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-2011/12

Fournitures d'Infrastructure Santé Social (FISS)
Version 1.12.10

Paris, le 17/10/2011

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 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-2011/12

Nom du produit

Fournitures d'Infrastructure Santé Social (FISS)

Référence/version du produit

1.12.10

Catégorie du produit

Communication sécurisée

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*

Développeur(s)

GIE SESAM-VITALE

5, boulevard Marie Alexandre Oyon

72019 LE MANS CEDEX 2

France

Commanditaire

GIE SESAM-VITALE

5, boulevard Marie Alexandre Oyon

72019 LE MANS CEDEX 2

France

Centre d'évaluation

Oppida

4-6, avenue du Vieil Etang - Bât B

78180 Montigny Le Bretonneux

Tél : 01 30 14 19 00, mél : cesti@oppida.fr

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 « Fournitures d'Infrastructure Santé Social (FISS)**,** version 1.12.10 **»** développé par le GIE SESAM-VITALE.

Ce produit est une interface applicative installée sur les postes de travail des professionnels de santé, qui permet d'établir un canal sécurisé SSL/TLS entre un progiciel de santé agréé par le GIE SESAM-Vitale et des services en ligne fournis par les partenaires du GIE SESAM-Vitale localisés sur un serveur appelé « serveur IMARS ».

Il est destiné aux développeurs de progiciels de santé souhaitant intégrer les fonctionnalités de FISS dans leurs applications.

FISS est composé des 4 briques fonctionnelles suivantes :

- Un module SIC (serveur interface client) permettant d'interfacer le progiciel de santé avec les composants métier (gestion des sessions et des contextes utilisateur) et de rediriger les appels émis par le progiciel vers le contrôleur approprié ;
- un contrôleur SEL (service en ligne) gérant l'accès sécurisé aux services web distants ;
- un contrôleur STC (services techniques communs) gérant l'accès aux ressources locales (données carte CPS/Vitale, fichiers locaux) ;
- un contrôleur SLC (service lecture carte) gérant les interactions avec la carte du professionnel de santé et la carte vitale.

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

1.2.2. Identification du produit

La version certifiée du produit est identifiable à l'aide de l'outil de diagnostic. La version de FISS 1.12.10 correspond aux versions des composants suivants :

- SIC 1.13
- SEL 1.11
- STC 1.12
- SLC 1.02

Le sha256 calculé sur le fichier d'installation fiss-1.12.10.msi est :

a11363425eace9d047c8e24238cae059d7be03a4f873a6693500eea51d8889d6

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- protection en confidentialité et en intégrité des échanges entre le progiciel et le serveur IMARS ;
- authentification mutuelle entre FISS et le serveur IMARS ;
- protection en intégrité des composants de FISS.

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 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 « Description (Argumentaire) du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

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

2.3.1.4. Fonctions de sécurité

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

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre « Description de l'environnement prévu pour son utilisation »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Le produit a été testé avec les systèmes d'exploitation suivants :

- Windows XP (Service Pack 3) 32 bits ;

- Windows Vista (Service Pack 2) 32 bits ;
- Windows Seven 32 bits.

L'interface logiciele FISS dépend de plusieurs éléments identifiés dans le § 2.3.2.2. Les versions de ces dépendances installées sur la plate-forme de test sont les suivantes :
- Java Runtime Environment (JRE) privée 1.6 Update 16;
- la librairie « *cryptolib* » en version 3.0.6 ;
- l'API GALSS en version 3.26.

Les matériels suivants ont été fournis à l'évaluateur :
- un lecteur de carte CPS / Vitale INGENICO ICT250 relié par USB au poste du professionnel de santé ;
- une carte CPS ;
- une carte Vitale.

2.3.2.2. Particularités de paramétrage de l'environnement

L'installation du produit nécessite les éléments suivants :
- Java Runtime Environment (JRE) privée 1.6 (JRE privée fournie par SESAM/Vitale) ;
- la librairie cryptographique « *cryptolib* » de l'ASIP-Santé ;
- l'API GALSS permettant de dialoguer avec les secteurs de carte SESAM-Vitale.

Ces dépendances sont identifiées dans la cible [CDS] et leur installation est décrite dans le manuel de programmation [GUIDES].

2.3.2.3. Options d'installation retenues pour le produit

Sans objet.

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

Sans objet.

2.3.2.5. Durée de l'installation

Sans objet.

2.3.2.6. Notes et remarques diverses

Hormis l'installation des dépendances nécessaires identifiées dans le § 2.3.2.2, l'installation est simple et ne requiert aucune configuration de la part de l'utilisateur.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. Il s'agit d'un manuel de programmation destiné aux développeurs de progiciels qui souhaitent s'appuyer sur l'interface FISS. La documentation décrit de façon claire la façon d'installer et d'utiliser le produit. Aucune non-conformité n'a été relevée.

