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°2243 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU STANDARD

CRYHOD version Q.2021.2

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 « CRYHOD » en version Q.2021.2 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 fiche 2.

Art. 2 – La fonction d'authentification et chiffrement de données 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 « CRYHOD » en version Q.2021.2 fournie par l'entreprise PRIM'X TECHNOLOGIES sous Windows 10 (64 Bits).

Cette qualification couvre l'amorçage en mode EFI et le mode SSO.

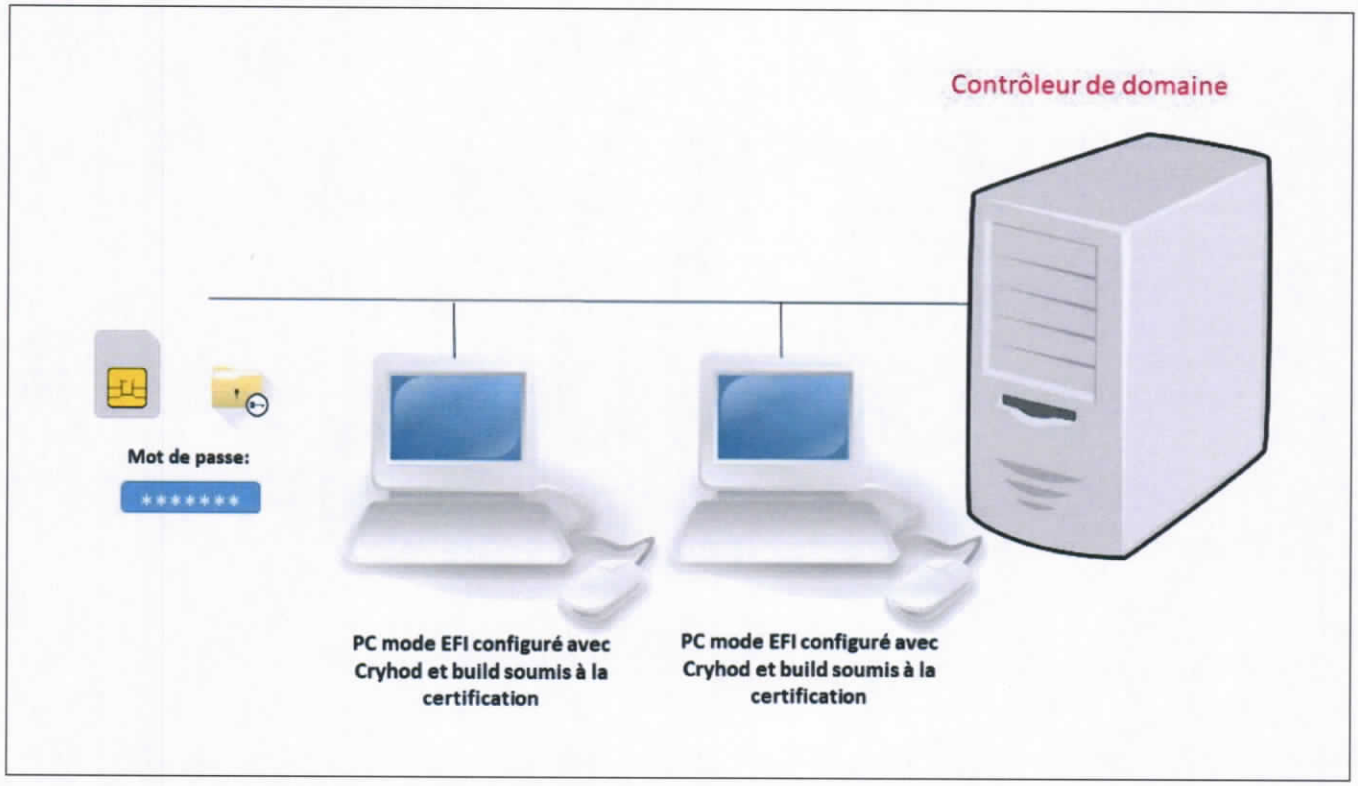

Figure 1. Cas d'usage classique du produit

Présentation générale

Le produit évalué est « CRYHOD » en version Q.2021.2 fournie par l'entreprise PRIM'X TECHNOLOGIES sous *WINDOWS 10* (64 Bits).

Le produit Cryhod est composé de 4 composants principaux :

- le pré-boot BIOS en charge de piloter la phase d'amorçage du poste de travail en gérant la phase d'authentification de l'utilisateur ainsi que quelques fonctions de base (langue, gestion par l'utilisateur du mode SSO, etc.) lorsque le mode BIOS ne nécessite pas le support des périphériques USB pour entrer la clé d'accès (clé d'accès de type mot de passe par exemple) ; Ce mode n'est pas dans le périmètre de la qualification.
- un système Linux propriétaire (construit à partir du noyau Linux 3.7.3) qui est chargé par le pré-boot BIOS de gérer la phase d'authentification de l'utilisateur lorsque le mode BIOS nécessite le support des périphériques USB pour entrer la clé d'accès (utilisation d'une carte à puce par exemple) ;
  Ce mode n'est pas dans le périmètre de la qualification.
- le pré-boot EFI qui effectue les mêmes fonctions que les 2 composants du mode BIOS décrits précédemment ;

- les drivers et services sous Windows assurant le fonctionnement du produit dans l'environnement de travail de l'utilisateur (chiffrement, déchiffrement et transchiffrement du poste, gestion des accès, audit, etc.).

