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-2010/51

Zed!, version 4.0, build 820

Paris, le 30 juillet 2010

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

Vice-amiral Michel Benedittini
[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-2010/51

Nom du produit

Zed !

Référence/version du produit

Version 4.0, build 820

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 2

Niveau d'évaluation

EAL 3 augmenté

ALC_FLR.3, AVA_VAN.3

Développeur(s)

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 « Zed ! » développé par Prim'X Technologies SA.

Ce produit permet la création et la consultation de conteneurs de répertoires et de fichiers chiffrés et compressés. Ces conteneurs sont destinés soit à être archivés, soit à être échangés avec des correspondants (par exemple, en pièces jointes de messages électroniques ou sur des clés USB). Les conteneurs ne modifient ni l'arborescence des fichiers ou des dossiers copiés, ni leurs caractéristiques (nom, dates, tailles).
Le chiffrement/déchiffrement des données est réalisé de façon la plus transparente possible pour les utilisateurs : il s'effectue lorsque les fichiers sont lus/copiés dans le conteneur et « à la volée » (sans manipulation particulière de l'utilisateur).

Les éditions suivantes de Zed ! ont été prises en compte dans le cadre de cette évaluation :
- l'édition standard, qui contient le produit complet ;
- l'édition limitée, gratuite, libre de distribution et d'usage, qui permet aux correspondants ne disposant pas de l'édition standard de lire et d'extraire les éléments d'un conteneur. L'édition limitée existe sous deux formes :
    - une forme installable (i.e. avec programme d'installation), intégrée à l'explorateur Windows ;
    - une forme exécutable, facile à transporter, qui évite d'avoir à effectuer une installation.

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 l'édition standard : « Setup Zed! 4.0 x86(b820).exe »,
- pour l'édition limitée : « Setup Zed! Limited Edition 4.0 x86(b820).exe ».

Une fois le produit installé, la version « 4.0.820.0 » du produit évalué est présentée à l'utilisateur final :
- en consultant les propriétés des binaires installés ;
- en lançant l'outil « zedcmd.exe » avec l'option « about » ;
- à l'aide du panneau d'options, accessible à partir du menu contextuel (clic-droit) dans le « fond » du conteneur ou sur le fichier conteneur lui-même.

Tous les fichiers binaires sont signés par la technologie Authenticode qui permet de s'assurer que les binaires sont intègres et qu'ils sont identiques aux binaires originaux émis par Prim'X.

1.2.2. Services de sécurité

Les principaux services de sécurité de l'édition standard du produit sont :

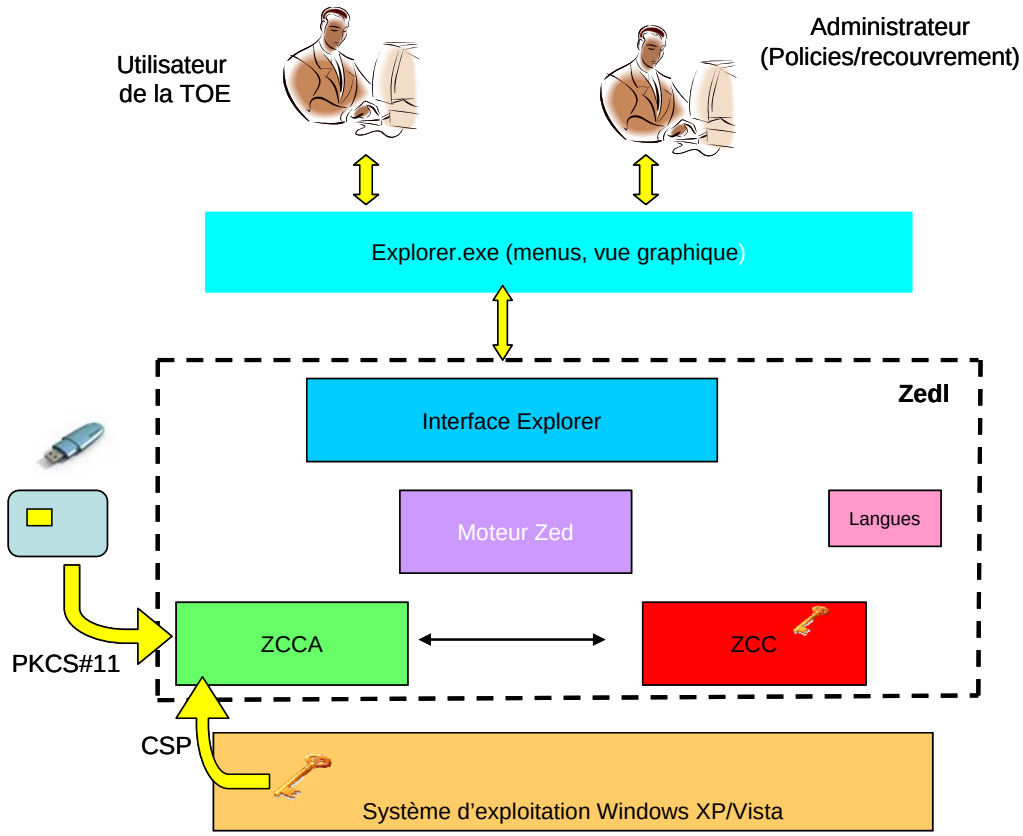
- la création de conteneurs, qui comporte les étapes suivantes :
  - l'initialisation du conteneur correspondant :
    - à l'association au conteneur des clés d'accès de son créateur. Une clé d'accès peut correspondre soit à un mot de passe, soit à une clé publiques RSA ;
    - à la génération, selon le standard PKCS#5 v2.0, de clé symétrique AES ou 3DES dérivée du mot de passe, si la clé d'accès au container correspond à un mot de passe ;
    - à la génération de la clé symétrique AES ou 3DES du containeur, stockée chiffrée soit par les clés d'accès, soit par la clé dérivée du mot de passe. Cette clé est spécifique à un conteneur particulier ;
  - l'ajout d'accès utilisateurs :
    - si l'accès du conteneur est protégé par des clés RSA, les clés publiques RSA des utilisateurs autorisés à consulter les éléments du conteneur doivent ici être fournies ; le produit chiffre alors la clé du containeur par ces clés RSA ;
    - si l'accès du conteneur est protégé par un mot de passe, il suffit ici de convenir d'un identifiant et mot de passe partagé ;
  - l'ajout, la suppression et l'extraction des fichiers ou répertoires du conteneur ;
- la lecture, l'ajout, la suppression, l'extraction des fichiers ou répertoire de conteneurs après présentation d'une clé d'accès préalablement autorisée ;
- le renommage ou la suppression d'un conteneur ;
- la modification des accès utilisateurs prévus par le créateur original du conteneur ;
- des fonctions d'administration permettant de restreindre certaines capacités du produit à partir de la configuration Windows (politiques configurées dans des stratégies de groupe), qui permettent notamment :
  - d'imposer le type des clés d'accès autorisé ;
  - de déterminer le comportement, d'activer et désactiver, de modifier le comportement des fonctions de chiffrement des conteneurs. Par exemple, choisir les longueurs de clé et l'algorithme de chiffrement des conteneurs lors de leur création (AES, 3DES, avec longueurs de clés de 128, 192 ou 256 bits) ;
  - d'activer la génération de données d'audit ;
  - d'ajouter des clés d'accès obligatoire (qui seront utilisées en tant que clés de recouvrement).

