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-2022/39

ZoneCentral (Version Q2021.1)

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-2022/39**
Nom du produit **ZoneCentral**
Référence/version du produit **Version Q2021.1**
Conformité à un profil de protection **Sans objet**
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 « ZoneCentral, Version Q2021.1 » développé par PRIM'X TECHNOLOGIES.

Le produit ZoneCentral, installé sur un équipement de type PC, a en charge de protéger en confidentialité les documents manipulés par les utilisateurs. Il offre un stockage chiffré des fichiers, sans modifier leurs caractéristiques (emplacement, nom, dates, tailles). Le chiffrement est effectué *in-place* (là où résident les fichiers) et *à la volée* (sans manipulation particulière de l'utilisateur). Afin de simplifier la gestion des fichiers chiffrés, ZoneCentral est basé sur le principe de zones : une zone chiffrée est un volume ou un dossier, avec tout ce qu'il contient.

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.

Cette cible de sécurité ne revendique pas de conformité à un profil de protection.

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- la protection en confidentialité par chiffrement des fichiers ;
- la gestion du contrôle d'accès aux zones chiffrées par l'utilisateur ;
- l'authentification des utilisateurs via une clé dérivée d'un mot de passe ou via une clé RSA stockée sur un porte-clé électronique (token USB, fichier de clé ou conteneur CSP/CNG) ;
- l'administration des zones permettant de gérer les clés et les accès (en particulier l'accès de recouvrement) ;
- la journalisation des évènements.

1.2.3 *Architecture*

Le produit ZoneCentral est constitué des éléments suivants :

- Les *drivers*
  - «ZCK», qui se place en filtre au-dessus des *drivers* de FileSystems et des volumes qu'il présente, et qui intercepte les requêtes d'accès au fichier ;
  - «ZCCK» qui est le centre cryptographique de ZoneCentral ;
  - «ZCKBD», qui est le filtre de saisie clavier ;
- Les services
  - «ZCS», qui coordonne les traitements entre le monde «kernel» (*drivers*) et le monde «*user*» (programmes et applications) ;
  - « ZCP » qui contrôle la signature des politiques ;
- Le *daemon* utilisateur «ZCU», instancié pour chaque session utilisateur Windows, qui gère les interfaces graphiques proposées aux utilisateurs et leurs clés d'accès ;
- Les composants additionnels suivants :
  - Une extension de l'Explorateur Windows, «ZCUSH», qui personnalise les icônes des dossiers chiffrés et qui affiche les propriétés des zones ;
  - L'extension Winlogon « ZCCP » qui permet d'entrer sa clé d'accès avant le *login* Windows ;

- Une interface graphique simple et légère pour les utilisateurs, «ZCGU» ('Moniteur') leur permet de voir la liste des zones chiffrées ouvertes, les clés d'accès présentées, et la version du logiciel. Il permet également de fermer manuellement des zones et des clés ;
- Une interface graphique pour les administrateurs, « ZoneBoard » leur permet de visualiser et de gérer l'ensemble des accès cryptographique sur les zones chiffrées partagées ;
- Deux outils de commande, «ZCACMD» et «ZCUCMD», le premier servant principalement à l'administrateur de la TOE pour la définition des zones chiffrées, le second étant un équivalent en mode commande de l'interface graphique «ZCGU».
- Un assistant de chiffrement « ZCAPPLY » qui est invoqué par ZoneCentral dès lors qu'une transformation de fichiers doit être effectuée : chiffrement, déchiffrement, transchiffrement. ZCAPPLY peut également être invoqué en mode commande par l'administrateur de la TOE ;
- Un éditeur graphique de listes d'accès et de profils de zone, « ZCEDIT » permet à l'administrateur de la TOE de préparer le déploiement en amont et d'administrer ensuite les accès aux zones. ZCEDIT permet également d'effectuer le secours utilisateur (par l'opérateur de secours).

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 via la fenêtre « propriétés » de l'exécutable d'installation *Setup ZoneCentral Q.2021.1 x64.exe* :

- Choisir l'onglet « Signatures numériques » ;
- La signature affichée doit coïncider avec la signature disponible sur le site web de Prim'X.

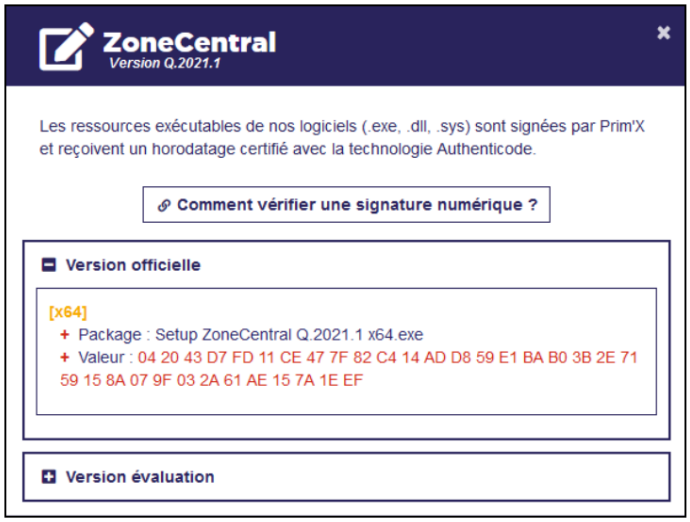

Figure 1 : signature **disponible** sur le site web du développeur

1.2.5 *Cycle de vie*

Le cycle de vie du produit est le suivant :

- le développement et la livraison du produit sont réalisés par PRIM'X TECHNOLOGIES ;
- 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

Pour l'évaluation, l'évaluateur a considéré les utilisateurs suivants :

