Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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-CSPN-2012/04

CRYPT2Protect
Version 8.04-03i

Paris, le 3 mai 2012

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2012/04**
Nom du produit **CRYPT2Protect**
Référence/version du produit **8.04-03i**
Catégorie de produit **Logiciel pour enceinte cryptographique**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **Bull SAS** **Rue Jean Jaures BP 68** **78340 Les Clayes sous Bois** **France**
Commanditaire **Bull SAS** **Rue Jean Jaures BP 68** **78340 Les Clayes sous Bois** **France**
Centre d'évaluation **Oppida** **4-6, avenue du Vieil Etang - Bât B** **78180 Montigny Le Bretonneux**

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 « CRYPT2Protect**,** version 8.04-03i **»** développé par Bull SAS.

CRYPT2Protect HR est une enceinte cryptographique autonome (*Hardware Security Module*, ci-après dénommé HSM) qui offre ses services cryptographiques à un serveur ou à un réseau complet via TCP/IP pour effectuer des opérations de cryptographie symétrique et asymétrique.

Il est composé d'une enceinte cryptographique sécurisée dans laquelle est embarqué le logiciel CRYPT2Protect, objet de la présente certification.

CRYPT2Protect fournit des services cryptographiques pour le chiffrement de données, l'intégrité de messages, l'authentification d'utilisateurs ou de données, la signature et le stockage sécurisé des clés et des informations de sécurité. Ces services peuvent être utilisés par des applications de gestion de titres électroniques sécurisées, des applications de type *eServices* ou des applications d'infrastructures de gestion de clés publiques (IGC).

1.2. Description du produit évalué

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

1.2.1. Catégorie du produit

☐ 1 - détection d'intrusions
☐ 2 - anti-virus, protection contre les codes malicieux
☐ 3 – firewall
☐ 4 - effacement de données
☐ 5 - administration et supervision de la sécurité
☐ 6 - identification, authentification et contrôle d'accès
☐ 7 - communication sécurisée
☐ 8 - messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 - matériel et logiciel embarqué
☒ **99 - autres : logiciel pour enceinte cryptographique**

1.2.2. Identification du produit

La version certifiée du produit est identifiable dans la première ligne en haut du panneau d'administration WEB du HSM.

Les options autorisées et activées sont disponibles sur le panneau d'administration, sur la page « Administration ».
L'empreinte SHA256 du *firmware* utilisé lors de l'évaluation est la suivante :

465caf51 d0e122ab 4ae328c6 98df07f1 254a5b10 a1db9780 5e46c9d2 804d0758

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- les fonctions de cryptographie génériques (mécanismes PKCS#11) ;
- les fonctions de cryptographie dédiées à des cas d'utilisation particuliers (carte *eServices*) ;
- les fonctions de gestion de clés statiques.

1.2.4. Configuration évaluée

La configuration évaluée est celle par défaut.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents constituant le référentiel se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 2 « Argumentaire (description) du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 4 « Description des biens sensibles que le produit doit protéger »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 4.2 « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 4.3 « Description des fonctions de sécurité du produit »).

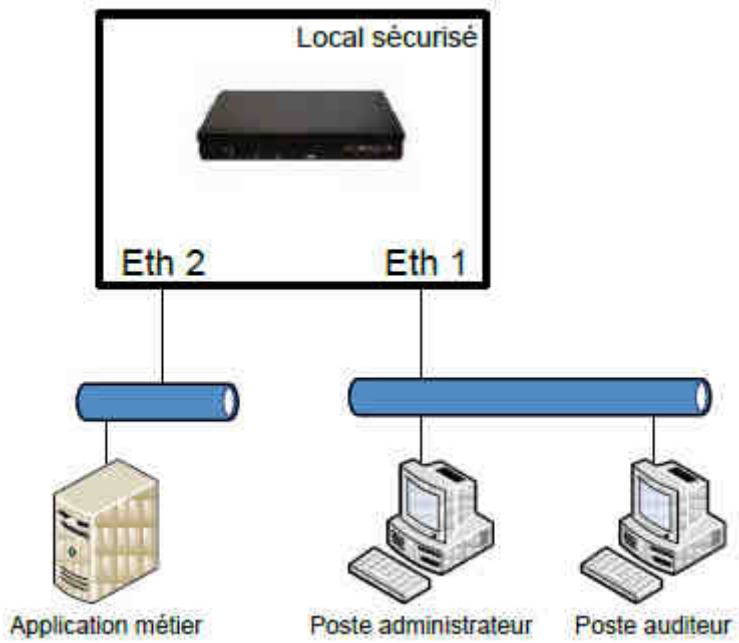
2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 2.6 « Description des utilisateurs typiques »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

La plate-forme de test utilisée par l'évaluateur était constituée de deux instances de machines virtuelles VMWare reliées à la première interface Ethernet du produit et d'un poste « application métier » relié à la seconde interface Ethernet du produit.