2.3.4. Revue du code source (facultative)

Les évaluateurs ont eu accès à l'intégralité du code source. Ils ont focalisé leur étude sur les fonctions cryptographiques. Aucune erreur de programmation n'a été identifiée dans la partie du code auditée.

Le code est correctement structuré et documenté.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Authentification mutuelle	**Réussite**
Chiffrement et intégrité	**Réussite**

2.3.6. Fonctionnalités non testées

Néant.

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

L'ensemble des fonctionnalités identifiées dans la cible [CDS] ont été testées et aucune non-conformité n'a été relevée.

2.3.8. Avis d'expert sur le produit

Le produit est conforme à sa cible de sécurité [CDS]. Les API sont claires, non ambigües et correctement détaillées.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

Les mécanismes de sécurité présents dans FISS sont des mécanismes cryptographiques. L'analyse de leur résistance est détaillée dans le § 2.4 du présent rapport.

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 particulier.

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

Une vulnérabilité impactant le poste de travail du professionnel de santé à été découverte durant l'évaluation. Cependant, cette vulnérabilité n'est pas exploitable si les recommandations présentes dans le manuel de programmation [GUIDES] et dans le § 2.3.12.2 du présent rapport sont suivies.

2.3.11. 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 bonne maîtrise de son produit et a été en mesure de répondre rapidement et efficacement 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

Recommandations pour le poste

L'utilisation du produit doit être faite sur un PC hébergeant un système d'exploitation à jour des correctifs de sécurité et correctement administré. Ce poste doit être au minimum protégé par un produit anti-virus (avec bases d'information à jour et proposant des fonctions de détection des infections informatiques furtives - anti-*spyware*, anti-*rootkit*, etc.) et un pare-feu correctement configuré. Ce dernier doit notamment empêcher tout accès au service réseau FISS sur les ports 1943, 4554 et 6880.

Le produit ne devrait pas être utilisé en cas de doute sur la sécurité du poste de travail.

Le lecteur de carte SESAM-VITALE doit être relié au lecteur de carte à puce uniquement via une liaison locale (USB par exemple).

Recommandations pour les développeurs d'applications

Les applications se basant sur FISS doivent être développées en suivant l'ensemble des recommandations présentes dans le manuel de programmation [GUIDES]. En particulier, lorsque les cartes SESAM/VITALE le permettent, il est recommandé d'utiliser des bi-clés dont la taille du module est au moins égale à 2048 bits.

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

Le public cible du produit est constitué de développeurs souhaitant intégrer les fonctionnalités de FISS dans leur application (progiciel). Bien que non évidente, l'utilisation de FISS est grandement facilitée par le manuel de programmation [GUIDES] qui fournit au développeur un niveau de détail suffisant.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

Le produit évalué offre les services cryptographiques suivants :

- Authentification mutuelle ;
- Chiffrement et intégrité des données ;
- Contrôle d'intégrité du code.

La résistance des mécanismes cryptographiques a été analysée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] et ne donnent lieu à aucune autre recommandation que celles présentes dans le manuel de programmation [GUIDES] et dans le § 2.3.12 du présent rapport.

Les mécanismes cryptographiques mis en œuvre par le produit sont conformes à [REF-CRY].

2.5. Analyse du générateur d'aléas

Le générateur d'aléas utilisé est celui de la carte à puce SESAM-VITALE. Il a donc été évalué dans le cadre de la certification de cette dernière.

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 « Fournitures d'Infrastructure Santé Social**,** 1.12.10 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS].

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.

Annexe 1. Références documentaires du produit évalué

[CDS]	*CSPN : Cible de sécurité FISS ;* Version : *1.0* ; Date : *10/01/2011*
[RTE]	*Rapport Technique d'Évaluation (RTE) : Fournitures d'Infrastructure Santé Social (FISS) ;* Référence : *OPPIDA/CESTI/BEA : 651/1.0* ; Date : *31/05/2011*
[ANA-CRY]	*Rapport d'évaluation des mécanismes cryptographiques ;* Référence : *OPPIDA/CESTI/2011/BEA/651/1.0* ; Date : *31/05/2011* *Addendum : Fournitures d'Infrastructure Santé Social (FISS) ;* Référence : *OPPIDA/CESTI/BEA/ADDENDUM/2.0* ; Date : *27/09/2011*
[GUIDES]	Manuel de programmation : *Fournitures d'Infrastructure Santé Social 1.12.10 : Manuel de programmation ;* Référence : *FISS-MP-001* ; Version : *1.16* Date : *juin 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