PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2008/46

ZoneCentral v3.1, build 533

Paris, le 18 décembre 2008,

Le Directeur central 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 la direction centrale de la sécurité des systèmes d'information (DCSSI), 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 nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

Référence du rapport de certification **DCSSI-2008/46**
Nom du produit **ZoneCentral**
Référence/version du produit **Version 3.1, build 533**
Conformité à un profil de protection **néant**
Critères d'évaluation et version **Critères Communs version 2.3** **conforme à la norme ISO 15408:2005**
Niveau d'évaluation **EAL 2 augmenté** **ADV_HLD.2, ADV_IMP.1*, ADV_LLD.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1*, AVA_MSU.1, AVA_VLA.2** ***appliqués aux exigences FCS**
Développeur(s) **Prim'X Technologies** **10 Place Charles Béraudier, 69428 Lyon Cedex 03, France**
Commanditaire **Prim'X Technologies** **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, 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 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 3.1, build 533» 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 des fichiers s'effectue « *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 au déchiffrement).

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

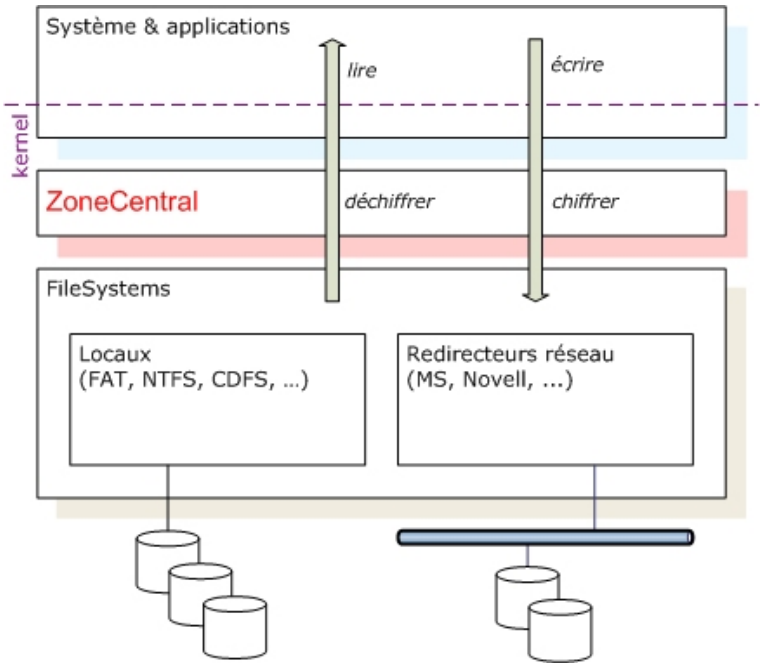
Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].
La version certifiée du produit est identifiable par la fenêtre « A propos » qui présente la version du produit ainsi que son numéro de build (ici, version 3.1, build 533).
L'intégrité du produit peut être vérifiée par comparaison des empreintes Authenticode générées par l'utilisateur ou l'administrateur avec celles disponibles sur le site web du développeur.

1.2.2. Services de sécurité

La TOE offre les services suivants :
- l'administration du produit en mode commande et en mode graphique ;
- la définition des zones chiffrées ;
- la gestion des droits d'accès aux zones chiffrées ;
- la coordination des traitements entre le monde "utilisateur" et le monde "kernel" ;
- le filtrage sur les accès aux fichiers ;
- les opérations cryptographiques pour la gestion des clés de zones et les opérations de calcul associées ;
- l'extension du Winlogon de Windows (écran de login pour ouverture de session) ;
- l'extension de l'Explorateur Windows qui permet la personnalisation des icônes des dossiers chiffrés ;
- 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).

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.

