CSPN : Cible de sécurité FISS

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
10/01/2011	1.0	Document validé	B.STAIQULY
15/06/2011	1.1	Prise en compte des remarques du CESTI	B.STAIQULY

TABLE DES MATIERES

1 Glossaire

ASIP-Santé	Agence des Systèmes d'Information Partagés de Santé
CC	Critères communs
CPS	Carte de Professionnel de santé
CSPN	Certification Sécurité de Premier Niveau
FISS	Fournitures d'Infrastructure Santé Social – objet de cette cible de sécurité
GIE	Groupement d'Intérêt Economique
GIP	Groupement d'intérêt Public
IMARS	Serveur portail des requêtes des progiciels – rôle d'ordonnanceur et de routage des requêtes vers les différents services en ligne
PS	Professionnel de Santé
TLS	Transport Layer Security

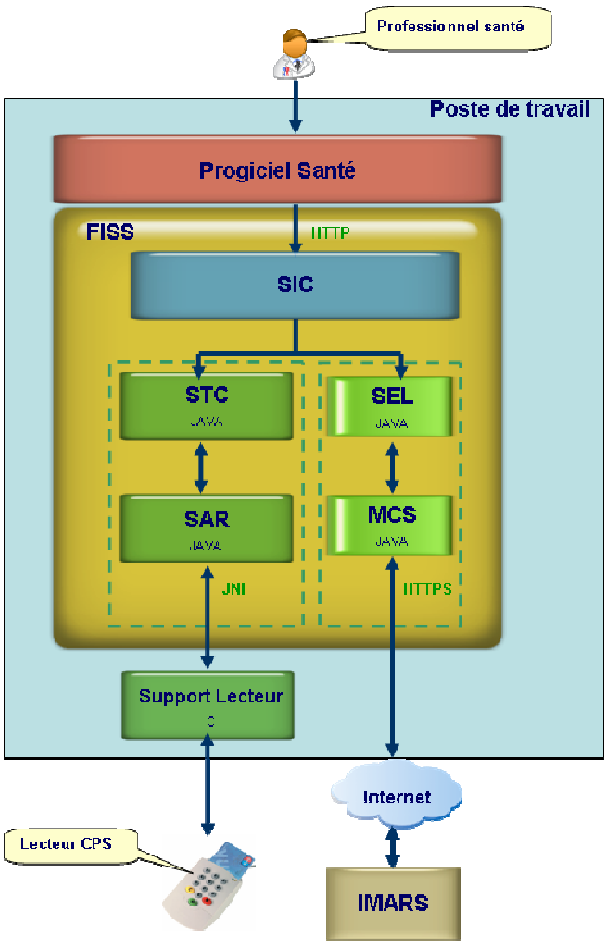
2 Identification du produit

Organisation éditrice	GIE SESAM-Vitale
Lien vers l'organisation	http://www.sesam-vitale.fr
Nom commercial du produit	**F**ournitures d'**I**nfrastructure **S**anté **S**ocial
Numéro de la version	FISS 1.12.10
Catégorie de produit	7 - communication sécurisée

3 Description (Argumentaire) du produit

3.1 Description générale du produit

Les Fournitures d'Infrastructure Santé Social (*noté FISS dans ce document*) constituent une interface applicative installée sur les postes de travail des professionnels de santé (*noté postes PS*) 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. Le canal sécurisé est établi entre les FISS et un serveur appelé IMARS, qui se comporte comme un ordonnanceur. Celui-ci effectue des contrôles métiers et route les requêtes vers le service en ligne demandé par le professionnel de santé (*noté PS*).



Les FISS sont constitués des briques fonctionnelles suivantes :

- Un module **SIC** (Serveur Interface Client) : cette brique est l'unique interface entre le progiciel de santé et les composants métier. Il offre des mécanismes de gestion de session et de contexte utilisateur et propose certains services Web locaux (ouverture/fermeture de session, gestion des appels différés …). Il possède également un rôle de routage en redirigeant les demandes émises par le progiciel vers le contrôleur métier approprié (STC, SEL …).
- Un contrôleur **SEL** : ce module a pour rôle d'offrir un accès sécurisé aux services Web distants. Il est en charge de la gestion de la cinématique du dialogue entre les FISS et l'IMARS, avec notamment la gestion de messages de services.
- Un module **MCS** (Module de Connexions Sécurisées) : cette couche applicative sert d'interface entre le SEL et le portail IMARS, c'est donc elle qui ouvre une communication sécurisée TLS avec l'IMARS (gestion de l'authentification mutuelle et du pool de connexions). Ce module est appelé par le contrôleur SEL.
- Un contrôleur **STC** : ce module offre des services Web locaux ayant pour objectifs de manipuler les ressources locales (données cartes CPS/Vitale, fichiers locaux).
- Un module **SAR** (Service Accès aux Ressources) : ce module représente l'interface avec les API de supports techniques. Il utilise une JNI pour appeler la librairie cryptographique Cryptolib CPS de l'ASIP Santé afin d'accéder aux fonctions de la carte CPS. Il utilise également une JNI pour appeler le GALSS pour dialoguer avec les lecteurs SESAM-Vitale et ainsi réaliser la lecture des données des cartes Vitale et CPS. Ce module est appelé par le contrôleur STC.