L'outil de gestion des clés cryptographiques (le Centre de Gestion et de Distribution des Clés nouvelle génération, ci-après dénommé CGDCng) est habituellement installé en dehors du réseau sur un poste connecté à un second HSM dédié à la génération des clés. Dans le cadre de cette certification, l'évaluateur ne disposant que d'un HSM, le CGDCng était installé sur le poste administrateur.

2.3.2.2. Particularités de paramétrage de l'environnement

Le produit n'est dépendant d'aucun module logiciel.

Cependant, afin d'utiliser les services cryptographiques fournis par le produit, les bibliothèques d'interface PKCS#11 doivent être installées et configurées sur le poste « application métier ». L'API Cryptoki PKCS#11 fournie par le développeur est compatible avec les systèmes d'exploitation Windows ou Linux pour des architectures 32 ou 64 bits.

Le CGDCng doit être installé sur un poste disposant du système d'exploitation Windows XP et de l'environnement d'exécution java (*java runtime environment* – JRE) 1.6 de SUN.

2.3.2.3. Options d'installation retenues pour le produit

Le HSM hébergeant le module logiciel a été personnalisé avec deux fichiers d'options permettant d'offrir tous les services rentrant dans le périmètre d'évaluation. Le premier fichier d'options autorise les services suivants :

- BASIC ;
- PKCS11 ;
- MULTI_C ;

- FULL_IP ;
- ENCRYPT ;
- SAM ;
- WATCHDOG.

Le second fichier d'options autorise les services suivants :

- BASIC ;
- PKCS11 ;
- CGDC ;
- WATCHDOG.

2.3.2.4. Description de l'installation et des non-conformités éventuelles

Le produit est livré avec le *firmware* de transport chargé dans les zones de boot. Il est configuré par défaut avec une configuration TCP/IP et avec une clé de vérification de signature des logiciels et des fichiers d'options.

Le produit est opérationnel après le chargement du logiciel embarqué (*firmware* de production) et d'un fichier d'options par un administrateur. Ce dernier doit ensuite adapter la configuration réseau du produit à sa plateforme.

La cérémonie de mise à la clé a été réalisée à partir de l'outil CGDCng (v4.7.0). Les principales opérations effectuées sur cet outil sont :

- la création et l'introduction de la clé maitre de stockage sur le CGDCng ;
- la création et l'introduction de la clé maitre du HSM cible ;
- la création et le tirage d'une clé de stockage vouée au transport de clés ;
- la création et le tirage de clés de service ;
- la création d'un groupe et d'un équipement sur le HSM ;
- l'affectation des clés précédemment créées.

2.3.2.5. Durée de l'installation

L'installation du produit a duré environ une heure.

2.3.2.6. Notes et remarques diverses

L'installation est simple et ne requiert aucune connaissance particulière de la part de l'administrateur.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et aucune non-conformité n'a été relevée. Elle est destinée aux administrateurs système et peut s'accompagner d'une formation de plusieurs jours afin de leur permettre d'appréhender les capacités du système ainsi que ses principes d'utilisation et d'administration.

2.3.4. Revue du code source (facultative)

Les évaluateurs n'ont pas eu accès au code source.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Authentification des administrateurs	**Réussite**
Authentification des opérateurs	**Réussite**
Authentification des applications clientes	**Réussite**
Personnalisation du boitier	**Réussite**
Protection des jetons	**Réussite**
Signature des logiciels embarqués et chargement par un administrateur authentifié	**Réussite**
Signature des fichiers d'option et chargement par un administrateur authentifié	**Réussite**
Typage des clés	**Réussite**
Contrôle d'accès aux clés	**Réussite**
Contrôle de l'usage des clés	**Réussite**
Gestion des clés sous contrôle mutuel sur le CGDCng avec des privilèges	**Réussite**
Authentification de l'opérateur du CGDCng	**Réussite**
Définition des listes d'accès au travers de l'administration	**Réussite**

2.3.6. Fonctionnalités non testées

Sans objet.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

Sans objet.

2.3.8. Avis d'expert sur le produit

Les guides fournis par le développeur sont clairs, suffisamment détaillés et cohérents avec le produit tel qu'il est décrit dans la cible de sécurité [CDS].
Le produit est fonctionnellement conforme à la cible de sécurité [CDS]. Son installation, tout comme son utilisation, est simple et efficace.
Toutes les fonctions de sécurité identifiées dans la cible de sécurité ont pu être testées par l'évaluateur et aucune non-conformité n'a été relevée.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Authentification
Gestion des sessions
Gestion des autorisations d'accès
Validation des données d'entrée
Personnalisation du boitier
Protection des jetons de clés
Signature des logiciels embarqués
Signature du fichier d'options
Typage des clés
Contrôle d'accès aux clés
Contrôle de l'usage des clés
Gestion des clés sous contrôle mutuel

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Ces fonctions s'appuient sur des mécanismes cryptographiques détaillés dans le §2.4. Leur implémentation est jugée robuste par l'évaluateur.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit.

