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-2014/10

VeriCert, version 2.1.2

Paris, le 23 décembre 2014

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

Guillaume POUPARD
[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-2014/10**
Nom du produit **VeriCert, version 2.1.2**
Référence/version du produit **Version 2.1.2**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **BULL** **210 Boulevard André Bahonneau** **49800 Trelazé**
Commanditaire **BULL** **210 Boulevard André Bahonneau** **49800 Trelazé**
Centre d'évaluation **OPPIDA** **6 avenue du Vieil Etang** **Bâtiment B** **78180 Montigny-le-Bretonneux** **France**

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 un composant logiciel fourni sous la forme d'une « *appliance* virtuelle » chargé de vérifier la validité de certificats au format X.509 pour le compte d'applications clientes. La solution VeriCert fait office d'autorité de validation de certificats multi-PKI[1], et permet aux applications d'externaliser cette fonctionnalité. En outre, cette factorisation de la fonction de vérification permet d'assurer l'homogénéité de la politique de validation et de faciliter l'audit des opérations de vérification.

Le produit est constitué de deux modules logiciels : VeriCert *Responder* et VeriCert *Collector*.

Le module VeriCert *Responder* :

- détermine à une date donnée la validité d'un certificat conformément à une politique de validation spécifique ;
- donne l'état de validité de chacune des données utilisées pour déterminer la validité d'un certificat ; plus précisément, le module effectue les contrôles suivants :
  - reconstitution de la chaine de certification jusqu'à l'AC[2] racine de confiance ;
  - vérification de la date de validité de l'ensemble des certificats composant la chaîne ;
  - vérification de l'intégrité et de l'authenticité de l'ensemble des certificats de la chaîne ;
  - vérification de la non-révocation des certificats de la chaîne ;
  - vérification de la validité de la chaîne conformément à la politique de validation spécifiée ;
- interroge soit l'annuaire interne de VeriCert, soit des points de distribution de CRL[3] afin de trouver la ou les CRL nécessaires aux opérations de vérification ;
- dispose de fonctions d'administration permettant la gestion du contenu des magasins de certificats, la gestion des politiques de validation, son audit et son paramétrage, ainsi que la gestion du contenu des magasins de clés.

Le module VeriCert *Collector* :

- collecte les CRL émises par les différentes PKI, suivant les émetteurs déclarés par l'administrateur ;
- dispose de fonctions d'administration permettant :
  - la gestion les points de distribution des CRL (déclaration, consultation et suppression de points de distribution, fréquence de rapatriement, importation des certificats et vérification de l'intégrité et de l'authenticité des CRL) ;
  - la consultation des CRL présentes dans son annuaire ;

[1] *Public Key Infrastructure* ou Infrastructure de Gestion de Clés.
[2] Autorité de Certification.
[3] *Certificate Revocation List* ou liste de certificats révoqués.

- l'audit des actions effectuées (toutes les actions d'administration sont journalisées, de même que les opérations de rapatriement automatique lancées par le *Collector*).

Les demandes de validation auprès de VeriCert sont anonymes ; les applications clientes n'ont pas à s'identifier. Les requêtes des applications clientes correspondent aux services (administration exclue) fournis par le *Responder*. Ceux-ci peuvent être invoqués via les protocoles SOAP ou OCSP, au travers de canaux SSL ou TLS.

VeriCert est fourni sous la forme d'une machine virtuelle fonctionnant sous environnement VMWare ESXi (version 4.1 et supérieur) et embarquent une instance du système CentOS.

