PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2022/35

Cryhod (Version Q2021.2)

Paris, le 27 juin 2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CC-2022/35**
Nom du produit **Cryhod**
Référence/version du produit **Version Q2021.2**
Conformité à un profil de protection **Profil de Protection Application de chiffrement de données à la volée sur mémoire de masse, version 1.4** certifié PP-2008/04 le 1 octobre 2008
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL 3 augmenté** ALC_FLR.3, AVA_VAN.3
Développeur **PRIM'X TECHNOLOGIES** Immeuble SKY56 18 rue du Général Mouton-Duvernet 69003 Lyon, France
Commanditaire **PRIM'X TECHNOLOGIES** Immeuble SKY56 18 rue du Général Mouton-Duvernet 69003 Lyon, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Accords de reconnaissance applicables **CCRA** Ce certificat est reconnu au niveau EAL2 augmenté de FLR.3. **SOG-IS** Ce certificat est reconnu au niveau EAL3 augmenté de FLR.3.

PREFACE

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Cryhod, Version Q2021.2 » développé par PRIM'X TECHNOLOGIES.

L'évaluation du produit Cryhod se limite au pré-boot EFI et aux drivers et services sous Windows (voir section 1.2.3).

Le produit Cryhod, installé sur un équipement de type PC, a en charge de protéger en confidentialité les informations stockées sur un ou plusieurs disques durs ainsi que de réaliser l'authentification de l'utilisateur avant l'amorçage de l'équipement sur lequel il est installé.

1.2 Description du produit

1.2.1 *Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme (conformité démontrable) au profil de protection [PP-2008/04].

1.2.2 *Services de sécurité*

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.

1.2.3 *Architecture*

Le produit Cryhod est constitué de quatre 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 composant n'est pas dans le périmètre de la TOE ;
- un Linux propriétaire (construit à partir du noyau Linux 3.7.3) qui est chargé par le pré-boot BIOS pour 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 composant n'est pas dans le périmètre de la TOE ;

- 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 TOE.

1.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments suivants :
- dans le coin supérieur droit de la fenêtre de pré-boot (lorsque les partitions sont chiffrées) ;
- à travers le centre de chiffrement, en cliquant sur l'icône Cryhod dans le coin supérieur gauche puis en choisissant le menu « A propos de Cryhod … ».

1.2.5 *Cycle de vie*

Le cycle de vie du produit est le suivant :
- le développement et la livraison du produit sont réalisés par PRIM'X TECHNOLOGIES ;
- l'installation, l'administration et l'utilisation du produit correspondent au déploiement du produit par le client.

Le produit a été développé sur le site suivant :

PRIM'X TECHNOLOGIES

Immeuble Sky56

18 Rue du Général Mouton-Duvernet,

69003 Lyon

Pour l'évaluation, l'évaluateur a considéré les utilisateurs suivants :
- l'administrateur du produit en charge de gérer les accès ;
- l'utilisateur dont certaines données sont à protéger en confidentialité sur le ou les disques durs de sa machine.

1.2.6 *Configuration évaluée*

Le certificat porte sur deux composants du produit Cryhod, dans la version Q2021.2 (voir section 1.2.3). L'évaluation couvre l'amorçage en mode EFI et le mode SSO.

Les éléments suivants ne sont pas couverts par l'évaluation :
- les systèmes d'exploitation Windows ;
- les porte-clés matériels utilisés ;
- l'outil de politique de sécurité utilisé GPOSign.exe ;
- la mise à jour système automatisée sans utilisateur ;
- le pré-chiffrement d'une machine par un opérateur externe.

L'évaluation a été réalisée à partir d'une plateforme de tests constituée de machines utilisant le système d'exploitation Windows, d'un contrôleur de domaine Windows Serveur 2019 et d'un lecteur de carte à puce.

Les machines utilisées sont :

- Windows 10 version 1809 LTSC 64 bits en modes d'authentification par *token* USB et fichier de clés ;
- Windows 10 version 20H2 64 bits en mode d'authentification par CSP et mot de passe.

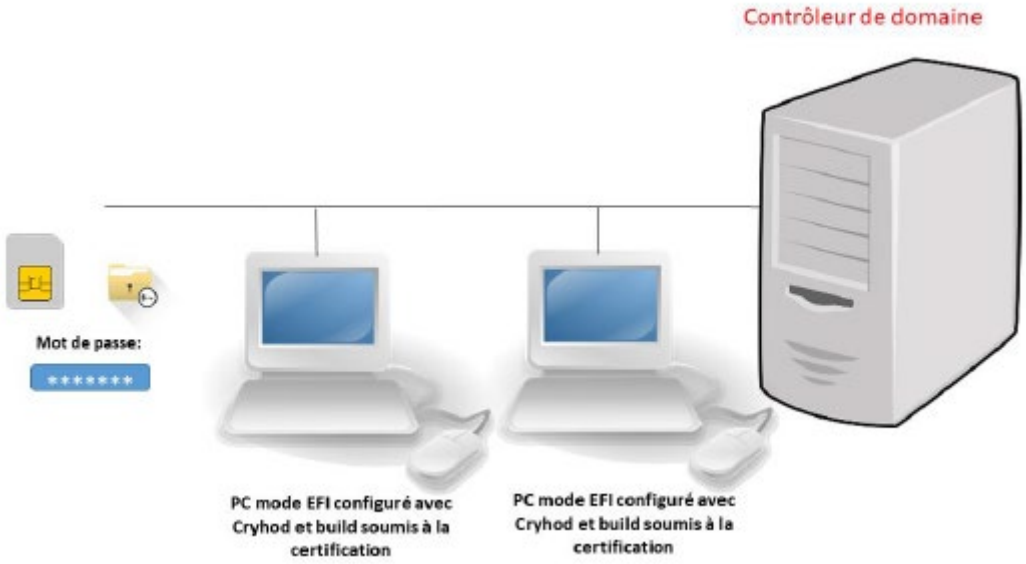

Figure 1 : Plateforme de tests

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 31 mai 2022, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [ANA_CRY].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.5 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

2.6 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'administrateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- 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.

2.7 Reconnaissance du certificat

2.7.1 *Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

2.7.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[2] , des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	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.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Évaluation Projet : CRYHOD2021, référence OPPIDA/CESTI/CC/CRYHOD2021/RTE, version 2.0, 21 mai 2022.
[ANA_CRY]	Rapport d'analyse des mécanismes cryptographiques CRYHOD2021, référence OPPIDA/CESTI/CRYHOD2021/CRYPTO/3.0, version 3.0, 24 mai 2022.
[CONF]	Liste de configuration du produit : - Cryhod Q.2021 Liste de configuration, référence PX2121442, version 1.2.
[GUIDES]	Guide d'installation du produit : - Cryhod Q.2021 Guide d'installation, référence PX20A1406r1, version 1.1. Mise en œuvre de la signature des politiques : - Mise en œuvre de la signature des politiques, référence PX13C133r4r2, version 1.4. Guide d'utilisation du produit : - Cryhod Q.2021 Guide d'utilisation, référence PX20A1404r3, version 1.3. Guide de démarrage rapide : - Cryhod Q.2021 Guide de démarrage rapide, référence PX20A1405r2, version 1.2.
[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.

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER-P-01]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 4.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *Part 3 : Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation : Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[ANSSI 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.