PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2020/31

ZoneCentral version 6.2, build 3030

Paris, le 23 octobre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2020/31**
Nom du produit **ZoneCentral**
Référence/version du produit **version 6.2, build 3030**
Conformité à un profil de protection **Aucun**
Critère d'évaluation et version **Critères Communs version 3.1 révision 4**
Niveau d'évaluation **EAL 3 augmenté** ALC_FLR.3, AVA_VAN.3
Développeur **PRIM'X TECHNOLOGIES S.A** Immeuble SKY56 18, rue du général Mouton-Duvernet 69003 Lyon, France
Commanditaire **PRIM'X TECHNOLOGIES S.A** 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 ALC_FLR.3. **SOG-IS** Ce certificat est reconnu au niveau EAL3 augmenté de ALC_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 national 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 6.2, build 3030 » développé par PRIM'X TECHNOLOGIES S.A.

Ce produit est destiné à préserver la confidentialité des documents manipulés par les utilisateurs que ce soit sur des postes isolés, des ordinateurs portables, ou des postes de travail connectés à un réseau d'un organisme. Ce produit de sécurité pour postes de travail opère avec des processeurs 64 bits sous les systèmes d'exploitation MICROSOFT WINDOWS 7 (64 bits) et WINDOWS 10 versions 1809 et 1903 (64 bits).

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 :

- l'administration du produit en rapport avec les rôles des utilisateurs ;
- l'identification et l'authentification des utilisateurs ;
- le chiffrement des zones et des fichiers *swap*[1] ;
- la définition et la gestion des zones chiffrées (droits d'accès, chiffrement, déchiffrement, nettoyage des données sensibles) ;
- l'effacement par surcharge des fichiers supprimés dans des zones en clair ;
- la vérification des politiques de sécurité ;
- l'intégrité du fichier de contrôle à l'ouverture d'une zone ;
- la génération d'évènements en rapport avec le fonctionnement de la TOE pour alimenter le journal d'audit du système d'exploitation ;
- les opérations cryptographiques pour la gestion des clés de zones (création, accès, suppression) et les opérations de calcul associées, réalisées dans des zones mémoires dédiées.

1.2.3 *Architecture*

L'architecture du produit ainsi que les composants qui composent le produit sont décrits au §2.3 de la [ST].

Le périmètre logique est décrit au §2.3.2.1 de la [ST].

Le périmètre physique est décrit au §2.3.2.2 de la [ST].

Les fonctionnalités, listées ci-après, sont hors périmètre de l'évaluation :

- l'outil GPOSign.exe permettant à l'administrateur de sécurité de signer les politiques. En revanche, la vérification de la signature des politiques par ZoneCentral fait bien partie du périmètre de la TOE ;
- l'utilisation du 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

[1] Fichier d'échange de la mémoire virtuelle de WINDOWS.

de WINDOWS ou du composant SSO tiers). En revanche, la présentation de la clé d'accès, avant l'ouverture de session, qui permet à la fois d'ouvrir les zones et la session WINDOWS, fait partie du périmètre ;
- l'interface de programmation (API).

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 en s'appuyant sur les informations fournies au §5.1 de [G_INSTAL].

1.2.5 *Cycle de vie*

Le cycle de vie du produit est le suivant :
- le développement du logiciel se déroule dans les locaux de PRIM'X TECHNOLOGIES S.A situés à Lyon ;
- l'administration, l'installation 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
Immeuble SKY56
18, rue du général Mouton-Duvernet
69003 Lyon, France

Pour l'évaluation, l'évaluateur a considéré trois rôles :
- l'administrateur de la sécurité et de l'environnement WINDOWS des utilisateurs. Il fixe la règle générale de sécurité à appliquer et définit les politiques de sécurité, c'est-à-dire le paramétrage de fonctionnement du produit ;
- l'administrateur de la TOE. Il est en charge de l'installation de la TOE, de définir les zones chiffrées, de configurer la liste des personnes associées à chacune des zones, des opérations de recouvrement et de la mise à disposition des clés d'accès et éventuellement des mots de passe ;
- l'utilisateur de la TOE. Il utilise la TOE selon la configuration imposée.

1.2.6 *Configuration évaluée*

La plateforme de tests retenue est la suivante :

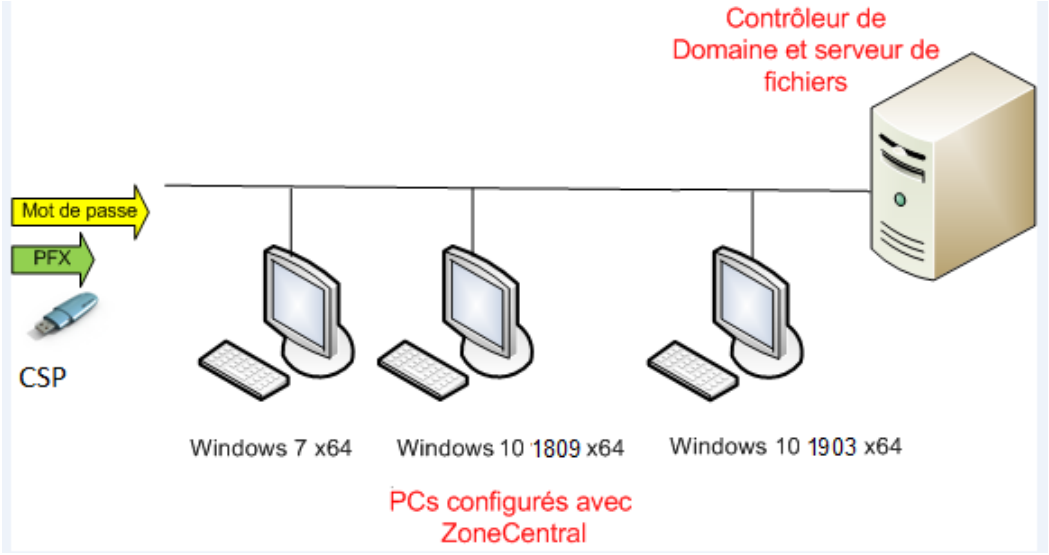

Figure 1 – Plateforme de tests

Elle est constituée des élément suivants :

