

## SOLUTION MESSAGERIE SÉCURISÉE SUR INTERNET

### I. DEFINITION

Le produit "solution de messagerie sécurisée sur internet" offrira à tout Professionnel de Santé (PS) possédant une Carte de Professionnel de Santé (CPS) valide, et abonné d'une offre "réseau" de Cegetel.rss ou de France Télécom, les fonctions de signature électronique et de chiffrement de ses messages électroniques échangés avec un autre Professionnel de Santé sur internet.

Ce produit s'appuiera sur une solution technique conçue et développée conjointement par France Télécom et Cegetel.rss, dont la réalisation a été confiée à Sagem.

### II. DESCRIPTION SYNTHETIQUE DE L'OFFRE

#### *II.1 Les fonctions de base vues par l'utilisateur final*

Le PS utilisera ce service à travers l'interface de son logiciel de messagerie habituel (les messageries supportées sont Outlook Express, Netscape Messenger, Outlook 97, Outlook 98, Outlook 2000, Exchange, Lotus Notes v5).

L'intégration dans la messagerie (faite à l'aide d'une extension appelée « plug-in ») se matérialisera sous la forme de deux boutons supplémentaires dans la barre d'outil, ainsi que deux choix supplémentaires dans le menu Action. Les boutons permettront de :

- Signer le message à émettre,
- Signer / chiffrer le message à émettre.

#### Emission de messages nouveaux

Lors de la création d'un nouveau message, le PS spécifiera les fonctions de sécurité souhaitées à l'aide des boutons ad-hoc.

- quand il activera la fonction "signer le message à émettre", le produit vérifiera la présence de la CPS, demandera au PS d'entrer ses 4 "digits", transmettra le message en confirmant qu'il a été signé, et l'archivera dans cet état "signé" dans l'espace "éléments envoyés" de son logiciel de messagerie.
- quand il activera la fonction "signer / chiffrer le message à émettre", le produit :
  - vérifiera la présence de la CPS, et demande au PS d'entrer ses 4 "digits"
  - vérifiera la disponibilité des certificats des destinataires :
    - s'ils ne sont pas disponibles, signalera au PS la marche à suivre pour les obtenir, et lui proposera de sauvegarder provisoirement son message en l'état
    - s'ils sont disponibles : transmettra le message en confirmant qu'il a été signé et chiffré, et l'archivera dans cet état "signé/chiffré" dans l'espace "éléments envoyés" de son logiciel de messagerie.

#### Emission (retransmission) de messages reçus

Dans ce cas, le PS n'aura pas à activer les fonctions de sécurité - celles-ci seront enchaînées automatiquement par le produit, qui se conformera au niveau de sécurité du message initial.

Ensuite tout s'enchaînera comme au paragraphe précédent.

## Réception de messages

Nb : ce chapitre décrit la réception de messages sécurisés émis par un autre utilisateur de la "messagerie CPS". Les cas d'échanges avec d'autres catégories d'utilisateurs sont décrits dans un chapitre séparé.

Les messages seront présentés à l'utilisateur dans son environnement habituel de messagerie. Lors de l'ouverture d'un message sécurisé, le produit prendra la main et vérifiera tout d'abord les informations de sécurité contenues dans l'enveloppe (certificats, ...). Puis :

- Si l'enveloppe est signée (non chiffrée), le produit :
  - vérifiera la validité de la signature
  - confirmera à l'utilisateur la validité de la signature
  - rendra la main au logiciel de messagerie qui affichera le message
- Si l'enveloppe est signée/chiffrée :
  - vérifiera la validité de la signature
  - confirmera à l'utilisateur la validité de la signature
  - procédera au déchiffrement du contenu
  - rendra la main au logiciel de messagerie qui affichera le message

L'utilisateur visualisera son message normalement. Lorsqu'il fermera le message, celui sera conservé dans l'état de réception (signé ou signé/chiffré) ce qui permettra lors de l'ouverture suivante de re-vérifier à nouveau les informations.