2.3.10.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Aucune.

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès aux développeurs du produit. Au cours des échanges techniques qui ont eu lieu, les développeurs ont fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement aux questions posées.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Néant.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Les postes en liaison avec le produit doivent héberger un système d'exploitation à jour concernant les correctifs de sécurité et correctement configuré (mise en place d'une politique de gestion de supports, authentification robuste), administré et supervisé. Ils doivent être par ailleurs au minimum, à défaut de l'emploi de technologies plus robustes, protégés par un produit anti-virus (avec bases d'informations à jour et proposant des fonctions de détection des infections informatiques furtives - anti-*spyware*, anti-*rootkit*, etc.) et un pare-feu correctement configuré.
Des interfaces réseau physiques différentes doivent être utilisées pour les interfaces métiers et les interfaces d'administration.

L'accès physique à la cible de l'évaluation doit être restreint à des personnes de confiance.

L'analyse selon le référentiel cryptographique de l'ANSSI [REF-CRY] n'a porté que sur certains mécanismes cryptographiques (cf. §2.4). L'utilisation d'autres mécanismes (algorithmes, modes opératoires,…) n'entre pas dans le cadre de cette certification.

Les recommandations présentes dans [GUIDES] doivent être appliquées.

2.3.12.3. Avis d'expert sur la facilité d'emploi

Le produit est destiné à être utilisé par des administrateurs de sécurité de confiance qui ont été formés à l'utilisation du produit. Dans ce cadre, il n'a pas été identifié de cas où le produit serait configuré ou utilisé de façon non sûre mais qu'un utilisateur pourrait raisonnablement croire sûre.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

La liste des mécanismes cryptographiques analysés est celle fournie par la cible de sécurité [CDS] et les spécifications cryptographiques [SPEC_CRY].

La résistance de ces mécanismes été analysée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et concluent que, si les recommandations présentes dans [GUIDES] sont appliquées, les mécanismes analysés atteignent le niveau standard défini dans [REF-CRY].

2.5. Analyse du générateur d'aléas

Le produit évalué offre plusieurs générateurs d'aléas qui peuvent être utilisés par le logiciel embarqué.

Ces générateurs ont fait l'objet d'une analyse qui a permis de mettre en évidence que, conformément aux recommandations indiquées dans [GUIDES], le générateur d'aléas décimaux ne doit pas être utilisé pour la génération de clés ou de vecteurs d'initialisation.

L'analyse du générateur d'aléas binaires n'a pas permis de mettre en évidence de biais statistique bloquant pour un usage direct des sorties des générateurs. Ceci ne permet pas d'affirmer que les données générées soient réellement aléatoires mais assure que le générateur ne souffre pas de défauts majeurs de conception.

Le générateur d'aléas du module cryptographique CRYPT2Protect HR a par ailleurs été certifié au niveau 3 selon la norme [FIPS 140-2].

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.

Ce certificat atteste que le logiciel « CRYPT2Protect, version 8.04-03i » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

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 spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport et dans l'ensemble des guides [GUIDES].

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN - CRYPT2Protect ;* Référence : *C2P/LP59035/FR* ; Date : *30/03/2012*
[RTE]	*Rapport Technique d'Evaluation (RTE) - CSPN CRYPT2Protect ;* Référence : *OPPIDA/DOC/2011/BFM/908* ; Date : *25/11/2011*
[SPEC-CRY]	*Principes cryptographiques C2P ;* Référence : *C2P/LP51102/FR* ; Date : *13/01/2012*
[ANA-CRY]	*Rapport d'évaluation des mécanismes cryptographiques - CRYPT2Protect HR ;* Référence : *OPPIDA/DOC/2011/BFM/831/1.0* ; Date : *25/11/2011*
[GUIDES]	Guide de prise en main : *Manuel utilisateur CHR ;* Référence : *CHR/LP54002/FR* ; Date : *26/11/2008* Guides d'utilisation détaillés: *Interface Commandes C2P - I - Basic ;* Référence : *C2P_LP51003A_FR* ; Date : *13/01/2012* *Interface Commandes C2P - I - Gestion des clés ;* Référence : *C2P_LP51003D_FR* ; Date : *13/01/2012* *Manuel de référence du Centre de gestion de clés ;* Référence : *KMC/LP54002/FR* ; Date : *19/09/2011*

Annexe 2. Références 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.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr
[FIPS 140-2]	Federal Information Processing Standards Publication 140-2 : Security requirements for cryptographic modules National Institute of Standard and Technology (NIST)