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-2014/05

Pare-feu applicatif i-Suite
Version 5.5.5 révision 21873

Paris, le 16 septembre 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-2014/05**
Nom du produit **Pare-feu applicatif i-Suite**
Référence/version du produit **5.5.5 révision 21873**
Catégorie de produit **Pare-feu**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **Bee Ware** **20 rue de Billancourt** **92100 Boulogne-Billancourt** **France**
Commanditaire **Bee Ware** **20 rue de Billancourt** **92100 Boulogne-Billancourt** **France**
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 i-Suite, développé par Bee Ware, est une *appliance* réalisant la fonction de pare-feu applicatif web (*Web Application Firewall* ou WAF) lorsqu'elle est positionnée en coupure entre des serveurs ou services web à protéger et internet.
Le produit agit alors en tant que *reverse-proxy,* interceptant et filtrant les flux HTTP entre les utilisateurs et les applications web.
Le produit permet de définir et d'appliquer des règles de filtrages et des *workflows*[1] propres à chaque application à protéger.

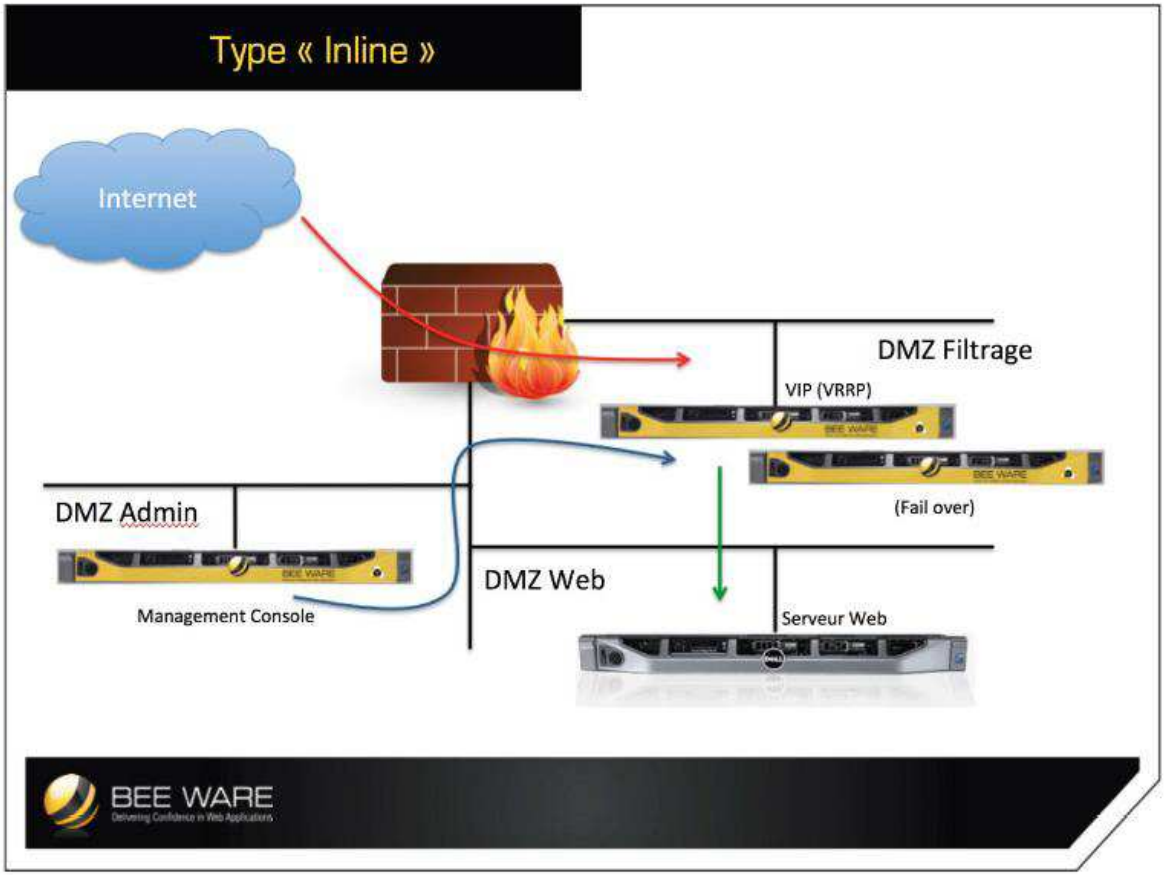

Figure 1- Positionnement du produit

[1] Un *workflow* définit l'enchaînement des opérations à effectuer pour le traitement des requêtes.

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	i-Suite
Numéro de version analysée	5.5.5 révision 21873

La version certifiée du produit est identifiable lors de la connexion à l'application d'administration.

