

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité
des systèmes d'information

Bureau Qualifications et Agréments

Paris, le 21 DEC. 2018
N°18134 /ANSSI/SDE/PSS/BQA

DECISION DE QUALIFICATION D'UN PRODUIT
AU NIVEAU STANDARD

ZED!version 6.1 build 2121

SOUS WINDOWS SEVEN, WINDOWS 8.1 ET WINDOWS 10

PRIM'X TECHNOLOGIES

RCS 448 603 985

27, rue Maurice Flandin

69 444 Lyon Cedex 03

France

Pièces constitutives de la décision de qualification :

Fiche 1 : Description du produit.

Fiche 2 : Conditions et limites de la qualification.

Fiche 3 : Base documentaire de la qualification.

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

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment son article 9 ;

Vu le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », notamment son article 1^{er} ;

Vu le décret du 27 mars 2014 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Vu la décision du 22 octobre 2014 portant délégation de signature (Secrétariat général de la défense et de la sécurité nationale) ;

Vu l'instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015, relative à la protection des systèmes d'information sensibles ;

Vu l'instruction générale interministérielle n° 2102 du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union européenne ;


Vu l'instruction générale interministérielle n° 2100 du 1^{er} décembre 1975 sur l'application en France du système de sécurité de l'organisation du traité de l'Atlantique Nord ;

Vu le *Processus de qualification d'un produit*,

Décide :

- Art. 1^{er} – Le produit fourni par la société *PRIM'X TECHNOLOGIES* portant le nom *ZED!* en version 6.1 *build 2121* respecte les règles fixées par le décret n° 2010-112 du 2 février 2010 et est qualifié au niveau « Standard » sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.
- Art. 2 – La fonction de création et de consultation de conteneurs de répertoires et de fichiers chiffrés et compressés est agréée pour la protection des informations marquées *Diffusion Restreinte* ou classifiées au niveau *Diffusion Restreinte OTAN* ou *Restreint UE/UE Restricted*.
- Art. 3 – La présente décision est valable jusqu'au 6 juillet 2019.
- Art. 4 – La présente décision annule et remplace les décisions [QUALIF1], [QUALIF2] et [QUALIF3].
- Art. 5 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.

Guillaume POMERAI
Directeur général de l'Agence nationale
de la sécurité des systèmes d'information



Fiche 1

Description du produit

Désignation et versions

Le produit qualifié est la solution logicielle *ZED!* en version 6.1 *build 2121* fournie par l'entreprise *PRIM'X TECHNOLOGIES*. Cette qualification couvre les déclinaisons « Standard » et « Limité » sur les plateformes *WINDOWS SEVEN*, *WINDOWS 8.1* et *WINDOWS 10*.

Présentation générale

Le produit *ZED!* en version 6.1 *build 2121*, 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.

Le *build 2121* permet, dans les conditions énoncées ci-dessous, un premier niveau de correction de la vulnérabilité décrite dans la CVE CERTFR-2018-AVI-440 [CVE].

Fiche 2

Conditions et limites de la qualification

Conditions

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

Lors de la mise en œuvre du produit, l'autorité d'emploi doit s'assurer que :

- C1. Les guides ([GUIDE_INSTALL], [MANUEL_POL], [GUIDE_UTIL] et [GUIDE_LIMITED]) sont respectés ;
- C2. Les restrictions d'emploi et recommandations issues du rapport technique d'évaluation des décisions [QUALIF2] et [QUALIF3] sont prises en compte. Cela comprend notamment la configuration des éléments suivants :
 - 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 attendu des mots de passe conformément à la note technique de l'ANSSI [MDP].
- C3. En complément, l'élément suivant doit être configuré :
 - **l'utilisation du *Watermark* doit être désactivée via l'option *DisableWatermark* de la politique P289 (options des conteneurs chiffrés) qui doit prendre la valeur « 1 » (valeur par défaut).**

Limites

- L1. Seules les fonctions décrites dans la fiche 1 sont couvertes par la présente décision de qualification.

Fiche 3

Base documentaire de la qualification

Cadre réglementaire

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, note n° 274/ANSSI/SDE du 12 janvier 2017, référence QUAL-PROD-PROCESS, version en vigueur. Disponible sur : https://www.ssi.gouv.fr/qualification-processus
[RGS]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Disponible sur : https://www.legifrance.fr
[II 901]	Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015, relative à la protection des systèmes d'information sensibles. Disponible sur : https://www.legifrance.gouv.fr/ .
[IGI 2100]	Instruction générale interministérielle n° 2100 du 1 ^{er} décembre 1975 sur l'application en France du système de sécurité de l'organisation du traité de l'Atlantique Nord.
[IGI 2102]	Instruction générale interministérielle n° 2102 du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union européenne

Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[QUALIF1]	Décision de qualification au niveau standard du produit <i>ZED!</i> en version 6.1 (<i>build 2121</i>) pour les plateformes <i>WINDOWS SEVEN</i> , <i>WINDOWS 8.1</i> et <i>WINDOWS 10</i> . - référence : 17217/ANSSI/SDE/PSS/BQA - en date du : 22 octobre 2018
[QUALIF2]	Décision de qualification au niveau standard du produit <i>ZED!</i> en version 6.1 (<i>build 2120</i>) pour les plateformes <i>WINDOWS SEVEN</i> et <i>WINDOWS 10</i> . - référence : 1820/ANSSI/SDE/PSS/BQA - en date du : 13 mai 2016
[QUALIF3]	Décision de qualification au niveau standard du produit « <i>ZED!</i> » en version 6.1 (<i>build 2120</i>) pour la plateforme <i>WINDOWS 8.1</i> . - référence : 2617/ANSSI/SDE - en date du : 6 juillet 2016
[MDP]	Note technique – Recommandations de sécurité relatives aux mots de passe. Disponible sur https://www.ssi.gouv.fr . - référence : DAT-NT-001/ANSSI/SDE/NP - en date du : 5 juin 2012
[CVE]	CVE CERTFR-2018-AVI-440

Guides d'utilisation et documentations techniques de l'industriel

[GUIDE_INSTALL]	Guide d'installation FR. - référence : PX156516 - version : v1r2 - en date du : 11 décembre 2015
[MANUEL_POL]	Manuel des politiques FR. - référence : PX156524 - version : v2.5 - en date du : 4 octobre 2018
[GUIDE_UTIL]	Guide d'utilisation des conteneurs chiffrés FR. - référence : PX156518 - version : v6.5 - en date du : 4 octobre 2018
[GUIDE_LIMITED]	<i>ZED! Limited Edition 6.1</i> Guide FR. - référence : PX156518 - version : v1r4 - en date du : 29 février 2016