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 17 OCT. 2022
N°2241 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU STANDARD

ZED! version Q.2021.1

Sous Windows 10 (64 Bits)

PRIM'X TECHNOLOGIES

RCS 448 603 985

18 rue du Général Mouton-Duvernet
69003 LYON CEDEX
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 1er ;

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 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 1er 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. 1er – Le produit fourni par la société PRIM'X TECHNOLOGIES portant le nom « ZED! » en version Q.2021.1 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 pour une durée de trois ans.

Art. 4 – 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 POUPARD
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 Q.2021.1 fournie par l'entreprise PRIM'X Technologies.

Cette qualification couvre les produit « ZED! ENTREPRISE EDITION COMPLETE » version Q.2021.1 et « ZED! ENTREPRISE EDITION COMPLETE » version Q.2021.1 intégré dans « ZONECENTRAL » version Q.2021.1 en version exécutable avec les politiques de sécurité activées en section 2.3.2.1 de la cible de sécurité [CDS].

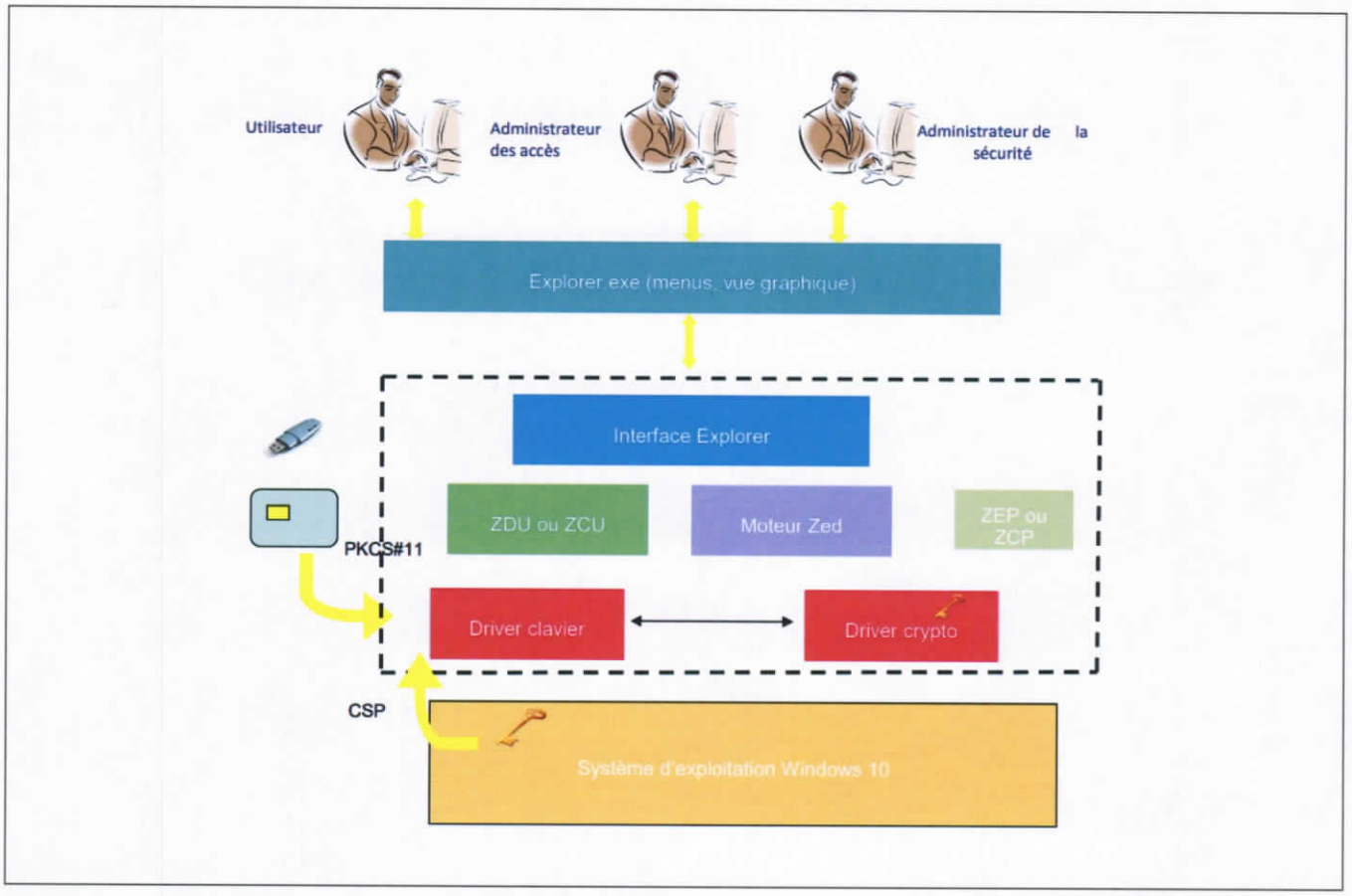

Figure 1. Cas d'usage classique du produit

Présentation générale

Le produit évalué est « ZED! » en version Q.2021.1 fournie par l'entreprise PRIM'X TECHNOLOGIES sous *WINDOWS 10* (64 Bits).

