PREMIÈRE
MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Le Directeur général

Paris, le 15 DEC. 2023
N°2173 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU STANDARD

ZED !
VERSION Q2021.X AVEC X≥2

PRIM'X TECHNOLOGIES

RCS 448 603 985

18 rue du Général Mouton-Duvernet
69003 Lyon Cedex
France

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

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 1er ;

Vu le décret du 4 janvier 2023 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. STRUBEL (Vincent) ;

Vu le processus de qualification d'un produit, version en vigueur ;

Vu le rapport de certification, ANSSI-CC-2022/40, 23/08/2022 ;

Vu le dossier de demande de qualification déposé par PRIM'X,

Décide :

Art. 1er – Le produit fourni par la société PRIM'X TECHNOLOGIES portant le nom « ZED ! » en version Q2021.X avec X≥2 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 annexe.

Art. 2 – Le produit fourni par la société PRIM'X portant le nom « ZED !» en version Q2021.X avec X≥2 est agréé pour la protection d'informations marquées Diffusion Restreinte ou classifiées Diffusion Restreinte OTAN/NATO Restricted ou Restreint UE/UE Restricted sous réserve du respect des conditions et limites d'utilisation énoncées en annexe.

Art. 3 – La présente décision est valable jusqu'au 17 octobre 2025.

Vincent STRUBEL
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

Annexe

Conditions et limites de la qualification.

Référence

[1].	Rapport de certification, ANSSI-CC-2022/40, 23/08/2022.
[GUIDE_INSTALL].	Zed! Q.2021.1 Guide d'installation FR, référence PX20A1391, version 1.2.
[GUIDE_ADMIN].	Manuel des politiques Zed ! Q.2021 FR, référence PX20A1376r3 ;
[GUIDE_UTIL].	Zed! Q.2021 Guide d'utilisation des conteneurs chiffrés FR, référence PX20A1397r3

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 :

C0. Elle emploie la version qualifiée du produit la plus à jour.

C1. Les objectifs de sécurité sur l'environnement définis dans la cible de sécurité référencée dans le rapport [1] doivent être respectés.

C2. Les restrictions d'usage figurant dans le rapport [1] doivent être respectées.

C3. Les restrictions d'usage figurant au chapitre 3.2 du rapport de certification [1] pour le produit Zed! doivent être respectées ; l'utilisateur du produit certifié devra en particulier s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [CDS] à savoir :

Mode *Active directory* :

- La politique P131 (accès obligatoires) doit être configuré avec l'accès de recouvrement de l'administrateur. Note : Au moment d'effectuer le recouvrement, les politiques P269 - Ouverture au moyen de clés de recouvrement, P198 - Affichage des accès de recouvrement et P199 - Affichage des accès obligatoires devront être activées. Ces politiques ne sont normalement pas activées dans un environnement de production (notamment pour masquer les accès de recouvrement) et ne font donc pas partie du périmètre de test de l'évaluation).
- La politique P730 (seuil d'acceptation des mots de passe) doit être configurée à 100% et la politique P732 (longueur des mots de passe) doit être configurée à 12.
- La politique P339 (options du rapport de configuration) doit être configurée à « 0 » qui permet la collecte (valeur par défaut), il faut également renseigner le mot NONE dans le nom de la valeur de la politique P137 (accès imposés lors du chiffrement des informations collectées).
- La politique P381 (mécanisme de chiffrement pour les conteneurs chiffrés) doit être configurée à « CTS » (valeur par défaut).

- La politique P382 (autoriser l'utilisation du jeu d'instructions AES-NI) doit être configurée à « Non ».
- 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 P386 (mécanisme de signature) doit être configurée à « PKCS#1 v2.2 PSS».
- La politique P387 (mécanisme de dérivation (mot de passe)) doit être configurée à « SHA256-PBKDF2 » ou « SHA512-PBKDF2 ».
- La politique P233 (masquage des noms de fichiers et de dossiers des conteneurs chiffrés) doit être configurée à « Toujours masquer ».

Pour Zed! Entreprise édition complète intégrée dans ZoneCentral :

En plus des politiques ci-dessus (P131, P730 et P732, P339 et P137, P381, P382, P399, P383, P386, P387 et P233), il faut ajouter les politiques ZoneCentral suivantes (qui s'appliquent à la création de la liste d'accès de l'utilisateur) :

- La politique P702 (durée de validité des mots de passe) doit être configurée à une valeur inférieure à 90 jours.
- La politique P710 (seuil d'acceptation des mots de passe) doit être configurée à 100% et la politique P712 (longueur des mots de passe) doit être configurée à 12.

Mode Alternatif :

Pour Zed! Entreprise édition complète :

- Toutes les politiques ci-dessus (P131, P730 et P732, P339 et P137, P381, P382, P399, P383, P386, P387 et P233) sont à configurer dans le fichier de configuration des politiques dédié au mode alternatif.

En dehors de ce fichier, il faut configurer la suivante dans les politiques *Active Directory*:

- La politique P070 (configuration alternative des politiques) doit être configurée en indiquant le chemin du fichier de configuration alternative des politiques

Pour Zed! Entreprise édition complète intégrée dans ZoneCentral :

En plus des politiques ci-dessus (P131, P730 et P732, P339 et P137, P381, P382, P399, P383, P386, P387 et P233), il faut ajouter les politiques ZoneCentral suivantes dans le fichier de configuration des politiques dédié au mode alternatif (qui s'appliquent à la création de la liste d'accès de l'utilisateur) :

- La politique P702 (durée de validité des mots de passe) doit être configurée à une valeur inférieure à 90 jours.
- La politique P710 (seuil d'acceptation des mots de passe) doit être configurée à 100% et la politique P712 (longueur des mots de passe) doit être configurée à 12.

En dehors de ce fichier, il faut configurer la suivante dans les politiques *Active Directory*:

- La politique P070 (configuration alternative des politiques) doit être configurée en indiquant le chemin du fichier de configuration alternative des politiques

C4. Les guides d'installation [GUIDE_INSTALL], d'administration [GUIDE_ADMIN] et d'utilisation [GUIDE_UTIL] sont mis en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout au long de son cycle de vie.

C5. Dans le cas d'un usage pour la protection d'informations *Diffusion Restreinte*, *Restreint OTAN/NATO Restricted* ou *Restreint UE/UE Restricted*, le système d'information support doit également être homologué pour ce même niveau.

C6. Pour chaque nouvel envoi, il est nécessaire de créer un nouveau conteneur chiffré.

C7. Afin de renforcer le contrôle d'intégrité, la politique P234 doit interdire l'ouverture de conteneurs ZED au format 2.2. A cet effet, elle doit être configurée en ajoutant la ligne « ZedFormatVersion2.2 | Deny ».

Limite

L1. Seules les fonctions identifiées dans le rapport [1] sont couvertes par la présente décision de qualification.