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

02 NOV. 2022

Paris, le
N°2344 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU STANDARD

CRYHOD version Q.2020.3

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 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.2020.3 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.

Emmanuel NAEGELEN
Directeur général adjoint 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.2020.3 fournie par l'entreprise PRIM'X TECHNOLOGIES sous *WINDOWS 10* (64 Bits).

Cette qualification couvre l'amorçage en mode BIOS et EFI.

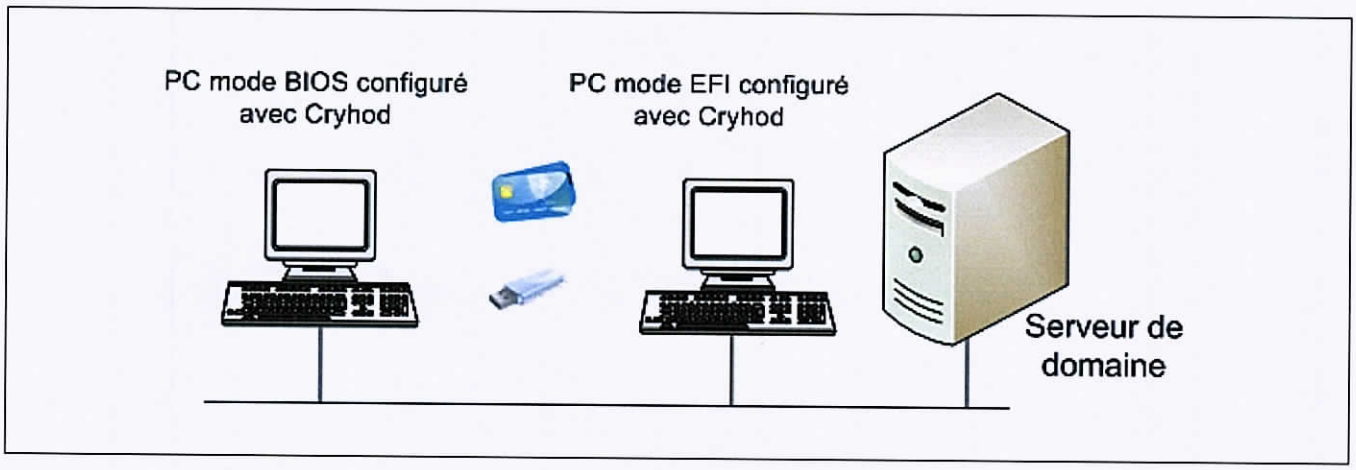

Figure 1. Cas d'usage classique du produit

Présentation générale

Le produit évalué est « CRYHOD » en version Q.2020.3 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 l'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) ;
- un système LINUX spécifique (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) ;
- le pré-*boot* EFI qui effectue les mêmes fonctions que les 2 composants du mode BIOS ;
- Les *drivers* et services sous WINDOWS qui assurent le fonctionnement du produit dans l'environnement de travail de l'utilisateur (chiffrement, déchiffrement et transchiffrement du poste, gestion des accès, audit, etc.).

Les principaux services de sécurité fournis par le produit sont :

- la protection en confidentialité et intégrité 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 aux chapitres 2.3 et 3.2 du rapport de certification [CERTIF] du produit Cryhod en version 3.0 Build 570 (la version qualifiée antérieurement) 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 :

- l'algorithme de HASH utilisé doit être SHA-256 (politique 292) ;
- l'usage du jeu d'instruction AES-NI ne doit pas être autorisé (politique 382) ;
- le mode de chiffrement RSA doit être PKCS#11 v2.2 avec utilisation de SHA 256 (politique 383) ;
- utiliser le générateur aléatoire Hash_DRBG/SHA512 du NIST défini par défaut (politique 385) ;
- la durée de validité des mots de passe doit être limitée à 90 jours (politique 702) ;
- le seuil d'acceptation des mots de passe doit être de 100% (politique 710) ;
- la longueur des mots de passe doit être à douze au minimum (politique 712) ;
- lorsque la TOE est installée sur un poste, la partition système doit être protégée par cette dernière ;
- la fonctionnalité de production d'une image mémoire doit être désactivée en cas de défaillance du système si elle n'est pas nécessaire ;
- l'utilisateur doit être sensibilisé au fait qu'il ne doit pas laisser son PC sans surveillance une fois que le système d'exploitation a été lancé.

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
[LPM]	Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale. Disponible sur https://www.legifrance.fr
[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]	Istruction 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 de tests - référence : OPPIDA/CESTI/CC/CRYHOD/TESTS/1.0 - version : 1.0 - en date du : 01/12/2020
[ANALYSE_CRYPTO]	Rapport d'analyse des mécanismes cryptographiques - référence : OPPIDA/CESTI/CRYHOD/CRYPTO/3.0 - version : 3.0 - en date du : 27/07/2020
[SITE]	Rapport de visite du site - référence : OPPIDA/CESTI/CC/CRYHOD/ALC/Rapport audit sur site/1.0 - version : 1.0 - en date du : 07/09/2020

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-2018/20 en date du 1er juin 2018.

[CRYPTO]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques,_annexée au Référentiel général de sécurité (RGS_B1), disponible sur www.ssi.gouv.fr. - version : 3.0 - en date du : 21 février 2014

Guides d'utilisation et documentations techniques de l'industriel

[GUIDE_INSTALL]	Guide d'installation CRYHOD et CRYHOD TO GO - référence : PX1991141r2 ; - version : Q.2020 révision 2
[GUIDE_ADMIN]	Guide d'administration – Mise en œuvre de la signature des politiques - Référence : PX13C133r2 - version : Q.2020 révision 2
[GUIDE_UTIL]	Guide d'utilisation CRYHOD et CRYHOD TO GO - référence : PX1991139r2 ; - version : Q.2020 révision 2
[CDS]	Cible de sécurité, Cible de Sécurité CRYHOD Critères Communs niveau EAL3+ - référence : PX1951078r3 - version : 1.3 - en date du : septembre 2020
[IAR]	Correction à PBKDF2 dans les versions Q.2020 – Analyse d'impact - référence : PX2251595 - date : 07/09/2022

Diffusion interne (par messagerie)

ANSSI DIR – SDE – PSS – DAT – Chrono informatique.