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° 2246 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU STANDARD

ZONECENTRAL 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 « ZONECENTRAL » 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 « ZONECENTRAL » en version Q.2021.1 fournie par l'entreprise PRIM'X Technologies sous le système d'exploitation Windows 10 versions 1809 LTSC et 20H2 (64 bits) de Microsoft.

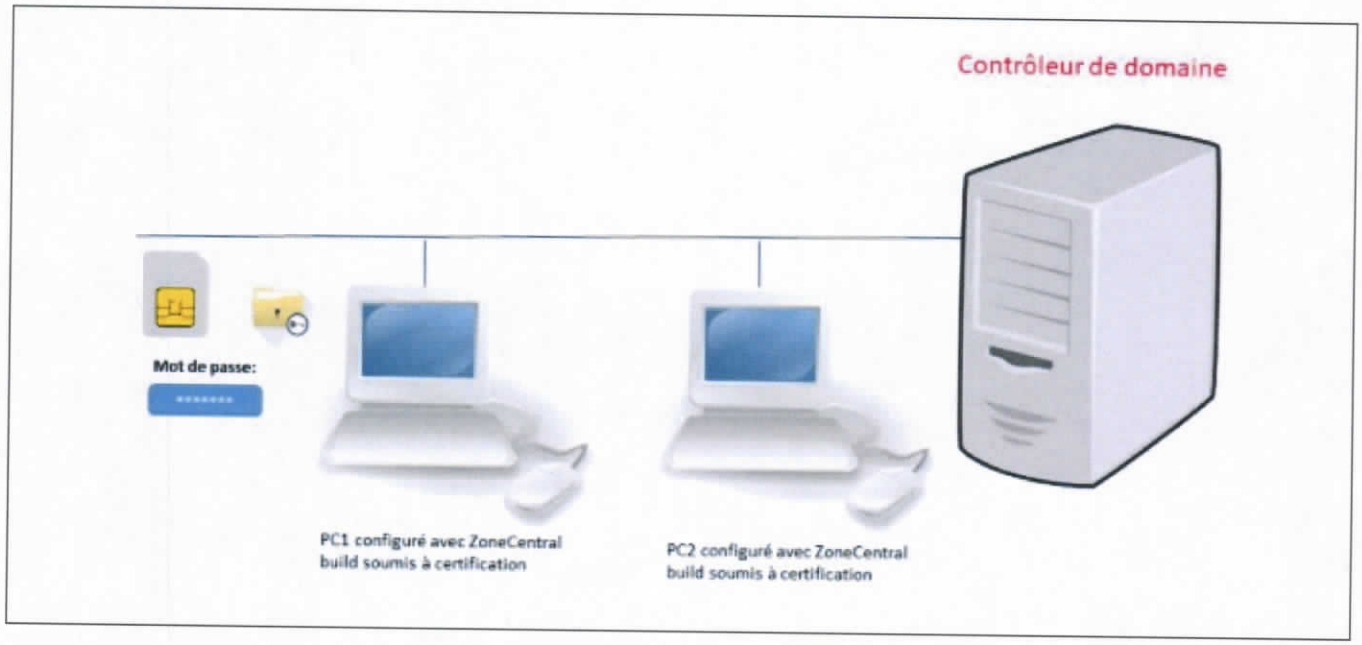

Figure 1. Cas d'usage classique du produit

Présentation générale

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

Le produit ZONECENTRAL, installé sur un équipement de type PC, a en charge de protéger en confidentialité les documents manipulés par les utilisateurs. Il offre un stockage chiffré des fichiers, sans modifier leurs caractéristiques (emplacement, nom, dates, tailles). Le chiffrement est effectué in-place (là où résident les fichiers) et à la volée (sans manipulation particulière de l'utilisateur). Afin de simplifier la gestion des fichiers chiffrés, ZONECENTRAL est basé sur le principe de zones : une zone chiffrée est un volume ou un dossier, avec tout ce qu'il contient.

