



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-2011/20

Cryhod version 2.0 build 200

Paris, le 13 juillet 2011

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

Patrick Pailloux
[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 présumées 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.anssi@ssi.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

| | |
|---------------------------------------|--|
| Référence du rapport de certification | ANSSI-CC-2011/20 |
| Nom du produit | Cryhod |
| Référence/version du produit | Version 2.0 build 200 |
| Conformité à un profil de protection | DCSSI-PP-2008/04 [PP CDISK] Application de chiffrement de données à la volée sur mémoire de masse, version 1.4 |
| Critères d'évaluation et version | Critères Communs version 3.1 révision 3 |
| Niveau d'évaluation | EAL 3 augmenté ALC_FLR.3, AVA_VAN.3 |
| Développeur(s) | Prim'X Technologies 10 place Charles Béraudier, 69428 Lyon Cedex 03, France |
| Commanditaire | Prim'X Technologies 10 place Charles Béraudier, 69428 Lyon Cedex 03, France |
| Centre d'évaluation | Silicomp AQL 1 rue de la châtaigneraie, CS 51766, 35513 Cesson Sévigné Cedex, France Tél : +33 (0)2 99 12 50 00, mél : cesti@aql.fr |
| Accords de reconnaissance applicables | <div style="display: flex; justify-content: space-around; align-items: center;"><div style="text-align: center;">CCRA </div><div style="text-align: center;">SOG-IS </div></div> |

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 | 6 |
| 1.1. PRESENTATION DU PRODUIT | 6 |
| 1.2. DESCRIPTION DU PRODUIT | 6 |
| 1.2.1. <i>Identification du produit</i> | 6 |
| 1.2.2. <i>Services de sécurité</i> | 7 |
| 1.2.3. <i>Architecture</i> | 7 |
| 1.2.4. <i>Cycle de vie</i> | 8 |
| 1.2.5. <i>Configuration évaluée</i> | 8 |
| 2. L’EVALUATION | 9 |
| 2.1. REFERENTIELS D’EVALUATION..... | 9 |
| 2.2. TRAVAUX D’EVALUATION | 9 |
| 2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI | 9 |
| 2.4. ANALYSE DU GENERATEUR D’ALEAS..... | 9 |
| 3. LA CERTIFICATION | 10 |
| 3.1. CONCLUSION | 10 |
| 3.2. RESTRICTIONS D’USAGE..... | 10 |
| 3.3. RECONNAISSANCE DU CERTIFICAT | 11 |
| 3.3.1. <i>Reconnaissance européenne (SOG-IS)</i> | 11 |
| 3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i> | 12 |
| ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT..... | 13 |
| ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE | 14 |
| ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION | 15 |

1. Le produit

1.1. Présentation du produit

Le produit évalué est le logiciel « Cryhod version 2.0 build 200 » développé par la société Prim'X Technologies.

Ce produit est destiné à être utilisé pour assurer la confidentialité de fichiers manipulés par des utilisateurs sur des ordinateurs portables ou des postes de travail isolés ou reliés à un réseau d'entreprise. Il permet de chiffrer des fichiers, sans modifier leurs caractéristiques (emplacement, nom, date, taille). Ce chiffrement s'effectue là où résident les fichiers (donc sans impact sur l'organisation des données de l'utilisateur) et « à la volée » (à la demande de l'utilisateur, sans manipulation particulière en dehors de la saisie des codes d'accès aux clés nécessaires pour le déchiffrement).

Cryhod est un produit de sécurité pour postes de travail opérant sous Windows XP SP3 (32 bits) et Windows Seven (64 bits). Il assure à la fois une authentification avant l'amorçage du poste et un chiffrement complet et transparent des données sur les disques durs internes ou additionnels. Il permet de réduire l'impact de la perte de données en cas de vol de l'ordinateur portable ou du poste de travail.

1.2. Description du produit

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 au profil de protection [PP CDISK]. Cette conformité est de type démontrable.

1.2.1. Identification du produit

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

Le numéro de la version certifiée du produit est intégré au nom des fichiers exécutables (téléchargeables sur le site de Prim'X Technologies pour un client disposant d'un login et d'un mot de passe de connexion) :

- version Windows 32 bits : « Setup Cryhod 2.0 x86 (b200).exe » ;
- version Windows 64 bits : « Setup Cryhod 2.0 x64 (b200).exe ».

