PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2018/20

Cryhod
Version 3.0 build 570

Paris, le 1er juin 2018

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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-2018/20

Nom du produit

Cryhod

Référence/version du produit

Version 3.0 build 570

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 1er octobre 2008

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 3 augmenté

ALC_FLR.3, AVA_VAN.3

Développeur

Prim'X Technologies

10 place Charles Beraudier

69428 Lyon Cedex 03

Commanditaire

Prim'X Technologies

10 place Charles Beraudier

69428 Lyon Cedex 03

Centre d'évaluation

Amossys

4 bis allée du bâtiment

35000 Rennes

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.

Préface

La certification

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 Premier ministre 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 matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « Cryhod, Version 3.0 build 570 » développé par *PRIM'X TECHNOLOGIES*.

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-CDISK].

1.2.2. Services de sécurité

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 passes (« 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) ;
- 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) ;
- le pré-boot EFI qui effectue les mêmes fonctions que les 2 composants du mode BIOS ;

- 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.).

Ces quatre composants font partie du périmètre d'évaluation 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, à savoir version 3.0 build 570, 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

10 place Charles Béraudier
69428 Lyon Cedex 03
France

Pour l'évaluation, l'évaluateur considérera 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 l'ensemble des composants du produit Cryhod, dans la Version 3.0 build 570. L'évaluation couvre l'amorçage en mode BIOS et en mode EFI ainsi que 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.

L'évaluation a été réalisée à partir d'une plateforme de tests constituée de machines utilisant le système d'exploitation *WINDOWS*, d'un serveur de domaine *WINDOWS* 2008 R2 et du lecteur de carte à puce *FEITIAN* de référence CAPD R301-U OEM[1].

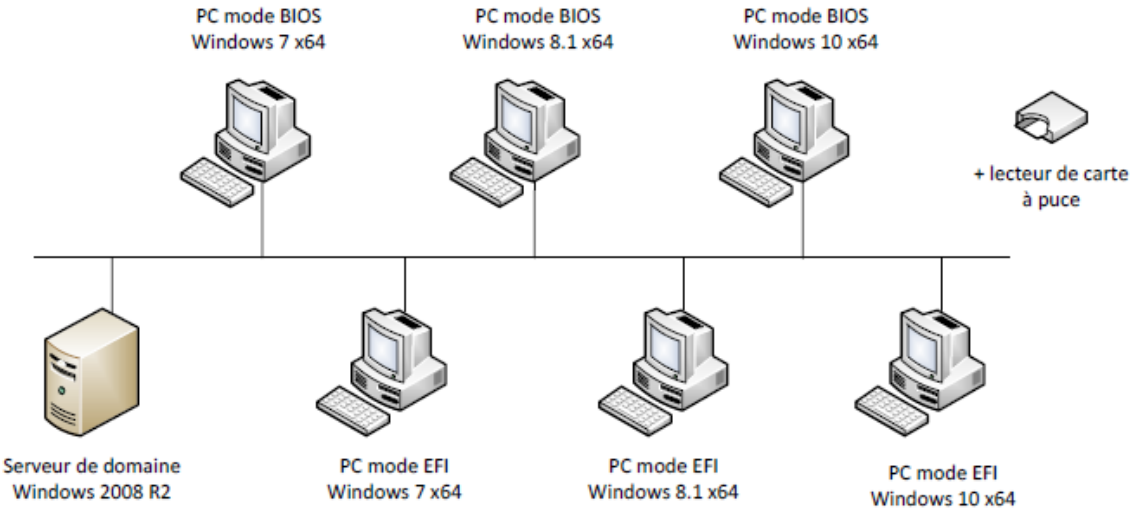

Figure 1 – Plateforme de test

Comme le montre la Figure 1, différentes versions du système d'exploitation *WINDOWS* ont été utilisées pendant l'évaluation :

- *WINDOWS* 10 64 bits en mode EFI ;
- *WINDOWS* 10 64 bits en mode BIOS ;
- *WINDOWS* 8.1 64 bits en mode EFI ;
- *WINDOWS* 8.1 64 bits en mode BIOS ;
- *WINDOWS* 7 64 bits en mode EFI ;
- *WINDOWS* 7 64 bits en mode BIOS.

