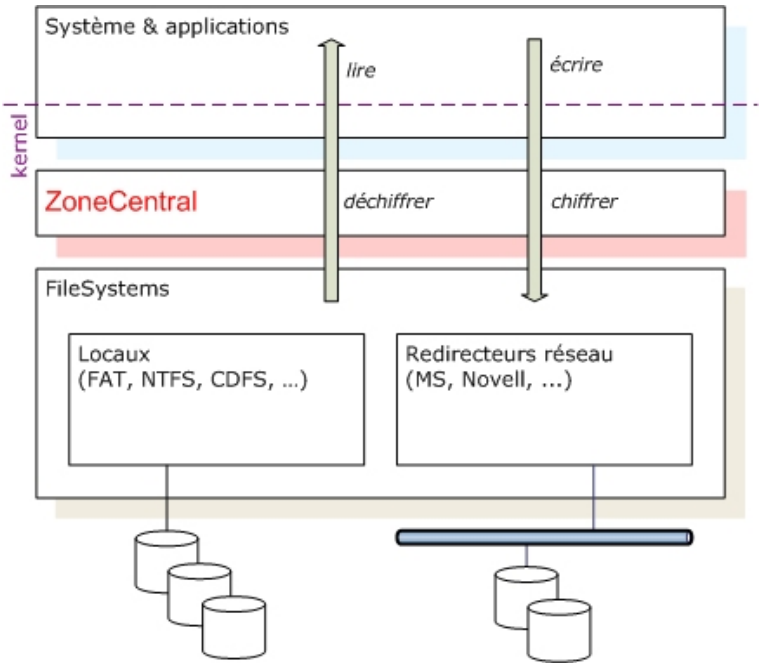
L'intégrité du produit peut être vérifiée par comparaison des empreintes Authenticodes générées par l'utilisateur ou l'administrateur avec celles disponibles sur le site web du développeur.

1.2.2. Services de sécurité

Les services de sécurité évalués du produit sont :
- l'administration du produit ;
- la définition et la gestion des zones chiffrées (chiffrement/déchiffrement, nettoyage des traces claires des données chiffrées, reprise en cas de problème, affichage des informations de zone, etc.) ;
- les opérations cryptographiques pour la gestion des clés de zones (création, accès, suppression) et les opérations de calcul associées, réalisées dans des zones mémoires dédiées ;
- la gestion des droits d'accès aux zones chiffrées ;
- l'audit des événements liés aux opérations réalisées par le produit.

1.2.3. Architecture

Sous Windows, un fichier appartient à un système de gestion de fichiers, qui le stocke et le gère (NTFS, FAT, CDFS …). Tous les systèmes de gestion de fichiers offrent des méthodes d'accès aux fichiers qu'ils hébergent, sous une forme relativement homogène et universelle, de façon à ce que les applications qui accèdent aux fichiers n'aient normalement pas à se préoccuper de la nature du système de gestion de fichiers qui héberge leurs fichiers.
Toute application, tout composant système sous Windows qui accède à un fichier (ouvrir un fichier, lire une partie de son contenu, écrire, réécrire, ajouter de l'information, etc.) soumet ses requêtes à un mécanisme qui les confie au système de gestion de fichiers concerné par le fichier en question.
ZoneCentral s'intègre au noyau Windows et se positionne dans les chaînes de systèmes de gestion de fichiers, selon une technologie de filtre prévue justement dans ces chaînes. Ainsi positionné, il reçoit (et retransmet ensuite à l'élément suivant de la chaîne) toutes les requêtes passées sur tous les fichiers de tous les systèmes de gestion de fichiers qu'il filtre. Au passage de ces requêtes, il est en mesure d'effectuer certaines opérations lorsque c'est nécessaire : déchiffrer la portion lue lorsqu'il s'agit d'une lecture d'un fichier chiffré, ou au contraire chiffrer la portion écrite lorsqu'il s'agit d'une écriture d'un fichier chiffré, ou encore effectuer un effacement par surcharge lorsqu'un fichier est supprimé.



Ce produit agissant comme une couche de sécurité intégrée au système, il est transparent pour les utilisateurs et permet d'appliquer la politique de sécurité à tous les systèmes de fichiers : locaux, amovibles, réseau …

Les éléments suivants sont inclus dans le périmètre de l'évaluation :
- le dialogue PKCS#11 entre la TOE et les porte-clés utilisateurs ;
- le dialogue PKCS#12 entre la TOE et les fichiers de clés ;
- le dialogue réseaux entre la TOE et les données utilisateurs stockées sur des médias distants (serveur sur un réseau local ou sur Internet par exemple).

