Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-2016/25

Zed!, version 6.1, build 2120

Paris, le 23 mai 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2016/25

Nom du produit

Zed!, version 6.1, build 2120

Référence/version du produit

Version 6.1, Build 2120

Conformité à un profil de protection

Aucune

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 3 augmenté

ALC_FLR.3, AVA_VAN.3

Développeur(s)

Prim'X Technologies S.A

10, place de Béraudier, 69428 Lyon Cedex 03, France

Commanditaire

Prim'X Technologies S.A

10, place de Béraudier, 69428 Lyon Cedex 03, France

Centre d'évaluation

Oppida

4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France

Accords de reconnaissance applicables

CCRA

Le produit est reconnu au niveau EAL2.

SOG-IS

Le produit est reconnu au niveau EAL3.

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 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Identification du produit 6
1.2.3. Services de sécurité 7
1.2.4. Architecture 7
1.2.5. Cycle de vie 9
1.2.6. Configuration évaluée 10

2. L'EVALUATION 11

2.1. REFERENTIELS D'EVALUATION 11
2.2. TRAVAUX D'EVALUATION 11
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L'ANSSI 11
2.4. ANALYSE DU GENERATEUR D'ALEAS 11

3. LA CERTIFICATION 12

3.1. CONCLUSION 12
3.2. RESTRICTIONS D'USAGE 12
3.3. RECONNAISSANCE DU CERTIFICAT 13
3.3.1. Reconnaissance européenne (SOG-IS) 13
3.3.2. Reconnaissance internationale critères communs (CCRA) 13

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT CCV3.1R4 14

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 15

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 16

1. Le produit

1.1. Présentation du produit

Le produit Zed!, version 6.1, build 2120 développé par la société *PRIM'X TECHNOLOGIES*, est un produit logiciel de sécurité pour des postes de travail opérant sur des plateformes sous *MICROSOFT Windows Seven (64 bit) et Windows 10 (64 bit)*. Ce produit permet aux utilisateurs, de créer, consulter et modifier des conteneurs contenant des répertoires ou des 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 dans des clés USB). Les conteneurs ne modifient ni l'arborescence des fichiers ou des dossiers copiés, ni leurs caractéristiques (noms, 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).

Dans le cadre de cette évaluation, deux éditions de Zed! ont été prises en compte :

- l'édition standard (Zed! Edition Standard) qui est constituée de l'intégralité du produit ;
- l'édition limitée (Zed! Edition Limitée) qui permet seulement aux récipiendaires de lire les contenus des conteneurs et d'en extraire les fichiers. Cette version ne permet pas de créer de nouveaux conteneurs ou d'en modifier les accès prévus par son créateur initial. L'édition limitée se présente sous forme d'un simple exécutable (zedle.exe), facile à transporter et qui évite d'avoir à effectuer une installation.

1.2. Description du produit

1.2.1. Introduction

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

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

Suivant l'édition, la version du produit apparait de la manière suivante :
Edition standard :

- nom du package : setup Zed! 6.1 x64(b2120).exe ;
- valeur de la signature : 04 14 7A 12 36 9D 30 1F B2 A6 FF 83 31 15 C7 67 97 13 00 D2 23 B7.

Edition Limitée :

- nom du package : zedle.exe ;
- valeur de la signature : 04 14 1E 51 F9 00 B2 B4 80 5E 89 B0 EA 4D 92 CA F6 83 84 9A 0F D0.

Comme indiqué dans le guide d'installation [GUIDES], l'authenticité du package installé peut être vérifiée en comparant la valeur de signature affichée avec celle indiquée sur le site de Prim'X : http://www.primx.fr/support/ctrl_authenticite.aspx.

1.2.3. Services de sécurité

Les principaux services de sécurité du produit sont :