Lorsque le produit est installé et activé, sa version peut être obtenue par l'utilisateur final par un clic droit avec la souris sur le haut de la fenêtre du centre de chiffrement puis par le choix de « A propos de Cryhod ... ».

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'implémentation d'opérations cryptographiques mises au service des autres fonctions de sécurité ;
- la journalisation des événements liés aux opérations réalisées par le produit ;
- la gestion des utilisateurs et de leurs droits d'accès aux partitions chiffrées ;
- le contrôle d'accès aux partitions chiffrées ;
- la gestion des opérations sur les partitions (chiffrement, déchiffrement, transchiffrement, affichage des informations sur les partitions) ;
- la gestion des données sensibles lors de l'arrêt du système.

1.2.3. Architecture

Le produit Cryhod est constitué de trois composants principaux :

- le résident BIOS (*Basic Input Output System* – Système élémentaire d'entrée-sortie) en charge de piloter la phase d'amorçage du poste de travail ;
- un Linux propriétaire (construit à partir du noyau Linux 2.6.27.46), chargé par le résident BIOS avant l'amorçage du poste, et gérant la phase d'authentification de l'utilisateur ;
- les drivers et services sous Windows qui assurent le fonctionnement du produit dans l'environnement de travail de l'utilisateur : chiffrement, déchiffrement, transchiffrement, gestion des accès, audit, ...

La figure ci-dessous schématise cette architecture :

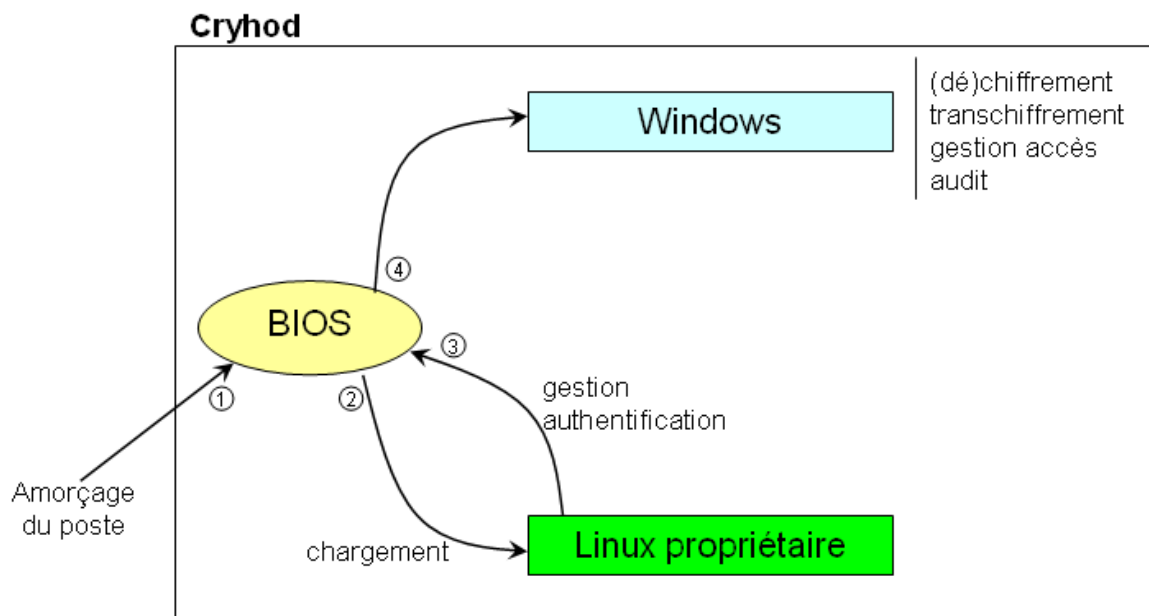


Figure 1 - Architecture de la cible d'évaluation

Les éléments suivants sont inclus dans le périmètre de l'évaluation :

- les trois composants décrits ci-dessus ;
- le dialogue PKCS#11 entre la cible d'évaluation et les porte-clés utilisateurs ;
- le dialogue PKCS#12 entre la cible d'évaluation et les fichiers de clés.