[1] Le choix du lecteur de carte et des cartes utilisés pour identifier l'utilisateur n'a pas d'influence sur le produit.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [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 18 avril 2018, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

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

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie et la cotation des mécanismes cryptographiques ont été réalisées par le CESTI, les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY].
Ces résultats ont été pris 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 AVA_VAN.3 visé.

2.4. Analyse du générateur d'aléas

Ce générateur a fait l'objet d'une analyse par le CESTI.

Les résultats ont été pris 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 AVA_VAN.3 visé.

3. La certification

3.1. 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 « Cryhod, Version 3.0 build 570 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté des composants ALC_FLR.3 et AVA_VAN.3.

3.2. Restrictions d'usage

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

L'utilisateur 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], suivre les recommandations se trouvant dans les guides fournis [GUIDES] à savoir :

- utiliser l'algorithme de hachage SHA256 (politique P292) ;
- ne pas activer l'utilisation du jeu d'instruction AES-NI (politique P382) ;
- utiliser la version 2.2 de RSA PKCS#1 avec SHA256 (politique P383) ;
- utiliser le générateur aléatoire Hash_DRBG/SHA512 du NIST défini par défaut (politique P385) ;
- fixer la durée de validité des mots de passe inférieure à 90 jours (politique P702) ;
- fixer le seuil d'acceptation des mots de passe à « 100% » (politique P710) et leur longueur à 12 au minimum (politique P712) ;
- lorsque la TOE est installée sur un poste, la partition système doit être protégée par cette dernière ;
- désactiver la fonctionnalité de production d'une image mémoire en cas de défaillance du système si elle n'est pas nécessaire ;
- 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.

3.3. Reconnaissance du certificat

3.3.1. 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 :

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

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

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 3+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	**3**	Functional specification with complete summary
	ADV_IMP				1	1	2	2		
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	**2**	Architectural design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	**3**	Authorisation controls
	ALC_CMS	1	2	3	4	5	5	5	**3**	Implementation representation CM coverage
	ALC_DEL		1	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			1	1	1	2	2	**1**	Identification of security measures
	ALC_FLR								**3**	Systematic flaw remediation
	ALC_LCD			1	1	1	1	2	**1**	Developer defined life-cycle model
	ALC_TAT				1	2	3	3		
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	**2**	Analysis of coverage
	ATE_DPT			1	1	3	3	4	**1**	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	**1**	Functional testing
	ATE_IND	1	2	2	2	2	2	3	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Cible de Sécurité Cryhod Critères Communs niveau EAL3+, version 1 révision 8, datée de janvier 2018, *PRIM'X TECHNOLOGIES*.
[RTE]	Rapport technique d'évaluation : - Projet « cryhod3 » rapport technique d'évaluation, référence RTE-CRYHOD3-1.02, version 1.02 datée du 14 mai 2108, *AMOSSYS*.
[ANA-CRY]	Projet Cryhod3 Expertise des mécanismes cryptographiques, référence CRY-CRYHOD3-1.02, version 1.02 datée du 20 mars 2018, *AMOSSYS*.
[CONF]	Liste de configuration du produit : - Cryhod version 3.0 - Liste de configuration, référence PX172731r3, 15 mai 2018, *PRIM'X TECHNOLOGIES*.
[GUIDES]	Guide d'installation du produit : - Guide d'installation Cryhod et Cryhod To Go, référence PX153500r12, version 3.0 révision 12, *PRIM'X TECHNOLOGIES*. Guide d'administration du produit : - Mise en œuvre de la signature des politiques, référence PX13C133r2, révision 2, *PRIM'X TECHNOLOGIES*. Guide d'utilisation du produit : - Guide d'utilisation Cryhod et Cryhod To Go, référence PX153501r17, version 3.0 révision 17, *PRIM'X TECHNOLOGIES*.
[PP-CDISK]	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 3. 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]	Procédure ANSSI-CC-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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; - Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; - Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[CC RA]	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.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.