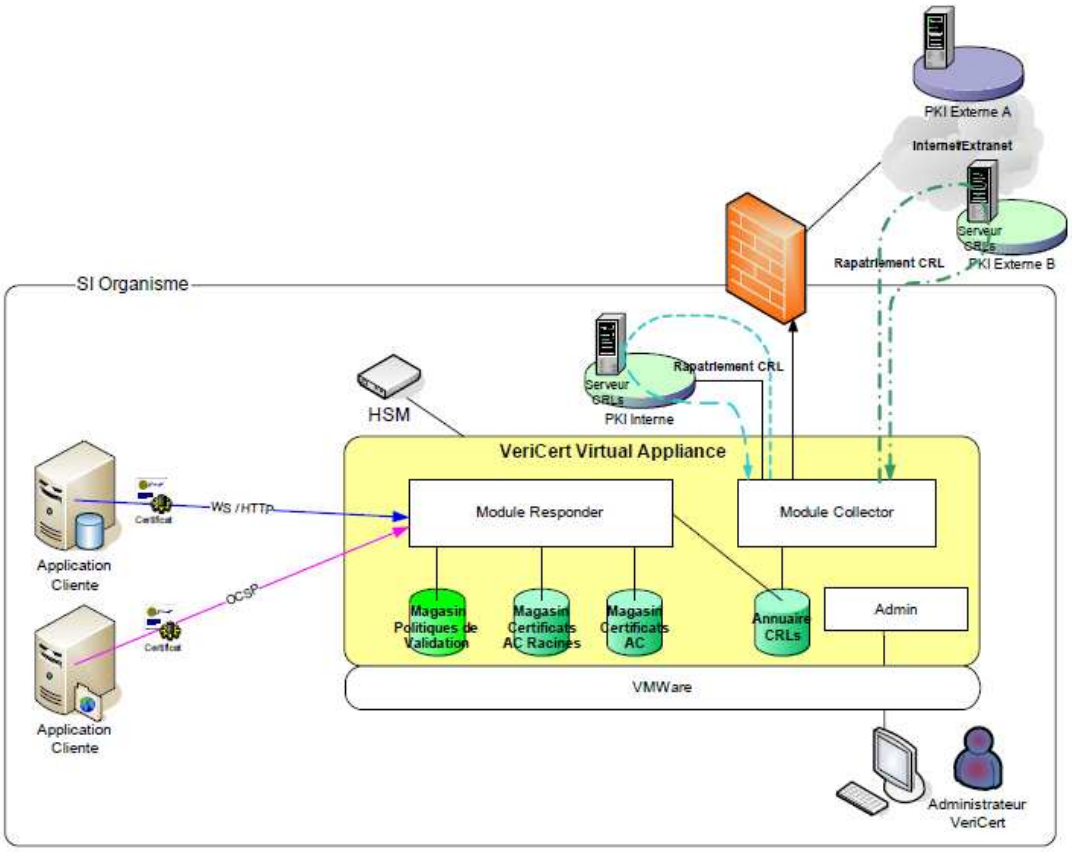

Figure 1 - schéma d'intégration du produit

1.2. Description du produit évalué

La cible de sécurité [CDS] 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 – pare-feu
☐ 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

1.2.2. Identification du produit

Nom du produit	VeriCert
Numéro de version analysée	2.1.2

1.2.3. Services de sécurité évalués

Les principaux services de sécurité fournis par le produit sont :

- l'authentification des administrateurs ;
- la protection en intégrité, authenticité et confidentialité des flux d'administration ;
- la protection en intégrité, authenticité et confidentialité des flux d'interrogation des applications clientes ;
- la signature des réponses VeriCert ;
- l'horodatage des réponses ;
- la protection contre le *SYN flooding* ;
- la vérification de l'intégrité et de l'authenticité des CRL ;
- le contrôle d'accès aux données contenues dans la base de données et dans l'annuaire interne de VeriCert ;
- la protection de l'intégrité et de l'authenticité des Politiques de validation stockées dans la base ;
- la journalisation des actions administrateurs ;
- la journalisation des demandes des applications clientes et des réponses faites.

1.2.4. Configuration évaluée

Le produit a été évalué dans sa configuration standard, les seuls paramétrages effectués par l'évaluateur concernant la configuration des interfaces réseau, le serveur NTP[1] et la connexion au HSM[2].

Le composant VeriCert, pour l'évaluation, était déployé dans un environnement comprenant :

- CentOS 6.5 ;
- Apache Tomcat 6.0.41 ;
- Apache Axis 1.4 ;
- JAVA 1.8.0_05 ;
- OpenSSL 1.0.1e-fips.

[1] *Network Time Protocol*.
[2] *Hardware Security Module* ou module matériel de sécurité.

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 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].

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 5 « 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 6 « description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 7 « description des fonctions de sécurité du produit »).

2.3.1.5. Utilisateurs typiques

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

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Pour les besoins de l'évaluation, le CESTI a mis en place une architecture jugée représentative du déploiement typique de la solution.

