

Secrétariat général  
de la défense  
et de la sécurité nationale

Paris, le 06 JUIN 2016  
N° 2637 /ANSSI/SDE

Agence nationale de la sécurité  
des systèmes d'information

Bureau Qualification et Agrément

## QUALIFICATION AU NIVEAU STANDARD

**ZED ! v6.1**  
**(SOUS WINDOWS 8.1)**  
*PRIM'X TECHNOLOGIES*

Le produit ZED! en version 6.1, en déclinaison « 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.

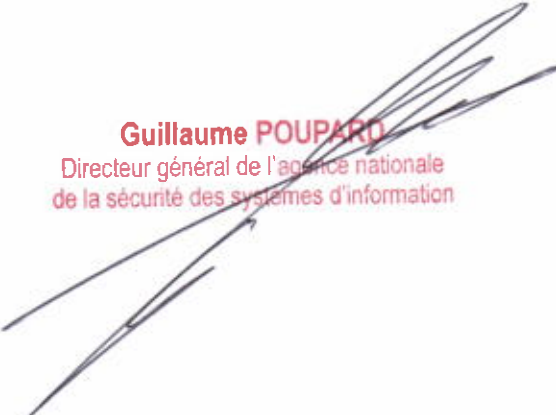
Suite à la qualification initiale sur les plateformes WINDOWS SEVEN et WINDOWS 10 [3], et au complément d'évaluation effectué [4], j'atteste que ce produit, dans ces déclinaisons « standard » et « limité », atteint le niveau de qualification standard pour la plateforme WINDOWS 8.1, sous réserve :

- du respect des guides ([6], [7], [8], [9]) et des hypothèses de la cible de sécurité [2], et
- de la prise en compte des restrictions d'emploi et recommandations issues du rapport technique d'évaluation, notamment :
  - o la politique P399 (version du format des conteneurs et messages chiffrés) doit être configurée à « Version 2 » ;
  - o la politique P383 (mode de chiffrement RSA) doit être configurée à « PKCS#1 v2.2 avec utilisation de SHA-256 » ;
  - o la politique P382 (autoriser l'utilisation du jeu d'instructions AES-NI) doit être configurée à « Non » (valeur par défaut) ;
  - o la politique P381 (mécanisme de chiffrement pour les conteneurs chiffrés) doit être configurée à « CBCCTS » (valeur par défaut) ;
  - o la politique P292 (algorithme de hash utilisé) doit être configurée à « SHA-256 » (valeur par défaut) ;
  - o la politique P233 (masquage des noms de fichiers et de dossiers des conteneurs chiffrés) doit être configurée à « Toujours masquer » ;
  - o 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 [5].

Le produit est de plus agréé<sup>1</sup> pour la protection d'informations sensibles marquées ***DIFFUSION RESTREINTE***, ou classifiées au niveau ***DIFFUSION RESTREINTE OTAN, RESTREINT UE/EU 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 qualifié.

**Guillaume POUPARD**  
Directeur général de l'agence nationale  
de la sécurité des systèmes d'information



---

<sup>1</sup> 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.

## Annexe

### Références

- [1]. Processus de qualification d'un produit de sécurité - niveau standard -, version 1.2, disponible sur [www.ssi.gouv.fr](http://www.ssi.gouv.fr).
- [2]. Cible de sécurité de ZED !V6.1, réf. n°PX14A459r4 d'avril 2015.
- [3]. Décision de qualification au niveau standard de ZED ! v6.1 (sous WINDOWS 7 et WINDOWS 10), réf. n°1820/ANSSI/SDE/PSS/BQA du 13 mai 2016.
- [4]. Rapport de tests ZED6-Complément, réf. n°OPPIDA/CESTI/ZED6/TESTS-WINDOWS8/1.0.
- [5]. 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](http://www.ssi.gouv.fr).
- [6]. Zed! 6.1 Guide d'installation FR, réf. PX 156516, version v1r2 du 11 décembre 2015.
- [7]. Manuel des politiques 6.1 FR, réf. PX156524, version v1r1 du 24 octobre 2015.
- [8]. Zed! 6.1 Guide d'utilisation des conteneurs chiffrés FR, réf. PX 156518, version vi r4 du 29 février 2016.
- [9]. Zed! Limited Edition 6.1 Guide FR, réf. PX156523, version v1r3 du 29 février 2016.