Les services de sécurité de l'édition limitée du produit sont :

- la lecture, l'ajout, la suppression, l'extraction des fichiers ou répertoires de conteneurs après présentation de sa clé d'accès et si l'accès a été préalablement autorisé ;
- le renommage ou la suppression d'un conteneur.

1.2.3. Architecture

La figure suivante présente l'architecture du produit (la TOE correspond au produit complet).



Le produit est constitué des éléments suivants :

- un module « Interface Explorer » qui implémente les interfaces Shell de Windows permettant de gérer les menus et la vue graphique accessibles à partir de l'explorateur Windows ;
- un module « ZCC » qui correspond au centre cryptographique de Zed! : il gère les clés et exécute les opérations de calcul associées. Les clés générées par le produit ne sortent jamais de son enceinte ;
- un module « ZCCA » qui référence les clés utilisateur saisies via l'entrée d'un mot de passe, l'interface PKCS#11 ou le CSP[1] ;
- un module « Moteur Zed » qui coordonne les différents traitements ;
- un module « Langues » qui représente les dlls[2] associées aux différentes langues supportées par le produit.

[1] Cryptographic Service Provider
[2] Bibliothèques de liens dynamiques

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 SA

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 XP et Windows Vista ;
- 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 « Zed! Edition Standard » et « Zed! Edition Limitée » en versions installables et exécutables (voir chapitre 1.1). Le produit intégré dans ZoneCentral ne fait pas partie du périmètre de l'évaluation.

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 28 juillet 2010, 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 du référentiel cryptographique de l'ANSSI.

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

L'édition standard de Zed! permet la génération de clés de chiffrement de containeurs.
Le générateur d'aléa utilisé et le retraitement d'aléa mis en œuvre le cadre de cette opération 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 « Zed !, version 4.0, build 820 » 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 (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 (clés utilisateur et clés de recouvrement) aux conteneurs chiffrées (OE.CONSERV_CLES) ;
- les utilisateurs et les administrateurs doivent être formés à l'utilisation du produit et être sensibilisés à la sécurité informatique (OE.FORMATION) ;
- les administrateurs doivent être sensibilisés à la problématique de la qualité des clés d'accès, ainsi qu'à celle de leurs supports (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 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 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'Espagne, la Finlande, la France, 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.

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**	**2**	**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

Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - « Zed ! Encrypted containers – version 4.0- Cible de Sécurité Critères Communs niveau EAL3+ », référence PX84140, version 1, révision 10.
[RTE]	Rapport technique d'évaluation : - « Rapport Technique d'Evaluation – Projet ZEBRA3 », référence OPPIDA/CESTI/ZEBRA3/RTE, version 1.2.
[ANA-CRY]	« Cotation des mécanismes cryptographiques – Projet ZEBRA3 », n° 1940/ANSSI/ACE du 20 juillet 2010.
[EXP-CRY]	« Expertise de l'implémentation de la Cryptographie – ZEBRA3 », référence PX97191, version 1, révision 3.
[CONF]	« Liste de configuration de la version 4.0 Build 820 », référence OPPIDA/CESTI/ZEBRA3/EXPERTISE_IMP_CRYPTO, version 2.0.
[GUIDES]	Guide d'installation, d'administration et d'utilisation de l'édition standard : - « Zed ! Encrypted containers – version 4.0- Guide d'utilisation », référence PX92171, révision 7. Guide d'installation et d'utilisation de l'édition limitée : - « Zed ! Encrypted containers – Limited Edition, version 4.0- Guide d'utilisation », référence PX92173, révision 5.

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, September 2006, version 3.1, révision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, révision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, révision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[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, 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, voir www.ssi.gouv.fr