Les FISS utilisent également le composant **d'accès aux lecteurs (Galss)** : c'est une API (bas niveau) écrite en langage C qui a pour rôle d'établir la communication entre le poste PS et les lecteurs de carte à puce SESAM-Vitale. Cette API est appelée par le module SAR via une JNI.

3.2 Description de la manière d'utiliser le produit

Le produit est démarré au démarrage du poste et reste actif en permanence.

Le produit sera livré à l'éditeur de progiciel afin qu'il installe les FISS avec son produit en respectant les recommandations du GIE SESAM-Vitale.

4 Description de l'environnement prévu pour son utilisation

Les FISS peuvent être installés sur plusieurs types de systèmes d'exploitation. Voici les éléments de configuration requis pour le fonctionnement des FISS :

Système d'exploitation (configuration minimum) :

- ⇨ Windows XP (Service pack 3), Architecture 32 bits.
- ⇨ Windows Vista (Service pack 2), Architecture 32 et 64 bits.
- ⇨ Windows Seven, Architecture 32 et 64 bits.
- ⇨ Linux noyau 2.4 ou 2.6, Architecture 32 bits.
- ⇨ Mac OSX 10.4.11 (Tiger), Architecture 32 bits.
- ⇨ Mac OSX 10.5.8 (Leopard), Architecture 32 et 64 bits.
- ⇨ Mac OSX 10.6.3 (Snow Leopard), Architecture 32 et 64 bits

Modules tiers nécessaires au fonctionnement des FISS :

- ⇨ Lecteur de carte CPS/Vitale 3.x ou supérieur (homologué par le GIE SESAM-Vitale),
- ⇨ Carte CPS et carte Vitale,
- ⇨ Java Runtime Environment 1.6.0 (JVM Privée),
- ⇨ Librairie Cryptographique de l'ASIP-Santé (anciennement GIP CPS), cryptolib en version 3.0.6.

Le contexte opérationnel des FISS est simple. Il concerne les PS (pharmaciens, médecins, infirmiers…) qui possèdent un lecteur de carte CPS/Vitale et qui souhaitent accéder via leur progiciel aux services en ligne des partenaires du GIE SESAM-Vitale.

4.1 Description des hypothèses sur l'environnement

Les composants FISS doivent être installés sur un système sain, régulièrement mis à jour, en particulier concernant les correctifs liés à la sécurité OS et à la base de signatures anti-virus. Le système d'exploitation du poste PS devra être sécurisé : installation d'une d'un anti-malware et d'un pare-feu personnel, sauvegarde régulière des données, utilisation de mot de passe robuste. Le poste de travail du PS n'est utilisé que dans le cadre de son activité professionnelle.

Les FISS sont exécutés dans une session en mode système.

A noter que les recommandations de sécurisation sont explicitées dans les documents fournis aux éditeurs de progiciels qui sont en charge de l'installation des FISS. Ces derniers doivent prendre en compte ces recommandations dans la programmation de leurs applications.

Les **équipes d'administration** du GIE SESAM-Vitale sont considérées comme non hostiles.

Les **éditeurs de progiciels** qui installent le produit chez le PS sont considérés comme non hostiles. Ils suivent les recommandations du GIE SESAM-Vitale quant à la vérification des pré-requis d'installation des FISS, et suivent les procédures d'installation et le manuel de programmation des FISS fournis par le GIE SESAM-Vitale.

Les **utilisateurs des FISS** (PS) sont considérés comme non hostiles. Ils utilisent le progiciel et les FISS sans volonté de porter atteinte à la sécurité des données manipulées.

Le **système d'exploitation** supportant les FISS est correctement administré et configuré, conformément aux recommandations formulées par le GIE SESAM-Vitale.

Le **serveur IMARS** ne doit pas pouvoir être utilisé comme oracle de vérification de padding. Il doit être capable de négocier uniquement les clés des suites supportées par FISS et définies dans le manuel de programmation. Il doit également implémenter la RFC 5746 concernant la renégociation de TLS.

4.2 Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le produit.

L'éditeur de progiciel qui installe les FISS sur les postes des professionnels de santé est en charge d'installer le lecteur de carte CPS/Vitale et doit s'assurer que les pré-requis techniques de bon fonctionnement des FISS sont respectés (installation de la JRE privée, sécurisation des postes PS, version OS et mises à jour associées).

Le lecteur de carte CPS/Vitale doit être relié au poste de travail soit sur l'interface USB soit par l'interface série RS232. Les autres interfaces (Ethernet, RTC) ne doivent pas être utilisées.

4.3 Description des utilisateurs typiques concernés (utilisateurs finaux, administrateurs, experts…) et de leur rôle particulier dans l'utilisation du produit.