Pour un usage monoposte de ce produit, le guide [GUIDE_USR] décrit l'ensemble des fonctionnalités du produit pouvant être mises en œuvre par un utilisateur qui est également administrateur de son poste de travail.
Pour un usage en entreprise, où généralement les rôles d'administration et d'utilisation sont distingués, le guide [GUIDE_ADM] décrit les fonctionnalités d'administration du produit qui correspondent à une gestion centralisée des politiques de sécurité appliquées aux postes de travail sur lequel le produit est installé. Le guide [GUIDE_USR] décrit toujours les fonctionnalités offertes à l'utilisateur. Le degré de liberté laissé aux utilisateurs dépend de la configuration sélectionnée par l'administrateur.

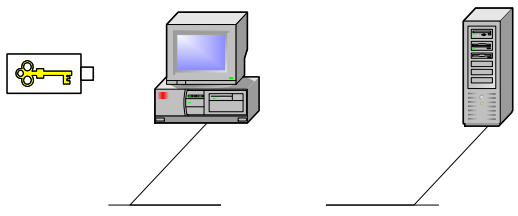
Le produit a été développé sur le site suivant :

Prim'X Technologies

10 Place Charles Béraudier
69428 Lyon Cedex 03
France

1.2.5. Configuration évaluée

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 2000, Windows XP, Windows Vista et Windows 2003 ;
- 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 2.3** [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 la DCSSI le 15 décembre 2008, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet du rapport d'analyse [ANA-CRY].
Les mécanismes analysés atteignent le niveau standard défini dans le référentiel cryptographique de la DCSSI (Cf. [REF-CRY]), sous réserve que les recommandations décrites dans les guides [GUIDES] soient appliquées.

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 3.1, build 533» soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 2 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- les utilisateurs et/ou les administrateurs doivent vérifier l'intégrité du produit (OE.SOFT_SIGNE) ;
- l'installation du produit doit être effectuée conformément à son manuel d'installation (OE.INSTALLATION) ;
- 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 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 utilisateurs et les administrateurs du produit 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 utilisateurs et 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 utilisateurs et/ou 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 administrateurs du domaine Windows doivent interdire aux administrateurs des sous-niveaux la modification des politiques de sécurité du produit (OE.ADM_ROOT_WINDOWS).

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 1999 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 E6 et CC EAL7. 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'Espagne, la Finlande, la France, la Grèce, 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, la République de Corée, les Pays-Bas, 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 2+	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2		
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**2**	Configuration items
	ACM_SCP			**1**	**2**	**3**	3	3		
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**1**	Delivery procedures
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**1**	Informal functional specification
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**1***	Subset of the implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1***	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3		
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic Flow remediation
	ALC_LCD				**1**	**2**	2	**3**		
	ALC_TAT				**1**	**2**	**3**	3	**1***	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**1**	Evidence coverage
	ATE_DPT			**1**	1	**2**	2	**3**		
	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_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**1**	Examination of guidance
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

** appliqués aux exigences FCS*

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - « ZoneCentral version 3.1 - Cible de Sécurité CC niveau EAL2+ », référence CSZC31, version 2, révision 6
[RTE]	Rapport technique d'évaluation : - « Rapport technique d'évaluation – Projet ZEBRA2 », réf.°OPPIDA/CESTI/ZEBRA2/RTE, version 1.0
[ANA-CRY]	« Cotation de mécanismes cryptographiques – Projet ZEBRA2 », N°1436/SGDN/DCSSI/SDS/Crypto, 3 juillet 2008
[CONF]	« Liste de configuration de la version 3.1 Build 533 », réf. PX81112, version 1, revision 3
[GUIDES]	[GUIDE_ADM] Guide d'installation et d'administration du produit : - « ZoneCentral - Manuel Technique de l'Administrateur- Version 3.1 », réf. PX81098, révision 5 [GUIDE_USR] Guide d'utilisation du produit : - « ZoneCentral, Version 3.1 - Guide d'utilisation et de mise en œuvre », réf. PX81092, révision 3

Annexe 3. 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.	
[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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[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.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, version courante, voir www.ssi.gouv.fr.