- d'un poste utilisateur équipé du système d'exploitation de type WINDOWS 7 (64 bits) et d'une authentification par mot de passe ;
- d'un second poste utilisateur équipé du système d'exploitation de type WINDOWS 10 (64 bits), version 1809 et fichier de clés (pfx) ;
- d'un troisième poste utilisateur équipé d'un système d'exploitation de type WINDOWS 10 (64 bits), version 1903 et d'un token physique (lecteur de carte à puce PKC#11 avec une carte à puce GEMALTO) ;
- d'un dernier poste utilisateur équipé du système d'exploitation WINDOWS 10 (64 bits), version 1903 et de CSP certificates ;
- d'un serveur équipé du système d'exploitation WINDOWS 2008 Server R2 Datacenter. Il fait office de contrôleur de domaine, d'annuaire LDAP et de PKI. Il est constitué de WINDOWS 2008 Server R2 Datacenter.

Le *middleware* PKC#11 de la carte à puce GEMALTO est installé sur chacun des systèmes d'exploitation.

Les tests ont été réalisés en considérant les politiques de sécurité suivantes :

- politique P702 : la durée de validité des mots de passe est limitée à 90 jours ;
- politique P710 : le seuil d'acceptation des mots de passe est de 100% ;
- politique P712 : la longueur des mots de passe est de 12 caractères ;
- politique P380 : le mode de chiffrement est CTS-3 ;
- politique P383 : le mode de chiffrement RSA est PKCS#11 v2.2 avec utilisation de SHA 256 ;
- politique P382 : l'usage du jeu d'instruction AES-NI n'est pas autorisé ;
- politique P292 : l'algorithme de HASH utilisé est SHA-256 ;
- politique P386 : le mécanisme de signature est PKCS#11 v2.2 PSS ;
- politique P396 : le contrôle des listes d'accès est configuré à « contrôle de la signature et de la taille » ;
- politique P131 : l'accès obligatoire est configuré avec « un accès de recouvrement ».

Pour plus de détails sur ces politiques, le lecteur se reportera à [G_POLICY].

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].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 4 septembre 2020, 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 conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Les mécanismes analysés sont conformes aux exigences des référentiels cryptographiques de l'ANSSI. 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 [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

La TOE supporte trois DRBG[2], à savoir :
- DRBG HASH (SHA 256 et SHA512, DRBG HASH SHA 512 étant le générateur par défaut) ;
- DRBG HMAC (SHA 256 et SHA 512) ;
- DRBG CTR (AES 256 avec fonction de dérivation).

Ces trois générateurs ont fait l'objet d'une analyse qui démontre qu'ils sont conformes à l'état de l'art.

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.

[2] *Deterministic Random Bit Generator*.

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 6.2, build 3030 » 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 et 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 les politiques de sécurité identifiées au §1.2.6 de ce rapport de certification doivent être mises en oeuvre.

Comme mentionné dans la cible de sécurité (voir [ST]), il est important de souligner que l'intégrité des fichiers chiffrés ne fait partie des objectifs de sécurité de la TOE.

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[3], 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 :

3.3.2 *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[4] , des certificats Critères Communs.

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

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

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 :

ANNEXE A. 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*

ANNEXE B. Références documentaires du produits évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - ZoneCentral version 6.2, Cible de sécurité CC niveau EAL3+, référence PX171727, version 1r7, janvier 2020, PRIM'X TECHNOLOGIES SA.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Évaluation, projet ZONECENTRAL6.1, référence OPPIDA/CESTI/ZONECENTRAL6.1/RTE, version 2.0, 4/9/2020, OPPIDA.
[ANA-CRY] [EXP-CRY]	Rapport d'analyse des mécanismes cryptographiques, Expertise cryptographique – ZoneCentral, référence OPPIDA/CESTI/ZONECENTRAL6.1/CRYPTO, version 5.0, 19/5/2020, OPPIDA.
[CONF]	Liste de configuration du produit : - ZoneCentral 6.2, Liste de configuration de la version 6.2 Build 3030, référence PX189934r6, 3/9/2020, PRIM'X TECHNOLOGIES SA.
[GUIDES]	Guide d'installation du produit : - [G_INSTAL] : ZoneCentral 6.2, Guide d'installation FR, référence PX187881, PRIM'X TECHNOLOGIES SA. Guides d'administration du produit : - [G_POLICY] : Manuel des politiques, référence PX187870r3, PRIM'X TECHNOLOGIES SA ; - [G_ADMIN] : ZoneCentral 6.2, Guide administrateur FR, référence PX187883r5, PRIM'X TECHNOLOGIES SA. Guide d'utilisation du produit : - [G_USER] : ZoneCentral 6.2, Guide d'utilisation des zones chiffrées FR, référence PX187874r4, PRIM'X TECHNOLOGIES SA.

ANNEXE C. 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 ANSSI-CC-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, 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.