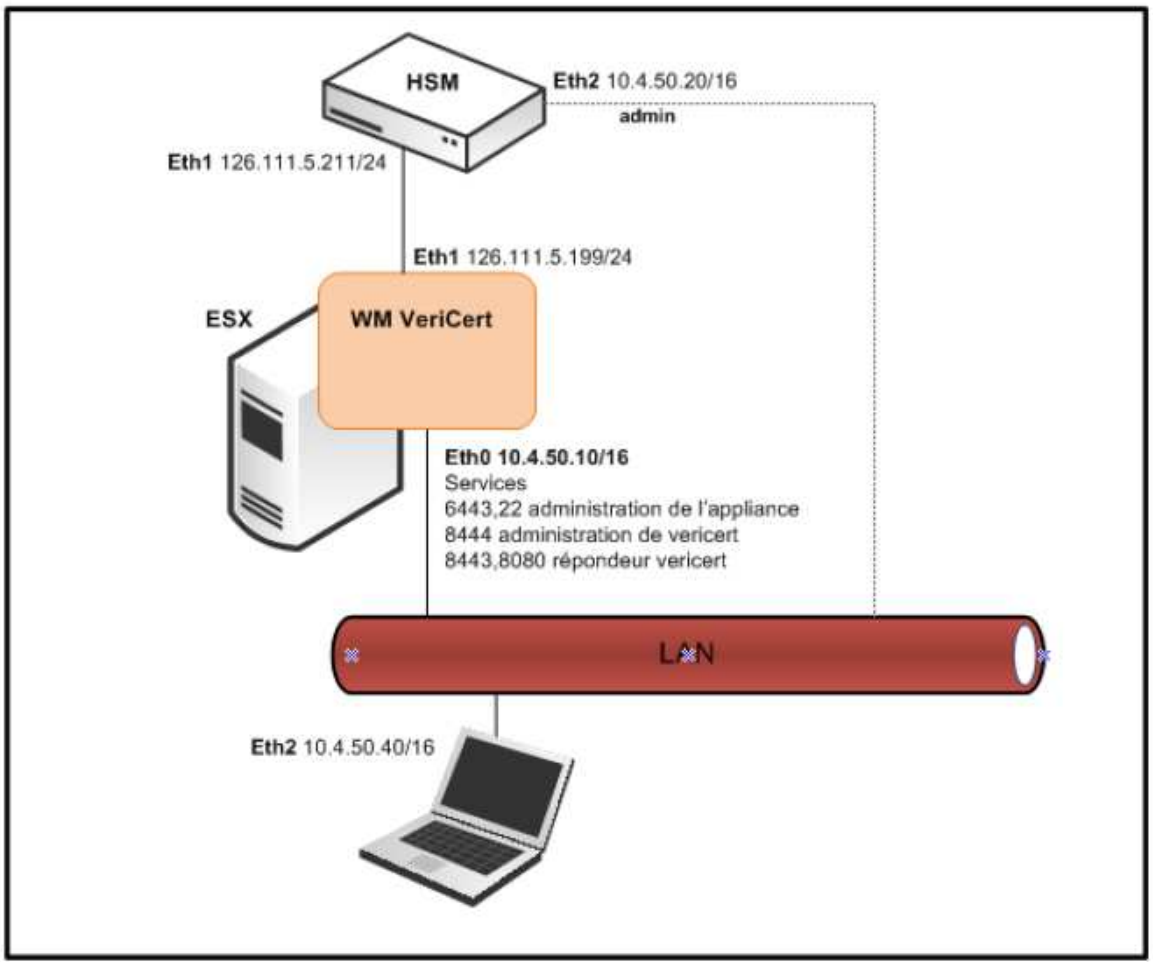

Figure 2 - schéma de la plateforme de test

2.3.2.2. Particularités de paramétrage de l'environnement

L'*appliance* virtuelle VeriCert doit être configurée pour utiliser les fonctions et services cryptographiques d'une *appliance* HSM. Pour les besoins de l'évaluation, un HSM Bull Crypt2Protect a été mis à disposition du CESTI.
Une source de temps de confiance, accessible en NTPv4, doit également être accessible par la TOE.

2.3.2.3. Options d'installation retenues pour le produit

Aucune option d'installation particulière n'a été utilisée.