- *L'utilisateur* qui utilise la TOE selon la configuration imposée par l'administrateur de la TOE, afin de protéger ses fichiers en confidentialité ;
- *L'administrateur de la sécurité* de la TOE, en charge de définir les zones chiffrées du « parc » et effectuer la procédure de migration initiale qui consiste à chiffrer leur contenu actuel, sur les serveurs (partages) et sur les postes de travail. Pour chaque zone chiffrée, il configure la liste des personnes pouvant y accéder en introduisant leurs clés d'accès (ou en paramétrant des listes d'accès). Par la suite, il crée de nouvelles zones si besoin est (nouveaux ordinateurs, nouveaux partages), gère les mouvements de personnel (nouvel utilisateur pour une zone, retrait d'accès pour une personne en partance), et, éventuellement, transchiffre les zones chiffrées (sur compromission ou régulièrement). Cet administrateur a par ailleurs en charge les opérations de signature des politiques et de recouvrement local. Sauf mention contraire dans la suite de ce document, toute référence à *l'administrateur* se rapporte à ce rôle ;
- *L'administrateur Windows*, en charge de définir les politiques de fonctionnement du produit : cette opération est effectuée sous le contrôle de l'administrateur de la sécurité de la TOE. Les *politiques* sont signées par l'administrateur de la sécurité de la TOE et vérifiées par ZoneCentral avant leur application. Il est à noter que ce rôle peut se décliner en plusieurs rôles hiérarchiques correspondant aux différents niveaux des domaines Windows. Dans ce cas les administrateurs des niveaux supérieurs doivent interdire aux administrateurs des sous-niveaux (domaines, contrôleurs de domaines, postes de travail) la modification des politiques de la TOE qu'ils souhaitent eux-mêmes contrôler ;
- L'*opérateur de secours* de la TOE, en charge des opérations de secours des utilisateurs distants ayant oublié leur mot de passe ou perdu / cassé / bloqué leur porte-clés physique. Contrairement à l'administrateur de la sécurité de la TOE, l'accès de l'opérateur de secours n'est pas déclaré dans les zones des autres utilisateurs.

Le périmètre d'évaluation prend en compte la fourniture de clés d'accès dérivées à partir d'un mot de passe ou utilisant un certificat X509, ces certificats pouvant être stockés dans différents magasins et annuaires : magasins Windows locaux, fichiers de certificats et fichiers listes de certificats, annuaires LDAP, etc.

Les éléments suivants ne sont pas couverts par l'évaluation :

- Les systèmes d'exploitation Windows ;
- Les éventuels porte-clés matériels utilisés ;
- L'outil de politique de sécurité utilisé GPOSign.exe ;
- La mise à jour système automatisée sans utilisateur ;
- Le pré-chiffrement d'une machine par un opérateur externe.

Le périmètre d'évaluation exclut l'utilisation des fonctionnalités suivantes :

- Le 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) ;
- L'interface de programmation (API).

1.2.6 *Configuration évaluée*

La configuration évaluée est le build Q.2021.1, configuré dans le mode *Active Directory* ou le mode *Alternatif* décrits dans le chapitre 2.3.2.1. Périmètre logique de [ST]. La plate-forme PC utilisée est sous le système d'exploitation Windows 10 versions 1809 LTSC et 20H2 (64 bits) de Microsoft.

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** ».

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.

2.5 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.

2.6 Restrictions d'usage

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

L'administrateur 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 :

- Limiter l'autorisation d'utilisation de l'interface WMI aux seuls administrateurs ayant le besoin d'en connaître ;

- Eviter d'utiliser des liens réels (*hardlinks*) ou des liens symboliques dans les zones – en cas d'utilisation, l'administrateur doit s'assurer que les différentes représentations (lien, fichier) sont dans le même état de chiffrement (tous chiffrés avec la même clé ou en clair).

2.7 Reconnaissance du certificat

2.7.1 *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 :

2.7.2 *Reconnaissance internationale critères communs (CCRA)*

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

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

[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 : - ZoneCentral version Q.2021.1 Cible de sécurité CC niveau EAL3+, référence PX2051295r6, version 1.6, mars 2022.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Évaluation Projet : ZONECENTRAL2021, référence OPPIDA/CESTI/CC/ZONECENTRAL2021/RTE, version 2.0, 30 juin 2022.
[ANA_CRY]	Rapport d'analyse des mécanismes cryptographiques - Rapport d'analyse des mécanismes cryptographiques : ZONECENTRAL2021, référence OPPIDA/CESTI/ZONECENTRAL2021/CRYPTO/2.0, version 2.0, 25 mai 2022.
[CONF]	Liste de configuration du produit : - ZoneCentral Q.2021 Liste de configuration, référence PX2131462, version 1.3.
[GUIDES]	Guide d'installation du produit : - ZoneCentral Q.2021 Guide d'installation, référence PX20A1391, version 1.1. Guide d'utilisation des zones : - ZoneCentral Q.2021 Guide d'utilisation des zones, référence PX20A1386, version 1.2. Guide administrateur du produit : - ZoneCentral Q.2021 Guide administrateur, référence PX20A1380, version 1.3. Guide d'utilisation de ZoneBoard : - ZoneCentral Q.2021 Guide d'utilisation de ZoneBoard, référence PX20A1389, version 1.1. Guide de démarrage rapide : - ZoneCentral Q.2021 Guide de démarrage rapide, référence PX20A1382, version 1.1. Mise en œuvre de la signature des politiques : - Mise en œuvre de la signature des politiques, référence PX13C133, version 1.4. Manuel des politiques : - Q.2021 Manuel des politiques, référence PX20A1376, version 1.2.

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.
[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.