Le produit ZED! est constitué des composants suivants :

- Le module « Interface Explorer » qui permet de gérer les menus et la vue graphique ;
- Le module « ZDU » (ou « ZCU » dans ZoneCentral) est un «daemon» utilisateur instancié pour chaque session utilisateur Windows et qui référence les clés utilisateur saisies via l'entrée d'un mot de passe, l'interface PKCS#11, le *Cryptographic Service Provider* (CSP) ou le *Cryptographic Next Generation* (CNG) ;
- Le service « ZEP » (ou « ZCP » dans ZoneCentral) qui contrôle la signature des politiques ;

- Le module « Moteur Zed » qui coordonne les différents traitements ;
- Le « driver crypto » qui est le centre cryptographique de Zed! ou de ZoneCentral : il gère les clés de conteneur et exécute les opérations de calcul associées. Les clés ne sortent jamais de son enceinte, sauf lorsque le produit est configuré pour utiliser des porte-clés (comme des extensions PKCS#11 pour des cartes à puce ou des CSPs/CNGs). Cette implémentation de la cryptographie en mode kernel du système renforce le niveau de protection global car c'est un emplacement très difficilement accessible aux logiciels 'pirates'.
- Le « driver clavier » qui est un filtre de saisie clavier dans Zed! ou ZoneCentral : il intercepte à très bas niveau les mots de passe et codes confidentiels saisis de façon à ce que leur valeur reste confinée le plus bas possible dans le système. Ils sont ensuite utilisés par le driver cryptographique, ou remis aux moteurs externes (CSP/PKCS#11). Cela ne concerne que les mots de passe gérés par Zed!, c'est-à-dire ceux qui conditionnent les accès aux fichiers chiffrés. Cette implémentation renforce également la protection de ces données sensibles, qui ne remontent pas au niveau applicatif du système, source régulière et préférée des logiciels 'pirates'.

A noter que :

- Les composants Interface Explorer et Moteur Zed sont les mêmes dans Zed ! Entreprise et ZoneCentral ;
- Les composants ZDU, ZEP, Driver crypto et Driver clavier de Zed ! Entreprise ont leur équivalent dans ZoneCentral (avec les mêmes fonctions et les mêmes interfaces).

Les principaux services de sécurité fournis par le produit sont :

- La protection des conteneurs chiffrés notamment lors de leur ouverture que ce soit pour la lecture, le remplissage ou la gestion des accès ;
- La gestion de la saisie du mot de passe et sa dérivation en une clé d'accès ;
- La gestion de la saisie du code confidentiel du fichier de clés ;
- La gestion de la saisie du code confidentiel du token logique ;
- La conservation dans le conteneur de fichiers et dossiers sous forme chiffrée avec la possibilité de masquer leurs noms ;
- Le contrôle de l'intégrité globale du conteneur chiffré lors de l'ouverture de celui-ci ;
- La protection des différentes clés ;
- La protection de chaque vecteur d'initialisation spécifique à chacun des fichiers ;
- La vérification, avant leur application, des politiques définies par l'administrateur de la sécurité.

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 restrictions d'usage figurant au chapitre 3.2 du rapport de certification [CERTIF] du produit Zed! en version Q.2021.1 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 Q.2021.1 intégrée dans ZoneCentral Q.2021.1 :

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 Q.2021.1 :

- 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 Q.2021.1 intégrée dans ZoneCentral Q.2021.1 :

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

C2. 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.

C3. Dans le cas d'un usage pour la protection d'informations ***Diffusion Restreinte***, ***Restreint OTAN*** ou ***Restreint UE/UE Restricted***, le système d'information support doit également être homologué pour ce même niveau.

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 1er 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 le centre d'évaluation

[RTE]	Rapport technique d'évaluation, référence OPPIDA/CESTI/CC/ZED/RTE, version 3.0, 30 juin 2022. Pour le besoin des évaluations en composition un rapport technique pour la composition a été validé : rapport de composition, référence OPPIDA/CESTI/ZED2021/COMPO, version 2.0, 30 juin 2022.
[ANALYSE_CRYPTO]	Rapport d'analyse des mécanismes cryptographiques ZED2021, référence OPPIDA/CESTI/ZED2021/CRYPTO, version 2.0, 20 avril 2022.
[SITE]	Rapport de visite sur site, référence OPPIDA/CESTI/CC/ZED2021/ALC/Rapport audit sur site/1.0, 20 juillet 2021

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

[CERTIF]	Rapport de certification, référence ANSSI-CC-2022/40, 23 août 2022.
[CRYPTO]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

Guides d'utilisation et documentations techniques de l'industriel

[GUIDE_INSTALL]	Guide d'installation du produit : - Zed! Q.2021.1 Guide d'installation FR, référence PX20A1391, version 1.2.
[GUIDE_ADMIN]	Guide d'administration : - Mise en œuvre de la signature des politiques FR, référence PX13C133, version 1.4.
[MANUEL_POL]	Manuel des politiques : - Manuel des politiques Q.2021 FR, référence PX20A1376, version 1.2.
[GUIDE_UTIL]	Guide d'utilisation des conteneurs chiffrés : - Zed! Q2021.1 Guide d'utilisation des conteneurs chiffrés FR, référence PX20A1397, version 1.2

[CDS]	Cible de sécurité de référence pour l'évaluation : - PRIMX-Zed Q.2021 Cible de Sécurité, référence PX2051296r5, version 1.5, avril 2021
[CONF]	Liste de configuration du produit : - PRIMX-Zed Q.2021 Liste de configuration, référence PX2131463, version 1.3, 30 juin 2022.