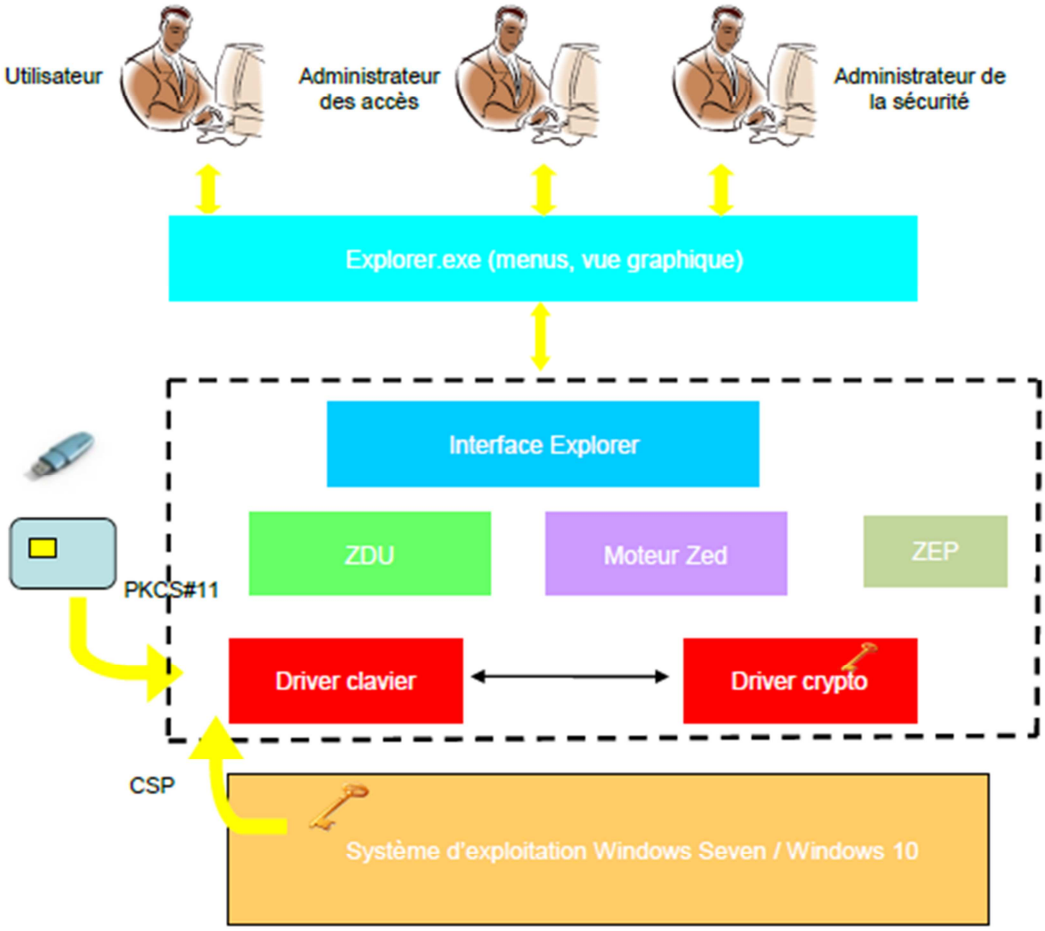
- la protection des conteneurs chiffrés notamment lors de leur ouverture que ce soit pour la lecture, le remplissage ou la gestion des accès ;
- la gestion de la saisie du mot de passe et sa dérivation en une clé d'accès ;
- la gestion de la saisie du code confidentiel du fichier de clés ;
- la gestion de la saisie du code confidentiel du *token* logique ;
- la conservation dans le conteneur des fichiers et dossiers sous forme chiffrée avec la possibilité de masquer leurs noms ;
- le contrôle de l'intégrité lors de l'ouverture d'un fichier ;
- la protection des différentes clés ;
- la protection de chaque vecteur d'initialisation spécifique à chacun des fichiers ;
- la vérification avant d'être appliquées des politiques définies par l'administrateur de la sécurité (version standard uniquement) ;
- la vérification de l'intégrité du fichier de contrôle. Ce fichier contient le libellé du conteneur, un identifiant unique, des informations de gestion et les clés de chiffrement du conteneur ;
- la vérification d'intégrité du fichier dit « catalogue ». Ce dernier contient les fichiers applicatifs du conteneur avec leurs positions dans l'arborescence, les tailles originales, les horodatages, etc.

1.2.4. Architecture

Le produit Zed! se décline en deux packages :

- l'édition standard contient le produit complet ;
- l'édition limitée est une version « bridée » de l'édition standard.

Zed! Edition Standard.