Les éléments suivants sont en dehors du périmètre de l'évaluation :
- le dialogue clavier entre la TOE et la saisie des mots de passe ;
- les systèmes d'exploitation Windows, y compris :
    - les drivers PC/SC ;
    - le service de gestion des certificats (CMS) ;
    - le service de gestion des profils utilisateurs (User management) ;
- les porte-clés utilisés (comme les porte-clés de type Token USB, les fichiers de clés ou les containers CSP) ;
- le tirage des clés d'accès utilisateur (clés RSA dans des porte-clés ou mots de passe fournis par l'administrateur du produit) ;
- l'outil GPOSign.exe permettant à l'administrateur de sécurité de signer les politiques. Par contre la vérification de la signature des politiques par ZoneCentral fait bien partie du périmètre de la TOE ;
- l'utilisation du mode SSO (*Single Sign On*) qui permet d'ouvrir automatiquement les zones chiffrées lorsque la session Windows est ouverte (mais reporte le niveau de sécurité à celui de Windows ou du composant SSO tiers).

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 de PRIM'X 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 :

Prim'X Technologies

10 Place Charles Béraudier
69428 Lyon Cedex 03
France

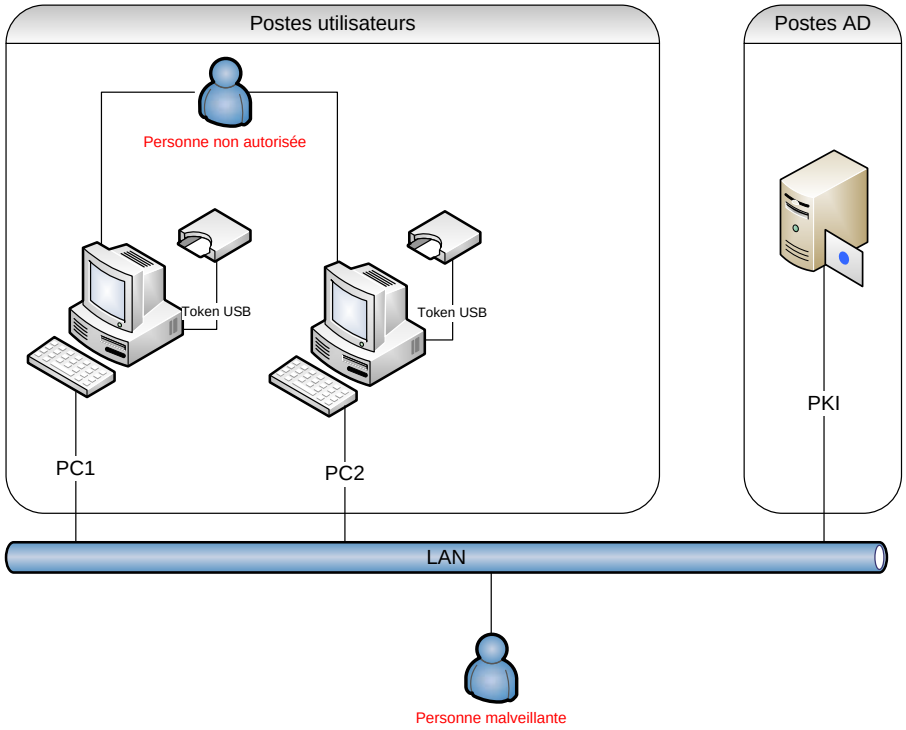
1.2.5. Configuration évaluée

Le certificat porte ainsi sur les environnements d'exploitation suivants :
- systèmes d'exploitation : Microsoft Windows Seven 32 bits et Microsoft Windows Seven 64 bits ;
- interfaces avec les supports des clés RSA d'accès aux zones : PKCS#11 (pour les porte-clés) et PKCS#12 (pour les fichiers de clés).

Les différents types de supports de clés envisageables n'ont pas été pris en compte dans la cadre de cette évaluation, seules les interfaces mentionnées ci-dessus l'ont été.

La cible d'évaluation correspond à ZoneCentral 5.0 en version installable et exécutable.

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



Cette plate-forme de tests disposait de systèmes d'exploitation virtualisés. Ce choix est sans conséquence sur l'évaluation de ce produit. En effet, le produit s'intègre au noyau de Windows et se positionne dans les chaînes de systèmes de gestion de fichiers (ZoneCentral agit comme un filtre logique entre le système d'exploitation et le système de fichier proposé par la machine hôte), et la technologie de virtualisation agit en amont de ces processus.
Les supports de clés qui ont été utilisés sur cette plate-forme sont l'eToken 72K pro de la marque Aladdin, le magasin de certificats Windows et un containeur de clés PKCS#12.