Les éléments suivants sont en dehors du périmètre de l'évaluation :

- les systèmes d'exploitation Windows, y compris :
 - o les drivers PC/SC ;
 - o le service de gestion des certificats ;
 - o le service de gestion des profils utilisateurs ;
- les porte-clés utilisés (comme les porte-clés de type Token USB ou les fichiers de clés) ;
- la génération des clés d'accès utilisateur (clés RSA dans des porte-clés ou mots de passe fournis par l'administrateur du produit).

1.2.4. 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 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 disque dur de sa machine ou sur des disques durs additionnels.

1.2.5. Configuration évaluée

La plate-forme de tests mise en œuvre par le CESTI correspond à la configuration suivante :

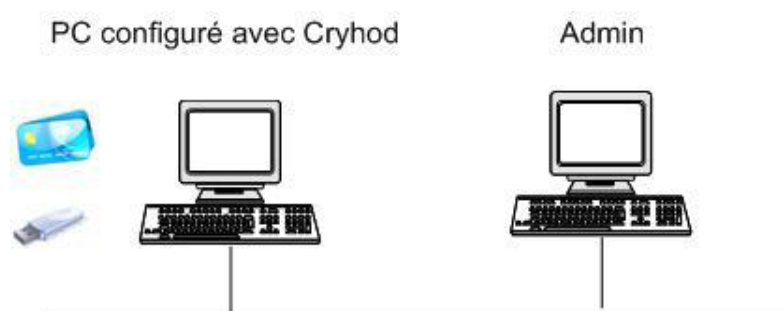


Figure 2 - Plate-forme de tests

Les tests ont été réalisés sur l'environnement d'exploitation suivant :

- un PC configuré avec Cryhod ayant pour système d'exploitation Microsoft Windows XP SP3 (architecture 32 bits) ou Windows Seven (architecture 64 bits) ;
- un contrôleur de domaine sous Microsoft Windows Server 2008 jouant le rôle d'administrateur d'un réseau local ;
- support de clé : token Aladdin.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

2.2. Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 29 juin 2011, 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

La cotation des mécanismes cryptographiques a été réalisée conformément aux référentiels techniques de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et conclut que les mécanismes analysés sont conformes aux exigences des référentiels techniques de l'ANSSI.

Dans le cadre du processus de qualification standard, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI [EXP-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 visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas et le retraitement d'aléas ont fait l'objet d'une analyse. Cette analyse conclut que le générateur d'aléas utilisé par le produit Cryhod et le retraitement d'aléas sont conformes au référentiel [REF-CRY].

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 2.0 build 200 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 3 augmenté.

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], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- OE.ENV_OPERATIONNEL.1 : lorsque l'utilisateur est authentifié, l'environnement opérationnel doit assurer la confidentialité de ses données, de ses clés d'accès et de ses données d'authentification. Les applications installées sur l'équipement ne doivent pas perturber le bon fonctionnement du produit. L'environnement doit fournir un système d'horodatage fiable permettant de dater précisément les événements enregistrés dans le journal ;
- OE.ENV_OPERATIONNEL.2 : l'utilisateur ne doit accéder à ses données chiffrées que lorsqu'il se trouve dans un environnement de confiance, c'est-à-dire lorsqu'il se trouve seul ou avec des personnes ayant le besoin d'en connaître ;
- OE.CONSERV_CLES : l'utilisateur doit conserver, de manière sûre, les clés d'accès qui lui ont été transmises et empêcher leur divulgation. L'administrateur du produit doit conserver, de manière sûre, les clés de recouvrement et empêcher leur divulgation ;
- OE.NON_REMANENCE_1 : les mémoires de travail utilisées par la machine qui exécute le produit ne doivent pas être rémanentes par construction ;
- OE.NON_REMANENCE_2 : l'environnement opérationnel du produit doit implémenter des mesures pour éviter la réutilisation de la rémanence des mémoires lors de l'arrêt de la machine dans laquelle s'exécute l'application de chiffrement de disque ;
- OE.SO_CONF et OE.ADM_ROOT_WINDOWS : les administrateurs du produit et les administrateurs Windows doivent être des personnes de confiance ;

- OE.FORMATION : les utilisateurs et les administrateurs du produit doivent être formés à son utilisation et être sensibilisés à la sécurité des systèmes d'information ;
- OE.CRYPTO_EXT : les administrateurs du produit doivent être sensibilisés à la problématique de la qualité des clés d'accès, ainsi qu'à celles de leurs supports ;
- OE.CERTIFICATS : l'administrateur du produit doit mettre en œuvre des procédures organisationnelles assurant la protection des certificats lors de leur remise aux utilisateurs. Il doit également, lors de la fourniture des clés d'accès possédant un certificat X509, vérifier la validité de ces certificats et leur adéquation avec l'usage qui en est fait par le produit.