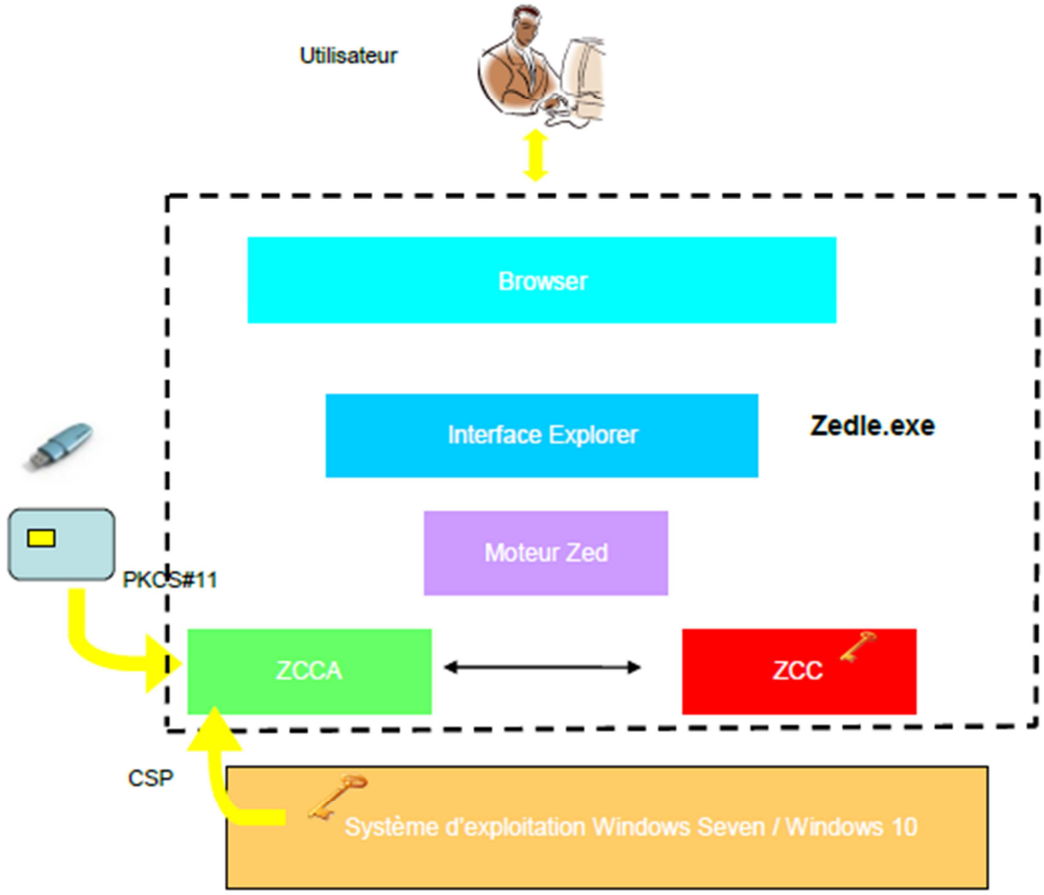
Cette figure présente l'architecture du produit dans sa version « standard » (TOE délimitée par les pointillés) ainsi que ses principaux composants :

- le module « *Interface Explorer* » implémente les interfaces *Shell* de Windows permettant de gérer les menus et la vue graphique accessibles à partir de l'explorateur Windows ;
- le module « ZDU » est un «daemon[1]» utilisateur instancié pour chaque session utilisateur Windows qui pointe les clés des utilisateurs générées par le produit via l'entrée d'un mot de passe, l'interface PKCS#11, le *Cryptographic Service Provider* (CSP) ou le *Cryptographic Next Generation* (CNG) ;
- le service « ZEP » contrôle la signature des politiques ;
- le module « Moteur Zed » coordonne les différents traitements ;
- le « *driver crypto* » implémenté en mode *Kernel*, est le centre cryptographique de Zed! « Edition Standard » : il gère les clés de conteneurs et exécute les différentes opérations de calcul. Les clés générées ne sortent jamais du produit ;
- le « *driver clavier* » est un filtre de saisie clavier : il intercepte à très bas niveau les mots de passe et codes confidentiels saisis de façon à ce que leurs valeurs restent confinées le plus bas possible dans le système.

[1] Un *daemon* désigne un processus qui s'exécute en arrière-plan sans intervention directe de l'utilisateur.

Zed! Edition Limitée.

Zed! Edition Limitée est une déclinaison du produit Zed! Edition Standard.