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

Le produit ne dispose pas à proprement parler d'une méthodologie d'installation. La documentation concernant la configuration de l'*appliance* VeriCert avec le HSM n'est en outre pas complète.
Afin d'assurer la confidentialité des échanges, il faut configurer via l'application d'administration de l'*appliance* les connections SSL vers le *Responder*, sinon celui-ci n'est pas accessible. De plus il faut créer un nouvel administrateur pour l'*appliance* et VeriCert et leur

associer une nouvelle clé afin de ne pas se servir des administrateurs par défaut qui ont tous la même clé (comme spécifié par la documentation d'administration et d'installation).

2.3.2.5. Durée de l'installation

L'installation complète, telle qu'elle devrait être réalisée par un administrateur, est estimée par l'évaluateur à deux heures environ.

2.3.2.6. Notes et remarques diverses

Néant.

2.3.3. Analyse de la documentation

Les guides utilisateur sont nombreux et assez longs, mais relativement clairs. Ils permettent de se servir correctement du produit même si la recherche d'informations précises peut se montrer fastidieuse.
Les guides d'administration sont assez succincts. Ils ne sont pas très directifs et difficiles d'utilisation en cas de dysfonctionnement ou mauvaise configuration de l'*appliance*.

2.3.1. Fonctionnalités testées

Les fonctionnalités suivantes ont été soumises à des tests de conformité.

Fonctionnalité	Résultat
Authentification sécurisée des administrateurs	**CONFORME**
Protection en intégrité, authenticité et confidentialité des flux d'administration	**CONFORME**
Protection en intégrité, authenticité et confidentialité des flux d'interrogation des applications clientes	**CONFORME**
Signature des réponses VeriCert	**CONFORME**
Horodatage des réponses	**CONFORME**
Protection contre le *SYN flooding*	**CONFORME**
Vérification de l'intégrité et authenticité des CRL	**CONFORME**
Contrôle d'accès aux données contenues dans la base de données et dans l'annuaire interne de VeriCert	**CONFORME**
Protection de l'intégrité et de l'authenticité des Politiques de Validation stockées dans la base	**CONFORME**
Journalisation des actions administrateurs	**CONFORME**
Journalisation des demandes des applications clientes et des réponses faites	**CONFORME**

2.3.2. Fonctionnalités non testées

Néant.

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

Les fonctionnalités testées sont conformes à ce qui est décrit dans la cible de sécurité [CDS].

2.3.4. Avis d'expert sur le produit

Le produit est fonctionnellement conforme à sa cible de sécurité et son utilisation est simple. En revanche, les guides manquent de détails pour permettre l'intégration simple d'un HSM à la TOE via l'interface d'administration. Lors de la configuration du HSM dans cette dernière, l'interface graphique a généré une erreur obligeant l'évaluateur à entrer des commandes via SSH.

2.3.5. Analyse de la résistance des mécanismes et des fonctions

2.3.5.1. Liste des fonctions et des mécanismes testés

Les fonctionnalités suivantes ont été soumises à des tests de pénétration :

Fonctionnalité	Résultat
Authentification sécurisée des administrateurs	**Réussite**
Protection en intégrité, authenticité et confidentialité des flux d'administration	**Réussite**
Protection en intégrité, authenticité et confidentialité des flux d'interrogation des applications clientes	**Réussite**
Signature des réponses VeriCert	**Réussite**
Horodatage des réponses	**Réussite**
Protection contre le SYN flooding	**Réussite**
Vérification de l'intégrité et authenticité des CRL	**Réussite**
Contrôle d'accès aux données contenues dans la base de données et dans l'annuaire interne de VeriCert	**Réussite**
Protection de l'intégrité et de l'authenticité des Politiques de Validation stockées dans la base	**Réussite**
Journalisation des actions administrateurs	**Réussite**
Journalisation des demandes des applications clientes et des réponses faites	**Réussite**

2.3.5.2. Avis d'expert sur la résistance des mécanismes

L'évaluateur n'a pas pu mettre en évidence de faiblesse dans l'implémentation des mécanismes selon les conditions définies dans la cible de sécurité.

2.3.6. Analyse des vulnérabilités (conception, construction…)

2.3.6.1. Liste des vulnérabilités connues

Des vulnérabilités publiques affectant certains composants utilisés par le produit étaient connues au moment de l'évaluation. Elles ont été analysées et jugées non applicables au produit ou non pertinentes par l'évaluateur dans le contexte d'emploi et la configuration retenus.