  Les deux derniers composants font partie du périmètre de la qualification.

Les principaux services de sécurité fournis par le produit sont :

- la protection en confidentialité des données stockées sur les mémoires de masse ;
- la protection de l'accès aux données par authentification de l'utilisateur ;
- l'authentification unique (Single Sign-On, SSO) évitant à l'utilisateur de saisir plusieurs fois ses secrets ;
- la journalisation des évènements ;
- le recouvrement des partitions chiffrées faisant intervenir un tiers, appelé l'assistance, qui fournit soit des mots de passe (« laissez-passer temporaire » (One-Time Access, OTA) ou « mot de passe de secours personnel »), soit un code de secours et une clé USB, contenant un fichier de secours.

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 Cryhod en version Q.2021.2 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 :

- sensibiliser l'utilisateur au fait qu'il ne doit pas laisser son PC sans surveillance une fois que le système d'exploitation a été lancé ;
- lorsque la TOE est installée sur un poste, protéger la partition système par la TOE ;
- désactiver l'utilisation des périphériques DMA dans les paramètres de configuration du BIOS de la station de travail ;
- désactiver la fonctionnalité de production d'une image mémoire en cas de défaillance du système si elle n'est pas nécessaire ;
- générer, conformément aux règles et recommandations de l'ANSSI, les clés RSA générées à l'extérieur du produit puis embarquées dans des fichiers de clés ou des objets physiques (pour être utilisées en tant que clés d'accès) ;
- configurer les accès obligatoires et l'accès de recouvrement de l'administrateur (politique P131) ;
- fixer le seuil d'acceptation des mots de passe à 100% (politique P710) et leur longueur à 12 caractères au minimum (politique P712) ;
- utiliser la politique P258 avec sa valeur par défaut soit « Imposer le transchiffrement de la partition » ;
- désactiver la politique P382 qui fait réaliser les calculs AES par le processeur plutôt que par le logiciel fourni par Prim'X ;
- utiliser la version 2.2 de RSA PKCS#1 avec SHA-256 (politique P383) ;
- configurer la politique P386 avec le mécanisme de signature « PKCS#1 v2.2 PSS » ;
- configurer la politique P387 avec le mécanisme de dérivation de mot de passe « SHA256-PBKDF2 » ou « SHA512-PBKDF2 » ;
- configurer la politique P885 à « Non installé » (valeur par défaut) pour ne pas autoriser l'installation du module de démarrage automatique ;
- configurer à « oui » la politique P303 afin d'activer les événements pour toutes les opérations d'administration ;
- configurer la politique P339 à « 0 » pour permettre la collecte d'information pour le support technique ;
- renseigner le mot NONE dans le nom de la valeur de la politique P137 ;
- pour le mode alternatif, configurer la politique P070 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 Projet : CRYHOD2021, référence OPPIDA/CESTI/CC/CRYHOD2021/RTE, version 2.0, 21 mai 2022.
[ANALYSE_CRYPTO]	Rapport d'analyse des mécanismes cryptographiques CRYHOD2021, référence OPPIDA/CESTI/CRYHOD2021/CRYPTO/3.0, version 3.0, 24 mai 2022
[SITE]	Rapport de visite sur site, référence OPPIDA/CESTI/CC/CRYHOD2021/ALC/Rapport audit sur site/1.0, 20 juillet 2021

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

[PP-2008/04]	Profil de Protection Application de chiffrement de données à la volée sur mémoire de masse, version 1.4 d'août 2008. Certifié par l'ANSSI sous la référence DCSSI-PP 2008/04.
[CERTIF]	Rapport de certification, référence ANSSI-CC-2022/35, 27 juin 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]	Cryhod Q.2021 Guide d'installation, référence PX20A1406r1, version 1.1.
[GUIDE_ADMIN]	Mise en œuvre de la signature des politiques, référence PX13C133r4r2, version 1.4
[GUIDE_UTIL]	Cryhod Q.2021 Guide d'utilisation, référence PX20A1404r3, version 1.3 Cryhod Q.2021 Guide de démarrage rapide, référence PX20A1405r2, version 1.2.
[CDS]	Cible de sécurité de référence pour l'évaluation : - Cryhod version Q.2021.2 Cible de sécurité CC niveau EAL3+, référence PX2051294r6, version 1.6, mai 2022.

[CONF]	Liste de configuration du produit : - Cryhod Q.2021 Liste de configuration, référence PX2121442, version 1.2

Diffusion interne (par messagerie)

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