Figure 2 - Identification de la version évaluée

1.2.3. Services de sécurité évalués

Les principaux services de sécurité fournis par le produit sont :

- le filtrage des requêtes et la protection contre les principales classes d'attaques connues ;
- la gestion sécurisée des cookies ;
- le filtrage et validation XML ;
- la sécurisation du trafic HTTP ;
- la protection contre les attaques de type déni de service.

Ces services sont déclinés en fonctionnalités détaillées au chapitre 2.3.4 qui ont été testées de façon unitaire par l'évaluateur.

1.2.4. Configuration évaluée

Le produit a été évalué avec les règles de filtrage « *Default policy (strict)* » dans leur version 3.16, accompagnées d'un *workflow* de décodage base64.

Figure 3 - Version de la politique 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 »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 5 « description des biens sensibles »).

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

Conforme à la cible de sécurité [CDS] (chapitre 5 « description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 6 « description des fonctions de sécurité du produit »).

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 2.1.3 « description des utilisateurs typiques concernés et de leur rôle dans l'utilisation du produit »).

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 des plateformes web couramment déployées.

Afin d'assurer la reproductibilité des tests les serveurs cibles ont été installés sur des machines virtuelles générées à l'aide de l'outil VMWare Workstation (version 8.0.6).

L'appliance i-Suite est placée en position de relais inverse. Elle protège deux serveurs virtuels :

- Serveur 1 : machine virtuelle embarquant un système d'exploitation Fedora 19 64 bits, un serveur web Apache 2.4.6, un serveur MySQL 5.5.32, un serveur PostgreSQL 9.2.4 et un serveur Oracle Database 11g Express Edition Release 11.2.0.2.0. Une application développée pour les besoins de l'évaluation permet de tester les fonctions de sécurité.
- Serveur 2 : machine virtuelle embarquant un système d'exploitation Windows 7 64 bits ainsi qu'un serveur web IIS et une application ASP permettant de jouer des tests sur les paramètres HTTP. Un serveur SQL Server Express 11.0.3128.0 est également installé et utilisé pour les besoins de l'application embarquée sur le serveur 1.

Les environnements déployés étaient à jour des correctifs de sécurité au moment où les tests ont été réalisés.

L'application d'administration de l'appliance i-Suite est téléchargée depuis le site internet de l'éditeur.

2.3.2.2. Particularités de paramétrage de l'environnement

L'architecture de test a été définie conformément au guide d'installation du produit. Le mode d'installation « inline » a été choisi dans le cadre de l'évaluation.
Les paramètres par défaut de l'appliance ont été utilisés pour l'évaluation. Les règles de filtrage étaient positionnées sur « *Default policy (strict)* » et accompagnées d'un *workflow* de décodage base64. Le *workflow* « standard » (voir figure 4) a également été appliqué. L'évaluateur a ensuite défini ses propres *workflows*, le *workflow* standard ne permettant pas d'utiliser toutes les fonctionnalités de sécurité offertes par la TOE.