Le certificat porte ainsi sur l'environnement d'exploitation suivant :
- systèmes d'exploitation : Microsoft Windows Seven 32 et 64 bits ;
- interfaces avec les supports des clés d'accès aux zones : PKCS#11 et PKCS#12.

2. L'évaluation

2.1. Référentiels d'évaluation

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

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 février 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 selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée par l'ANSSI conformément à ses référentiels techniques [REF-CRY] et [REF-KEY]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] : les mécanismes analysés sont conformes aux exigences de [REF-CRY] et [REF-KEY].

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [EXP-CRY]. Ces résultats 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 générateur d'aléa utilisé par le produit et le retraitement d'aléas qu'il met en œuvre sont conformes au référentiel [REF-CRY].

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 le produit « ZoneCentral, version 5.0, build 960 » 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 opérationnel 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 physique d'utilisation du produit doit permettre aux utilisateurs et aux administrateurs d'entrer leur mot de passe sans qu'il ne soit directement observable ou sans que sa saisie ne soit interceptable par d'autres utilisateurs ou attaquants potentiels ; des mesures organisationnelles adaptées doivent permettre à l'administrateur d'authentifier l'utilisateur distant avant toute transmission du mot de passe de secours (OE.NON_OBSERV) ;
- lorsque l'utilisateur est authentifié, l'environnement opérationnel doit assurer la confidentialité des données sensibles et des données d'authentification (OE.ENV_OPERATIONNEL) ;
- les administrateurs du produit et les administrateurs Windows doivent être des personnes de confiance (OE.SO_CONF, OE.ADM_ROOT_WINDOWS) ;
- les utilisateurs et les administrateurs doivent empêcher la divulgation des clés d'accès aux zones chiffrées (OE.CONSERV_CLES) ;
- les utilisateurs et les administrateurs doivent être sensibilisés à la sécurité informatique et être formés à l'utilisation du produit (OE.FORMATION, OE.ADM_DELEGATION) ;
- les administrateurs doivent être sensibilisés à la problématique de la qualité des clés d'accès ainsi qu'à celle de leur support (OE.CRYPTO_EXT) ;
- les administrateurs doivent vérifier la validité des certificats X509 et leur adéquation avec l'usage qui en est fait par le produit ; cette exigence s'applique en particulier aux certificats racines dits « authenticode » à partir desquels la vérification de l'intégrité du produit peut être effectuée (OE.CERTIFICATS) ;
- les opérations de ZoneCentral réalisées au travers de scripts doivent respecter les consignes intégrées à l'aide en ligne de l'interface de programmation (OE.API).

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[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. 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[2], 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 :

[1]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.

[2] 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.

Annexe 1. 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	**3**	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**	**1**	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

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - « ZoneCentral version 5.0 - Cible de Sécurité Critères Communs niveau EAL3+ », référence PX105233, version 1, révision 9.
[RTE]	Rapport technique d'évaluation : - « Rapport Technique d'Evaluation – ZEBRA5 », référence OPPIDA/CESTI/ZEBRA5/RTE, version 2.0.
[ANA-CRY]	« Cotation des mécanismes cryptographiques – Projet ZEBRA5 », n° 723/ANSSI/ACE du 21 mars 2011.
[EXP-CRY]	« Rapport d'expertise de l'implémentation de la Cryptographie – ZEBRA5», référence OPPIDA/CESTI/ZEBRA5/CRYPTO, version 2.0.
[CONF]	« Liste de configuration Zone Central version 5.0 Build 960 », référence PX108254, version 1, révision 4.
[GUIDES]	Guide d'installation : - « ZoneCentral version 5.0 - Guide d'installation », référence. PX104211, révision 2; Guides d'administration : - « ZoneCentral version 5.0 - Guide Administrateur », référence. PX104209, révision 5 ; - « ZoneCentral version 5.0 - Guide d'utilisation de ZoneBoard », référence. PX109283, révision 1 ; - « ZoneCentral, ZoneExpress !, ZedMail, Zed ! version 5.0 - Manuel des politiques », référence. PX104202, révision 4 ; Guide d'utilisation : - « ZoneCentral version 5.0 - Guide d'utilisation des zones chiffrées », référence. PX104210, révision 5.

Annexe 3. 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.
[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 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010. Annexe B1 du Référentiel général de sécurité, voir www.ssi.gouv.fr.
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008. Annexe B2 du Référentiel général de sécurité, voir www.ssi.gouv.fr.