La figure ci-dessus présente l'architecture du produit dans sa version « limitée » (TOE délimitée par les pointillés) ainsi que ses principaux composants :

- le module « *Browser* » émule l'*Explorer Windows* ;
- le module « *Interface Explorer* » permet de gérer les menus et la vue graphique ;
- le module « Moteur Zed » coordonne les différents traitements ;
- le module « ZCC » est le centre cryptographique de Zed! « Edition Limitée » : il gère les clés et exécute les opérations de calcul. Ici, « ZCC » est un applicatif alors que le « *driver crypto* » de Zed! « Edition Standard » est implanté en mode *Kernel* ;
- le module « ZCCA » pointe les clés des utilisateurs générées par le produit via l'entrée d'un mot de passe, l'interface PKCS#11 ou le CSP.

1.2.5. 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 TECHNOLOGIES* 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 S.A
10, place Charles BERAUDIER
69428 LYON Cedex 03
France

1.2.6. Configuration évaluée

Les produits « Edition Standard » et « Edition Limitée » ont été évalués sur deux systèmes d'exploitation différents à savoir *WINDOWS SEVEN* (64 bits) et Windows 10 (64 bits).

La cible d'évaluation correspond à « Zed! Edition Standard » et « Zed! Edition Limitée » en version exécutable.
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 révision 4** [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 4 mai 2016, 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. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-EXP-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations suivantes doivent être suivies :

- la taille des clés RSA doit être au moins de 2048 bits ;
- seule la fonction de hachage SHA2-256 doit être utilisée dans le cadre du mécanisme RSA-OAEP ;
- la fonction de hachage SHA2-256 doit être utilisée dans le mécanisme HMAC ;
- la fonction de hachage utilisée par défaut pour les mécanismes de dérivation de clé et IV doit être SHA-256.

Les 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.3 visé.

Dans le cadre du processus de qualification standard une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [ANA-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.3 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires du produit a été évalué. Comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie de son alimentation en bruit subit un retraitement de nature cryptographique.
Les résultats ont été pris en compte dans l'analyse de vulnérabilité réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.3 visé.

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 6.1, build 2120 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3, AVA_VAN.3.

3.2. Restrictions d'usage

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

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

- utiliser la version 2.2 de RSA PKCS#1 (politique P383) ;
- fixer le seuil d'acceptation des mots de passe à 100% (politique P730) et leurs longueurs à 12 au minimum (politique P732) ;
- masquer les noms de fichiers et de dossiers des conteneurs chiffrés en fixant la valeur de type « Choix » à « Toujours masquer » (politique P233) ;
- utiliser l'algorithme de hachage SHA-256 tel que mis par défaut (politique P292) ;
- forcer l'utilisation du mode de chiffrement ES CBC CTS (politique P381) ;
- utiliser le format v2 des conteneurs (politique P399) ;
- ne pas activer la politique P382 qui fait réaliser les calculs AES par le processeur plutôt que par le logiciel fourni par *PRIM'X* et qui est évalué.

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 EAL2 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, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit CCv3.1R4

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 : - Zed! 6.1 build 2120, référence PX14A459, version 1 révision 9 de mars 2016, *PRIM'X*. Cette cible de sécurité est publique, elle est publiée dans son intégralité.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation, référence OPPIDA/CESTI/ZED6/RTE du 29/02/2016, version 3.0 du 4 mai 2016, *OPPIDA.*
[ANA-EXP-CRY]	Analyse des mécanismes cryptographiques : – Référence : OPPIDA/CESTI/ZED/CRYPTO/1.0, 16 décembre 2015, *OPPIDA.*
[CONF]	Liste de configuration du produit : - Zed! version 6.1 Build 2120 – Liste de configuration, référence PX156527, version v1r2 du 17 novembre 2015, *PRIM'X.*
[GUIDES]	Guide d'installation du produit : - Zed! 6.1 Guide d'installation FR, référence PX156516, révision 2, *PRIM'X*. Guide d'administration du produit : - Manuel des politiques 6.1 FR, référence PX156524, révision 1, *PRIM'X ;* - Mise en œuvre de la signature des politiques FR, référence PX13C133, *PRIM'X*. Guide d'utilisation du produit : - Zed! 6.1 Guide d'utilisation des conteneurs chiffrés, référence PX156518, révision 5, *PRIM'X* ; - Zed! Limited Edition 6.1 Guide, référence PX156523, révision 3, *PRIM'X*.

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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, Septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.
	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.