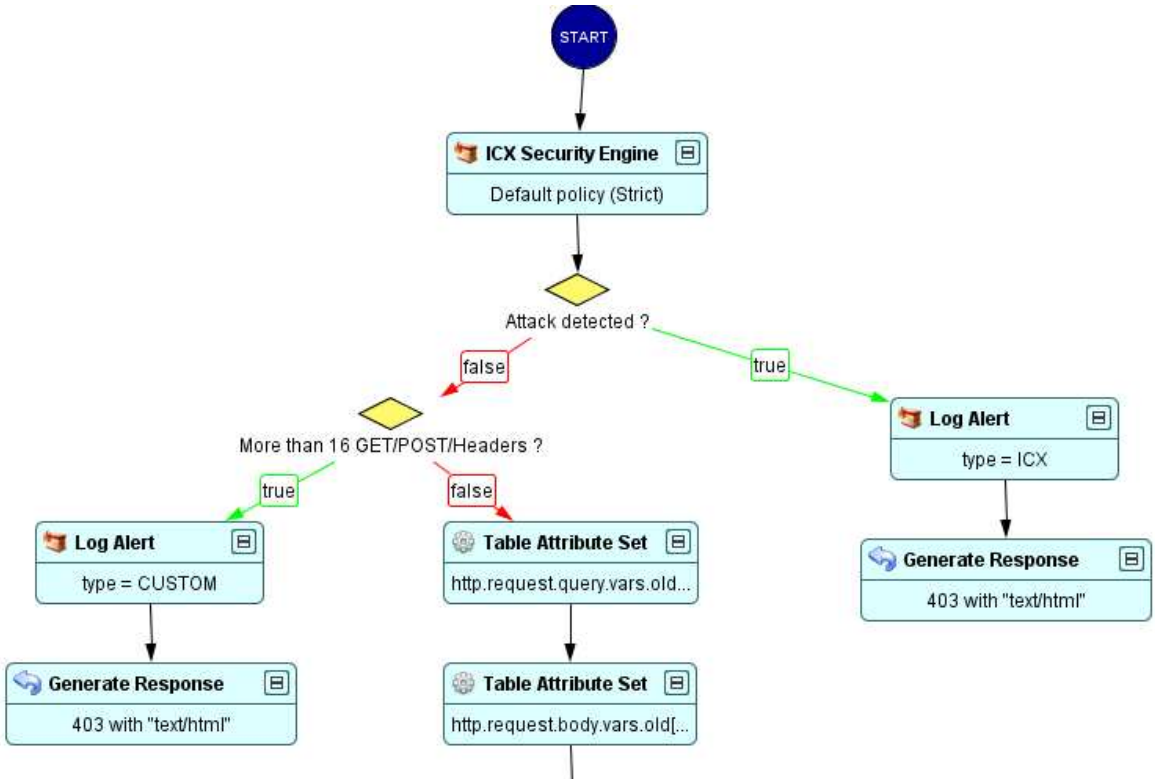

Figure 4 : workflow standard utilisé pour les tests

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

L'*appliance* a été livrée et sa configuration réseau réalisée par un personnel de la société Bee Ware.
La configuration des services d'i-Suite s'effectue simplement et sans problème particulier.

2.3.2.5. Durée de l'installation

La configuration d'i-Suite avec le *workflow* standard est rapide. L'administrateur du produit devra configurer un tunnel afin de rediriger les flux reçus par i-Suite vers le serveur web à protéger. Sur ce tunnel, il faudra appliquer un *workflow* ou une *focus table*, qui correspondent à une politique de filtrage.
L'administrateur d'i-Suite pourra également configurer des liens SSL, de la répartition de charge ou modifier les politiques de filtrage afin d'y ajouter des fonctionnalités (authentification utilisateur par certificat, protection des cookies, etc.).

La mise en place d'un workflow adapté à une application peut être complexe et nécessiter un travail de plusieurs semaines. Cette opération doit être réalisée par une personne formée à l'utilisation du produit ou assistée du développeur.

2.3.2.6. Notes et remarques diverses

L'installation du produit est simple et consiste en une rapide configuration réseau du boitier une fois ce dernier branché et démarré. Les règles de filtrage « *default strict* », version 3.16 sont figées lors de la production du boitier chez le développeur et ne sont pas modifiables. La procédure d'installation, détaillée dans [GUIDE], est claire et précise.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès au guide d'utilisation du produit [GUIDE]. La documentation est claire, complète et assiste efficacement l'administrateur dans l'installation et la configuration du produit.

La documentation administrateur, téléchargeable sur le site du développeur, manque parfois de détail dans la description des différents aspects des fonctionnalités de sécurité, ainsi que d'exemples simples pour permettre la création de *workflows* adaptés à chaque fonctionnalité.

2.3.4. Fonctionnalités testées

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

Fonctionnalité	Résultat
Protection contre les attaques de type *Command Injection*	**Réussite**
Protection contre les attaques de type *Cross-Site Scripting*	**Réussite**
Protection contre les attaques de type *SQL injection*	**Réussite**
Protection contre les attaques de type *LDAP injection*	**Réussite**
Protection contre les attaques de type *XPATH injection*	**Réussite**
Protection contre les attaques de type *Remote File Inclusion*	**Réussite**
Cookie ciphering	**Réussite**
Cookie tracking	**Réussite**
Cookie virtualization	**Réussite**
Validation du format XML d'entrée	**Réussite**
Protection contre l'inclusion d'entités XML	**Réussite**
Protection contre la récursivité XML	**Réussite**
Validation par WSDL/XSD de fichiers XML	**Réussite**
Signature/Chiffrement de XML	**Réussite**
Terminaison SSL entrante	**Réussite**
Validation des certificats clients	**Réussite**
Request limiter	**Réussite**
Filtrage par géolocalisation	**Réussite**
Décodage des entrées utilisateurs	**Réussite**

2.3.5. Fonctionnalités non testées

Néant.

2.3.6. 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]. Il est à noter que la fonction de protection contre la modification de contenu statique, hors périmètre de l'évaluation, ne fonctionnait pas correctement sur le produit livré à l'évaluateur. Cette fonction doit permettre de détecter la modification malicieuse du contenu d'une page web protégée par i-Suite. Lors des tests, le produit n'a jamais renvoyé le code erreur attendu alors même que le contenu avait été modifié par l'évaluateur.

