PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CC-2022/40

Zed!
(Version Q.2021.1)

Paris, le 23 août 2022

Le Directeur général adjoint de l'Agence nationale de la sécurité des systèmes d'information

Emmanuel NAEGELEN

[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-2022/40**
Nom du produit **Zed!**
Référence/version du produit **Version Q.2021.1**
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL 3 augmenté** ALC_FLR.3, AVA_VAN.3
Développeur **PRIM'X TECHNOLOGIES** Immeuble SKY56, 18 rue du Général Mouton-Duvernet 69003 Lyon, France
Commanditaire **PRIM'X TECHNOLOGIES** Immeuble SKY56, 18 rue du Général Mouton-Duvernet 69003 Lyon, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2 augmenté de FLR.3. **SOG-IS** Ce certificat est reconnu au niveau EAL3 augmenté de FLR.3.

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Zed!, Version Q.2021.1 » développé par PRIM'X TECHNOLOGIES.

Zed! est un produit de sécurité pour postes de travail opérant sous Windows, Linux et Mac. Il se présente comme un produit autonome. Son rôle est de permettre aux utilisateurs de fabriquer des conteneurs de fichiers compressés et chiffrés. Le produit intègre par ailleurs un mécanisme de contrôle de l'intégrité globale du conteneur. Ces conteneurs sont destinés à servir d'archive, ou, plus généralement, de pièce-jointe chiffrée dans des courriers électroniques échangés dans une société.

Zed! se décline en différents packages :

- Zed! Entreprise édition complète qui contient le produit complet ;
- L'édition limitée (appelé « Zed! Entreprise édition limitée ») qui se présente sous la forme d'un simple exécutable (zedle.exe) et permet aux correspondants de lire le contenu des conteneurs et d'en extraire les fichiers. Le correspondant a également le droit de modifier le contenu du conteneur (enlever, ajouter des fichiers) pour pouvoir le renvoyer à l'émetteur d'origine. L'édition limitée ne lui permet pas, cependant, de créer de nouveaux conteneurs ou de modifier les accès prévus par le créateur original du conteneur ;
- Zed! Entreprise édition complète est également incorporé dans ZoneCentral.

Dans le cadre de cette évaluation, seules les éditions Zed! Entreprise édition complète et Zed! intégré dans ZoneCentral, toutes les deux installées sous Windows 10, ont été prises en compte.

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 *Services de sécurité*

Les principaux services de sécurité fournis par le 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 de fichiers et dossiers sous forme chiffrée avec la possibilité de masquer leurs noms ;
- Le contrôle de l'intégrité globale du conteneur chiffré lors de l'ouverture de celui-ci ;
- La protection des différentes clés ;
- La protection de chaque vecteur d'initialisation spécifique à chacun des fichiers ;
- La vérification, avant leur application, des politiques définies par l'administrateur de la sécurité.

1.2.3 *Architecture*

Le produit est composé de deux parties :
- Zed! Entreprise édition complète version Q.2021.1 qui permet aux utilisateurs de fabriquer des conteneurs de fichiers compressés et chiffrés ;
- ZoneCentral version Q.2021.1 qui permet le chiffrement à la volée des fichiers des postes de travail sur lequel est installé le logiciel Zed!

L'architecture complète du produit est décrite dans la cible de sécurité [ST] section 2.3.

1.2.4 *Identification du produit*

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

La version certifiée du produit est identifiable par les éléments suivants :
- Zed! Entreprise édition complète version Q.2021.1 :
  - nom du package : Setup Zed! Q.2021.1 x64.exe ;
  - valeur de la signature : 04 20 01 FA 37 66 4E F6 36 6E 8B C7 15 83 43 C4 D8 FD F2 51 32 E3 3D D2 90 88 20 EE 4A 60 3A F6 9F 8E.
- Zed! Entreprise édition complète version Q.2021.1, intégré dans ZoneCentral version Q.2021.1 :
  - nom du package : Setup ZoneCentral Q.2021.1 x64.exe ;
  - valeur de la signature : 04 20 43 D7 FD 11 CE 47 7F 82 C4 14 AD D8 59 E1 BA B0 3B 2E 71 59 15 8A 07 9F 03 2A 61 AE 15 7A 1E EF.

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

Immeuble SKY56

18 rue du Général Mouton-Duvernet

69003 Lyon France

1.2.6 *Configuration évaluée*

La cible d'évaluation correspond à « Zed! Entreprise édition complète » version Q.2021.1 et « Zed! Entreprise édition complète » version Q.2021.1 intégré dans « ZoneCentral » version Q.2021.1 en version exécutable avec les politiques de sécurité activées en section 2.3.2.1 de la cible de sécurité [ST].

Le produit a été évalué sur le système d'exploitation Windows 10 version 1809 LTSC et version 20H2 (64 bits) conformément aux plateformes décrites dans la section 2.3.2.3 de la cible de sécurité [ST].

2 L'évaluation

2.1 Référentiels d'évaluation

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

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 30 juin 2022, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le produit « ZoneCentral » déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du produit « ZoneCentral », voir [CER_ZC].

2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises 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 d'attaquant 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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

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].

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 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

Le présent certificat est reconnu par le SOG-IS au niveau EAL3 augmenté de ALC_FLR.3.

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

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 :

Le présent certificat est reconnu par le CCRA au niveau EAL2 augmenté de ALC_FLR.3.

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - PRIMX-Zed Q.2021 Cible de Sécurité, référence PX2051296r5, version 1.5, avril 2021.
[RTE]	Rapport technique d'évaluation : - Rapport technique d'évaluation, référence OPPIDA/CESTI/CC/ZED/RTE, version 3.0, 30 juin 2022. Pour le besoin des évaluations en composition un rapport technique pour la composition a été validé : - Rapport de composition, référence OPPIDA/CESTI/ZED2021/COMPO, version 2.0, 30 juin 2022.
[ANA_CRY]	Rapport d'analyse des mécanismes cryptographiques : - Rapport d'analyse des mécanismes cryptographiques ZED2021, référence OPPIDA/CESTI/ZED2021/CRYPTO, version 2.0, 20 avril 2022.
[CONF]	Liste de configuration du produit : - PRIMX-Zed Q.2021 Liste de configuration, référence PX2131463, version 1.3, 30 juin 2022.
[GUIDES]	Guide d'installation du produit : - Zed! Q.2021.1 Guide d'installation FR, référence PX20A1391, version 1.2. Guide d'utilisation des conteneurs chiffrés : - Zed! Q2021.1 Guide d'utilisation des conteneurs chiffrés FR, référence PX20A1397, version 1.2. Manuel des politiques : - Manuel des politiques Q.2021 FR, référence PX20A1376, version 1.2. Mise en œuvre de la signature des politiques : - Mise en œuvre de la signature des politiques FR, référence PX13C133, version 1.4.
[CER_ZC]	Produit ZoneCentral version Q2021.1 Certifié par l'ANSSI sous la référence ANSSI-CC-2022/39.

ANNEXE B. 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 4.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *Part 3 : Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[COMP]*	*Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices*, version 1.5.1, mai 2018.
[CCRA]	*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.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.