Le contexte d'emploi organisationnel est le suivant :

⇨ un ou plusieurs administrateurs dont le rôle est de procéder aux opérations d'installation, de configuration et de maintenance. Ces administrateurs disposent de droits d'accès privilégiés au système d'exploitation : compte administrateur ou similaire ;

⇨ des professionnels de santé (utilisateurs du système) qui utilisent le progiciel, ce dernier sollicite les FISS pour accéder aux services en ligne.

4.4 Définition du périmètre de l'évaluation, à savoir les caractéristiques de sécurité du produit concernées par l'évaluation

Dans le périmètre :

- La communication SSL/TLS entre les FISS et l'IMARS.

Hors périmètre :

- Progiciel,
- IMARS,
- Lecteur de carte CPS/Vitale,
- Les cartes CPS et Vitale,
- OS,

- Librairie Cryptographique de l'ASIP-Santé.

Les fonctions de sécurité inclues dans le périmètre de l'évaluation sont les suivantes :

⇨ **Authentification** mutuelle entre les **FISS** et le serveur **IMARS** par certificat X509 ;

⇨ **Chiffrement et Intégrité des données** SSL/TLS entre les **FISS** et le serveur **IMARS** ;

5 Description de l'environnement technique dans lequel le produit doit fonctionner

⇨ **Configuration matérielle minimum requise :**

Pentium 400 MHz minimum (1 GHz recommandé)
25 Mo d'espace disque disponible
128 Mo de mémoire RAM (512 Mo recommandé)

⇨ **Systèmes d'exploitation retenus**

- Windows XP (Service pack 3),
- Windows Vista (Service pack 2),
- Windows Seven.

6 Description des biens sensibles que le produit doit protéger

Les FISS permettent l'établissement d'un canal SSL/TLS sécurisé entre le progiciel et les services en ligne des partenaires SESAM-Vitale afin de protéger l'intégrité et la confidentialité des **données médicales et médico-administratives** qui transitent sur le réseau.

Les **biens et les données qui transitent** par les FISS sont :

⇨ Données métiers (données médico-administratives ou médicales) des assurés du PS,

⇨ Données issues des cartes Vitale et CPS.

7 Description des menaces

L'agent menaçant contre qui le GIE SESAM-Vitale souhaite se protéger est une personne externe ayant un potentiel d'attaque faible (au sens des CC), connaissant les services offerts par le GIE SESAM-Vitale. Le niveau de résistance des fonctions doit être de niveau élémentaire.

Par hypothèse, les administrateurs des FISS, le Professionnel de Santé et l'administrateur du poste PS ne sont pas considérés comme des attaquants potentiels.

Description des menaces :

⇨ Un attaquant externe (sur Internet) récupère les données échangées entre les FISS et le serveur IMARS ;

⇨ Un attaquant externe (sur Internet) modifie les données contenues dans les échanges entre les FISS et le serveur IMARS.

8 Description des fonctions de sécurité du produit

La fonctionnalité principale des FISS est de permettre aux professionnels de santé d'accéder aux nouveaux services en ligne des partenaires du GIE SESAM-Vitale. Les professionnels de santé utilisent leur progiciel métier pour accéder aux services en ligne. Les informations contenues dans les échanges entre le progiciel et les services en ligne sont susceptibles de contenir des données techniques, médicales et médico-administratives confidentielles. Les FISS permettent alors l'envoi sécurisé de ces données sur Internet depuis les FISS jusqu'au serveur IMARS.

Afin de répondre aux menaces identifiées, les FISS implémentent les deux fonctions de sécurité suivantes :

- **Chiffrement et Intégrité** des échanges entre le progiciel et le serveur IMARS. Le protocole de chiffrement utilisé par les FISS est TLS version 1.0. Ce chiffrement intervient dans les échanges entre les FISS et le serveur IMARS : un tunnel SSL/TLS est créé à la première connexion entre les FISS et le serveur IMARS.
- **Authentification** mutuelle entre les FISS et le serveur IMARS : les FISS utilisent le certificat et la clé privée de la carte CPS (présents dans le HSM de la carte) pour s'authentifier auprès de l'ordonnanceur IMARS et ouvrir le tunnel SSL/TLS. De même, le serveur IMARS dispose d'un certificat et d'une clé privée associée.

De plus**,** un mécanisme de défense en profondeur assure l'intégrité des composants FISS (**archives JAR** et des **fichiers en code natif).** L'ensemble des classes JAVA utilisé dans les FISS est encapsulé dans des archives JAR signées par un certificat SESAM-Vitale. De même, un contrôle d'intégrité est réalisé sur les librairies JNI. Ce contrôle d'intégrité offre l'assurance que les FISS ne sont pas modifiés par un attaquant.

La disponibilité des FISS (protection contre l'effacement) n'est pas un objectif de sécurité.

Les **fichiers de configuration des FISS** et les **données du progiciel de santé** doivent être protégés par le système d'exploitation du poste PS, lequel est soumis aux recommandations de sécurité du GIE SESAM-Vitale mises en œuvre par les éditeurs de progiciels.

Remarque :

Les informations de révocation des certificats seront publiées via les éditeurs de progiciel. En cas de compromission du certificat du serveur IMARS, le service sera suspendu.