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

Il n'a pas été identifié de vulnérabilité majeure exploitable dans le périmètre d'évaluation et pour le cas d'usage considéré.

2.3.7. Accès aux développeurs

Aucun support du développeur n'a été requis au cours de l'évaluation.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

L'auditeur n'a pas identifié de cas où la sécurité du produit était ambiguë.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Les recommandations suivantes sont formulées par l'évaluateur :

- le poste d'administration doit être sain et il doit être placé dans une enceinte de confiance, conformément aux hypothèses faites dans la cible. Sinon toute personne ayant accès à la machine d'administration peut récupérer les certificats nécessaires aux connexions d'administration et s'en servir ultérieurement pour reconfigurer les fonctions de sécurité de l'*appliance* (notamment les connexions SSL). En effet les interfaces d'administration sont dépourvues d'identifiant/mot de passe de connexion en plus du certificat client ;
- les certificats utilisés par défaut pour les connections SSL doivent être changés et ils doivent être protégés par des mots de passe forts ;
- le HSM servant à l'horodatage des réponses doit être correctement configuré.

De manière générale l'administrateur doit bien veiller à ce que les configurations par défaut et notamment celle de la connexion au serveur soient impérativement changées à l'installation du produit.

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

La phase d'installation est relativement simple, hormis la configuration du HSM qui est insuffisamment documentée. L'administrateur doit posséder de bonnes connaissances en termes de gestion de PKI : gestion de certificats d'AC, CRL, chemins de certification, politiques de validation etc. En outre, il est nécessaire d'être très attentif à la bonne configuration de la TOE (connexion SSL, HSM) afin de garantir que celle-ci soit déployée avec un niveau de sécurité satisfaisant.

2.3.8.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

L'évaluateur a procédé à une analyse des mécanismes cryptographiques offerts par le produit. Celle-ci n'a pas relevé de manquements jugés bloquants, néanmoins l'évaluateur a mis en évidence la non-conformité suivante :

- l'algorithme de signature utilisé pour signer les requêtes et les réponses est RSASSA-PKCS1v1_5 qui n'est pas conforme aux recommandations du [RGS] car ne disposant pas de preuve de sécurité.

2.5. Analyse du générateur d'aléas

Le produit fait appel au générateur d'*OpenSSL* pour la génération de nombres pseudo-aléatoires.
L'évaluation n'a pas mis en évidence de vulnérabilités dans le produit liées à l'utilisation de ce générateur.

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 produit « VeriCert, version 2.1.2 » 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, notamment assurer la protection physique du produit.

Annexe 1. Références documentaires du produit évalué

[CDS]	Cible de sécurité CSPN – VeriCert ; Référence : BULL.VRC.CSPN.01 ; Version : 2.0 ; Date : 30/05/2013.
[RTE]	Rapport Technique d'Évaluation (RTE) CSPN VeriCert V2.1.2 ; Référence : OPPIDA/CESTI/BULL.CDR.CSPN/RTE/1.1 ; Version : 1.1 ; Date : 12/12/2014.
[GUIDE]	Guide Utilisateur final ; Référence : VeriCert_MA002_Guide-Utilisateur-Final_v1.0_fr.pdf ; Version : 1.0. Guide Administrateur ; Référence : VeriCert_MA003_Guide-Administrateur_v1.1_fr.pdf ; Version : 1.1. Guide Auditeur ; Référence : VeriCert _MA004_Guide-Auditeur_v1.0_fr.pdf ; Version : 1.0. Guide d'exploitation de l'*appliance* VeriCert ; Référence : Vericert_ME001_Appliance Virtuelle.pdf. Guide d'installation de l'*appliance* VeriCert ; Référence : Vericert_MI001_Appliance Virtuelle_fr.pdf ; Guide d'administration de l'*appliance* VeriCert ; Référence : Vericert_MA001_Appliance Virtuelle_fr.pdf. Documentation utilisateur de l'interface d'administration du VeriCert ; Référence : VeriCert_MA001_Guide-Utilisateur_v1.7_fr.pdf. Guide général ; Référence : VeriCert_MA004_Guide-Général_v1.2_fr.pdf ; Version : 1.2.
[CRY]	*Description des mécanismes cryptographiques ;* Référence : Cericert_st002_mécanismes_cryptographiques_v1.1_fr ; Version : 1.1 ; Date : 23 juin 2014.

Annexe 2. 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.	
[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.