Si l'utilisateur décide de répondre ou de transmettre le message, les fonctions de sécurité appliquées par défaut seront celles du message d'origine.

### *II.2 La Délégation de Messagerie Sécurisée*

La clé de confidentialité stockée sur le poste pourra être déléguée par le porteur de cette clé à un tiers. Il sera le seul à pouvoir déléguer cette utilisation. La procédure mise en place nécessitera l'intervention du porteur et du bénéficiaire de la délégation .

### *II.3 Echanges avec des utilisateurs non équipés*

Entre un utilisateur équipé de la solution et un interlocuteur doté d'outils SMIME, mais non équipé du module de messagerie sécurisée par CPS, l'interopérabilité se présentera comme suit :

- le chiffrement / déchiffrement fonctionnera dans les 2 directions
- la signature / vérification de signature ne fonctionnera dans aucune direction. Un message "impossible de vérifier la signature" sera affiché.

## **III. AVANTAGES DE LA SOLUTION DEVELOPPEE**

Les avantages de cette solution se déclinent selon 3 axes :

- les services offerts aux Professionnels de Santé
- le niveau de sécurité
- les aspects industriels

### *III.1 Services offerts aux Professionnels de Santé*

- Cette solution offre tout d'abord les services de base de la messagerie sécurisée :
  - la signature électronique, qui permet au destinataire de s'assurer de l'identité de l'expéditeur, ainsi que de l'intégrité du message transmis
  - le chiffrement, qui rend le message illisible pour des tiers
- mais elle intègre des besoins particuliers au monde de la Santé, liées notamment à l'urgence médicale :
  - possibilité pour un PS de déléguer à un confrère la lecture des messages chiffrés, ce qui sera utile en médecine de ville dans des cas de remplacement, ou de jours de garde au sein d'un même cabinet, mais aussi au sein des services hospitaliers conformément à leurs organisations
  - mode de fonctionnement dégradé, permettant là encore de prendre connaissance des messages, même en cas de perte ou de panne de la carte CPS

### *III.2 Niveau de sécurité*

- la solution intègre tout d'abord les meilleurs dispositifs de sécurité sur l'Internet. En standard elle fonctionne en chiffrement 128 bits.
- de plus, cette solution apporte quatre atouts essentiels par rapport aux solutions banalisées sur Internet :
  - elle est étroitement associée à la carte CPS, dans sa version actuelle (la CPS2), et dans sa version future (la CPS2bis). Or la CPS est destinée à devenir le passeport électronique des PS leur permettant d'avoir accès à de nombreuses applications avec une identification claire en tant que PS.
  - elle met en œuvre une sécurisation supplémentaire qui consiste à utiliser la CPS comme “ clé d'accès ”, puis à terme, comme support des clés de confidentialité utilisées,
  - elle utilise des bi-clés différents pour chaque usage : chiffrement, signature.
  - elle repose sur des Autorités de Certification déjà utilisées par les deux opérateurs dans le domaine de la santé puis, dès que cette solution sera disponible, sur l'Autorité de certification que mettra en place le GIP CPS.

### *III.3 Aspects industriels*

- la solution est développée par un industriel (SAGEM) reconnu dans le domaine de la sécurité.
- elle repose sur des standards établis et largement adoptés de l'Internet :
  - certificats X509 V3,
  - listes de révocations CRL V2,
  - annuaire X500, LDAP V2, LDAP V3,
  - algorithmes de chiffrement DES, 3xDES, RC2, RC4, ACR (128 bits),
  - algorithmes de signature DSA et RSA (PKCS#1),
  - algorithmes de condensé MD2, MD5 et SHA1,
  - algorithmes d'échange de clés Diffie-Hellman et RSA,
  - messagerie sécurisée SMIME V3,
- elle offre aux éditeurs de logiciels "santé" une API (Application Programming Interface) simple