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

Affaire suivie par Olivier LE ROCH

Paris, le 13 MAI 2016

N°1820 /ANSSI/SDE/PSS/BQA

QUALIFICATION AU NIVEAU STANDARD

ZED ! V6.1
(SOUS WINDOWS SEVEN ET WINDOWS 10)
PRIM'X TECHNOLOGIES

Références

[a] Processus de qualification d'un produit de sécurité - niveau standard -, version 1.2, disponible sur www.ssi.gouv.fr.
[b] Cible de sécurité de ZED !V6.1, réf. n°PX14A459r4 d'avril 2015.
[c] Rapport technique d'évaluation Projet ZED6, réf. n°OPPIDA/CESTI/RTE/ZED6 du 29/02/2016.
[d] Note technique - Recommandations de sécurité relatives aux mots de passe, ANSSI, n°DAT-NT-001/ANSSI/SDE/NP du 5 juin 2012, disponible sur www.ssi.gouv.fr.
[e] Zed! 6.1 Guide d'installation FR, réf. PX156516, version v1r2 du 11/12/2015.
[f] Manuel des politiques 6.1 FR, réf. PX156524, version v1r1 du 24/10/2015.
[g] Zed! 6.1 Guide d'utilisation des conteneurs chiffrés FR, réf. PX156518, version v1r4 du 29/02/2016.
[h] Zed! Limited Edition 6.1 Guide FR, réf. PX156523, version v1r3 du 29/02/2016.

Le produit ZED! en version v6.1, en déclinaisons « standard » et « limité », 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). Le produit intègre par ailleurs un mécanisme de contrôle de l'intégrité des fichiers stockés dans les conteneurs.

Eu égard au rapport technique d'évaluation [c], et conformément au processus de qualification au niveau standard [a], j'atteste que ce produit, dans ses déclinaisons « standard » et « limité », atteint le niveau de qualification standard, sous réserve :

- du respect des guides ([e], [f], [g], [h]) et des hypothèses de la cible de sécurité [b], et
- de la prise en compte des restrictions d'emploi et recommandations issues du rapport technique d'évaluation, notamment :
  - la politique P399 (version du format des conteneurs et messages chiffrés) doit être configurée à « Version 2 » ;
  - la politique P383 (mode de chiffrement RSA) doit être configurée à « PKCS#1 v2.2 avec utilisation de SHA-256 »
  - la politique P382 (autoriser l'utilisation du jeu d'instructions AES-NI) doit être configurée à « Non » (valeur par défaut) ;

- la politique P381 (mécanisme de chiffrement pour les conteneurs chiffrés) doit être configurée à « CBCCTS » (valeur par défaut) ;
- la politique P292 (algorithme de hash utilisé) doit être configurée à « SHA-256 » (valeur par défaut) ;
- la politique P233 (masquage des noms de fichiers et de dossiers des conteneurs chiffrés) doit être configurée à « Toujours masquer » ;
- la politique P730 doit être configurée pour fixer le seuil d'acceptation des mots de passe à 100% ; les autres politiques (P732 à P740) doivent ensuite être utilisées pour fixer le niveau de complexité des mots de passe attendu conformément à la note technique de l'ANSSI [d].

Le produit est de plus agréé[1] pour la protection d'informations sensibles marquées ***Diffusion Restreinte***, ou **classifiées au niveau *Diffusion Restreinte OTAN*, *Restreint UE/UE Restricted* ou *EUROCOR Diffusion Restreinte*.**

Cette qualification est valable pour une durée de 3 ans. Elle pourra être prolongée par la mise sous surveillance du produit certifié.

[1] Cet agrément concerne le produit ZED ! V6.1 seul. Il ne dispense pas de la réalisation d'une homologation de sécurité, conformément aux exigences de l'IGI 1300 du 30 novembre 2011, qui permet notamment d'attester que les postes sur lesquels sont effectuées les opérations de chiffrement/déchiffrement sont aptes à traiter des informations du niveau considéré.