Les principaux services de sécurité fournis par le produit sont :

- la protection en confidentialité par chiffrement des fichiers ;
- la gestion du contrôle d'accès aux zones chiffrées par l'utilisateur ;
- l'authentification des utilisateurs via une clé dérivée d'un mot de passe ou via une clé RSA stockée sur un porte-clé électronique (token USB, fichier de clé ou conteneur CSP/CNG) ;
- l'administration des zones permettant de gérer les clés et les accès (en particulier l'accès de recouvrement) ;
- la journalisation des évènements.

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 ZONECENTRAL 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 P278 (dossiers temporaires pour l'agent de chiffrement) doit être configurée en indiquant un emplacement local au poste de l'utilisateur (par exemple %USERPROFILE%\EncryptionBackup) et la politique P499 avec le nom de valeur PreferAlternateBackupLocationsOnNetwork doit être configurée avec la valeur « 1 ». Il faut également s'assurer que les autres utilisateurs n'ont pas d'accès en lecture à l'emplacement choisi.
- 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.
- La politique P303 (activer les événements pour toutes les opérations d'administration) doit être configurée à « oui ».
- 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 P380 (mécanisme de chiffrement) doit être configurée à « CTS-3 »
- La politique P382 (autoriser l'utilisation du jeu d'instructions AES-NI) doit être configurée à « Non ».
- 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 P398 (contrôle d'intégrité des zones chiffrées) doit être configurée à « contrôle avec avertissement d'absence d'informations d'intégrité »

Mode Alternatif :

Toutes les politiques ci-dessus (P131, P278, P499, P702, P710 et P712, P303, P339 et P137, P380, P382, P383, P386, P387 et P398) 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.

Dans les 2 modes, toutes les autres politiques sont configurées avec leur valeur par défaut.

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 Projet : ZONECENTRAL2021, référence OPPIDA/CESTI/CC/ZONECENTRAL2021/RTE, version 2.0, 30 juin 2022
[ANALYSE_CRYPTO]	Rapport d'analyse des mécanismes cryptographiques : ZONECENTRAL2021, référence OPPIDA/CESTI/ZONECENTRAL2021/CRYPTO/2.0, version 2.0, 25 mai 2022.
[SITE]	Rapport de visite sur site, référence : OPPIDA/CESTI/CC/ZONECENTRAL2021/ 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-2022/39, 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 : - ZoneCentral Q.2021 Guide d'installation, référence PX20A1391, version 1.1
[GUIDE_ADMIN]	Guide administrateur du produit : - ZoneCentral Q.2021 Guide administrateur, référence PX20A1380, version 1.3.
[MANUEL_POL]	Mise en œuvre de la signature des politiques : - Mise en œuvre de la signature des politiques, référence PX13C133, version 1.4 Manuel des politiques : - Q.2021 Manuel des politiques, référence PX20A1376, version 1.2.
[GUIDE_UTIL]	Guide d'utilisation des zones : ZoneCentral Q.2021 Guide d'utilisation des zones, référence PX20A1386, version 1.2

	Guide d'utilisation de ZoneBoard : ZoneCentral Q.2021 Guide d'utilisation de ZoneBoard, référence PX20A1389, version 1.1. Guide de démarrage rapide : ZoneCentral Q.2021 Guide de démarrage rapide, référence PX20A1382, version 1.1
[CDS]	Cible de sécurité de référence pour l'évaluation : - ZoneCentral version Q.2021.1 Cible de sécurité CC niveau EAL3+, référence PX2051295r6, version 1.6, mars 2022
[CONF]	Liste de configuration du produit : ZoneCentral Q.2021 Liste de configuration, référence PX2131462, version 1.3

Diffusion interne (par messagerie)

ANSSI DIR – SDE/PSS – SDE/DAT – Laurent Carlander – Eloïse Descarpentrie - chrono informatique.