2.3.7. Avis d'expert sur le produit

Le produit est fonctionnellement conforme à sa cible de sécurité.

2.3.8. Analyse de la résistance des mécanismes et des fonctions

2.3.8.1. Liste des fonctions et des mécanismes testés

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

Fonctionnalité	Résultat
Protection contre les attaques de type *Command Injection*	**Réussite**
Protection contre les attaques de type *Cross-Site Scripting*	**Réussite**
Protection contre les attaques de type *SQL injection*	**Réussite**
Protection contre les attaques de type *LDAP injection*	**Réussite**
Protection contre les attaques de type *XPATH injection*	**Réussite**
Protection contre les attaques de type *Remote File Inclusion*	**Réussite**
Cookie ciphering	**Réussite**
Cookie tracking	**Réussite**
Cookie virtualization	**Réussite**
Validation du format XML d'entrée	**Réussite**
Protection contre l'inclusion d'entités XML	**Réussite**
Protection contre la récursivité XML	**Réussite**
Validation par WSDL/XSD de fichiers XML	**Réussite**
Signature/Chiffrement de XML	**Réussite**
Terminaison SSL entrante	**Réussite**
Validation des certificats clients	**Réussite**
Request limiter	**Réussite**
Filtrage par géolocalisation	**Réussite**
Décodage des entrées utilisateurs	**Réussite**

2.3.8.2. Avis d'expert sur la résistance des mécanismes

Comme tout système de filtrage, i-Suite a des limites. Ainsi, il sera toujours possible de contourner le filtrage en cherchant des variations ou des encodages non gérés par i-Suite.
Cependant, l'ensemble des fonctionnalités et des modules de la version évaluée apporte un bon niveau de protection en détectant globalement les principaux types d'attaques.
Seule la fonction de protection contre la modification de contenu statique s'est avérée inefficace sur le produit mis à disposition de l'évaluateur.

2.3.9. Analyse des vulnérabilités (conception, construction…)

2.3.9.1. Liste des vulnérabilités connues

Aucune vulnérabilité publique n'est connue pour le produit.

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

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

2.3.10. Accès aux développeurs

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

2.3.11. Analyse de la facilité d'emploi et préconisations

2.3.11.1. Cas où la sécurité est remise en cause

Néant.

2.3.11.2. Recommandations pour une utilisation sûre du produit

Le produit doit être déployé au sein d'une architecture respectant les préconisations du développeur. Par ailleurs, pour assurer une utilisation sûre du produit, l'évaluateur recommande :

- d'utiliser des suites de chiffrement conformes aux règles et recommandations de l'ANSSI pour la configuration des tunnels SSL ;
- d'utiliser la politique de sécurité « *Default policy (strict)* » lors de la configuration de l'*ICX Security Engine* de l'*appliance* ;
- de ne pas se reposer uniquement sur la capacité du WAF à bloquer les requêtes malveillantes ; l'état de l'art des attaques évoluant rapidement, un effort particulier doit être mis sur la configuration de *workflows* pour chaque application à protéger ainsi que sur leur mise à jour.

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

La configuration initiale du produit est simple et claire, et l'intégration modulaire des fonctions de sécurité facilite la compréhension des tâches de configuration de même que l'ergonomie de l'interface d'administration.
En revanche, la configuration de workflows dédiés aux applications à protéger se révèle plus complexe et nécessite une bonne maîtrise du produit voire le support du développeur afin que leur mise en place ne laisse pas apparaître de vulnérabilités.

2.3.11.4. 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 relevés de manquements jugés bloquants, néanmoins l'évaluateur a mis en évidence les non-conformités suivantes :

- l'intégrité des pages statiques protégées par la fonction *anti-deface* est assurée à l'aide de l'algorithme MD5, non conforme aux règles établies dans le RGS [REF-CRYPTO] ;
- la signature des fichiers XML lorsque l'algorithme RSA est utilisé fait appel au *padding* PKCS#1 v1.5, non conforme aux recommandations du RGS.

2.5. Analyse du générateur d'aléas

Le produit fait appel au générateur de Linux, `/dev/urandom`, 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 « i-Suite, version 5.5.5 révision 21873 » 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]	*Bee Ware i-Suite Cible de sécurité CSPN;* Référence : *BNX_Cible-de-sécurité_CSPN ;* Version : *1.3*; Date : *03/09/2014.*
[RTE]	*Rapport Technique d'Évaluation (RTE) CSPN Bee Ware i-Suite ;* Référence : *OPPIDA/CESTI/2014/CBC/1.0* ; Version : *1.0* ; Date : *24/05/2014.*
[GUIDE]	*Guide d'administration ;* Référence : *Guide d'administration-v29-20140423_1120 ;* Version du *23 avril 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.