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'accord¹, des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E3 Elémentaire et CC EAL4. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.

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 signataires¹, des certificats Critères Communs. La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :



¹ Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

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 | 1 | Security architecture description |
| | ADV_FSP | 1 | 2 | 3 | 4 | 5 | 5 | 6 | 3 | 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 | 2 | Architectural design |
| AGD Guides d'utilisation | AGD_OPE | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Operational user guidance |
| | AGD_PRE | 1 | 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 | 3 | Authorisation controls |
| | ALC_CMS | 1 | 2 | 3 | 4 | 5 | 5 | 5 | 3 | 3 | Implementation representation configuration management coverage |
| | ALC_DEL | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Delivery procedures |
| | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 | 1 | 1 | Identification of security measures |
| | ALC_FLR | | | | | | | | 3 | 3 | Systematic flaw remediation |
| | ALC_LCD | | | 1 | 1 | 1 | 1 | 2 | 1 | 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 | 1 | Conformance claims |
| | ASE_ECD | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Extended components definition |
| | ASE_INT | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | ST introduction |
| | ASE_OBJ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Security objectives |
| | ASE_REQ | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | Derived security requirements |
| | ASE_SPD | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | Security problem definition |
| | ASE_TSS | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | TOE summary specification |
| ATE Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 | 2 | 2 | Analysis of coverage |
| | ATE_DPT | | | 1 | 1 | 3 | 3 | 4 | 1 | 1 | Testing: basic design |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 1 | Functional testing |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | Independent testing: sample |
| AVA Estimation des vulnérabilités | AVA_VAN | 1 | 2 | 2 | 3 | 4 | 5 | 5 | 3 | 3 | Focused vulnerability analysis |

Annexe 2. Références documentaires du produit évalué

| | |
|------------|---|
| [ST] | Cible de sécurité de référence pour l'évaluation : <ul style="list-style-type: none">- Cible de Sécurité Cryhod, Critères Communs niveau EAL3+ Référence : PX109266, version 2 révision 5 d'Avril 2011 Prim'X Technologies |
| [RTE] | Rapport technique d'évaluation : <ul style="list-style-type: none">- Evaluation du produit de sécurité Cryhod – Rapport technique d'évaluation Référence : PRI007-ZEBRA4-RTE, version 3.01 du 29/06/2011 Silicomp-AQL |
| [PP CDISK] | Profil de protection – Application de chiffrement de données à la volée sur mémoire de masse, Référence : PP-CDISK-CCv3.1, version 1.4 d'Août 2008 <i>Certifié par l'ANSSI le 1^{er} octobre 2008 sous la référence DCSSI-PP-2008/04.</i> |
| [ANA-CRY] | Cotation des mécanismes cryptographiques – Qualification ZEBRA4, Référence : 451/SGDSN/ANSSI/ACE datée du 28 février 2011, ANSSI |
| [EXP-CRY] | Evaluation du produit de sécurité Cryhod – Analyse des mécanismes cryptographiques Référence : PRI007-ZEBRA4-AMC, version 1.01 du 29/06/2011 Silicomp-AQL |
| [CONF] | Liste de configuration Cryhod version 2.0 Build 200 Référence : PX113309, version 1 du 17/03/2011 Prim'X Technologies |
| [GUIDES] | Guide d'installation du produit : <ul style="list-style-type: none">- Guide d'installation Référence : PX113302, révision 2 Prim'X Technologies Guide d'utilisation du produit : <ul style="list-style-type: none">- Guide d'utilisation Référence : PX113301, révision 2 Prim'X Technologies |

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 CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI. |
| [CC] | Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003. |
| [CEM] | Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004. |
| [CC RA] | Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000. |
| [SOG-IS] | « Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee. |
| [REF-CRY] | Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr |
| [REF-KEY] | Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr |
| [REF-AUT] | Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr |