



La solution commune Cegetel.rss - France Télécom de messagerie sécurisée sur internet pour le monde de la santé

L'ACCORD

France Télécom et Cegetel.rss ont décidé d'harmoniser leurs solutions de sécurisation en matière de messagerie afin d'assurer l'interopérabilité des échanges électroniques dans le monde de la santé.

L'objectif des deux opérateurs est de permettre l'échange de messages signés et chiffrés entre utilisateurs de leurs réseaux respectifs. Qu'ils soient hospitaliers ou libéraux, tous les Professionnels de Santé raccordés à ces différents réseaux pourront désormais échanger en toute sécurité des informations confidentielles comme des résultats d'examen ou des éléments de dossier médical.

Des discussions ont eu lieu avec les institutions pour assurer une cohérence entre la démarche commune de Cegetel et France Télécom et leurs projets de déploiement des cartes de la famille CPS. Une concertation étroite avec le GIP-CPS permet de garantir que la solution Cegetel.rss-France Télécom sera conforme aux spécifications du GIP. Le ministère a assuré Cegetel.rss et France Télécom de son soutien, dans une démarche qui ne peut que faire progresser les échanges et la sécurité dans le monde de la Santé. Il a par ailleurs réaffirmé le rôle éminent et obligatoire que la CPS joue et jouera dans ce secteur.

L'OUTIL

En pratique, cet accord se traduit par l'intégration d'un outil de messagerie commun dans les offres proposées aux utilisateurs. Il place la carte CPS au cœur du système de sécurité dans le domaine de la santé puisque les Professionnels pourront l'utiliser pour sécuriser leurs messages.

L'outil, choisi par France Télécom et Cegetel.rss sur la base de spécifications communes, a été développé par la société Sagem, choisie à la suite d'une étude détaillée de toutes les réponses à la consultation à laquelle plusieurs industriels ont répondu. C'est l'industriel qui offrait la meilleure réponse, sur les plans techniques et économiques, et pour les délais. Sagem a également une très bonne connaissance de la CPS.

Il est conçu pour utiliser les fonctionnalités de la Carte de Professionnel de Santé (CPS), délivrée par le Groupement d'Intérêt Public CPS, et respecte les critères d'homologation que celui-ci mettra en place. Dans la solution commune, les cartes de la famille CPS sont en effet utilisées comme un véritable passeport électronique qui garantira l'identité des porteurs.

Il est conforme aux standards de chiffrement en usage sur l'Internet et compatible avec les principaux systèmes de messagerie.

La solution de signature et de chiffrement (clefs de 128 bits) choisie en commun comporte deux volets:

- un logiciel de sécurisation de messagerie indépendant et autonome, qui s'interface avec les principaux clients de messagerie du marché,
- un ensemble d'API de haut niveau qui peuvent être intégrées dans des applications pré-installées sur le poste et qui permettent à ces applications de faire appel aux principales fonctions du logiciel de sécurisation

Le logiciel de sécurisation comporte bien entendu toutes les fonctions auxiliaires qui permettent de l'installer, de l'initialiser et de le gérer. Citons comme exemple d'opérations de gestion : la gestion des cartes, la gestion des certificats.

La solution est pleinement compatible, pour le chiffrement, avec d'autres solutions de chiffrement sans carte, sous réserve qu'elles respectent les standards SMIME et sous réserve également que les interlocuteurs disposent de leurs certificats de clé publique respectifs. Ceci signifie qu'un message chiffré par un professionnel de Santé avec la solution pourra être déchiffré par un destinataire doté d'outils SMIME ; réciproquement, un message chiffré par un expéditeur SMIME sera déchiffré par un professionnel de Santé doté de la solution.

En ce qui concerne la signature, la compatibilité ne sera pas totale avec la version actuelle de la CPS (la CPS2) qui utilise un algorithme particulier. Cela signifie que le destinataire non équipé de la solution ne pourra pas reconnaître la signature du PS. Cette compatibilité sera retrouvée avec la version attendue de la CPS, dite CPS2bis.

LES AVANTAGES

Notre solution apporte trois atouts essentiels par rapport aux solutions banalisées sur Internet :

1. 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 " clés d'accès ", puis à terme, comme support des clés de confidentialité utilisées,
 - elle utilise des bi-clés différents pour chaque usage : chiffrement, signature.
2. 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.

Le mécanisme dit d'autorités de certification est une donnée fondamentale et trop souvent méconnue de la " robustesse " d'un système de protection des données.

Dans une première phase, les deux opérateurs utiliseront les autorités de certification qu'ils ont déjà mis en place et qu'ils utilisent pour leurs réseaux, RSS et Liberalis. Chaque Autorité de Certification mettra à disposition de tous les internautes un annuaire de certificats de ses abonnés

Dans une seconde phase, il sera possible bien entendu d'utiliser l'Autorité de Certification que prévoit de mettre en place le GIP CPS lorsqu'elle sera disponible.
3. elle répond également à des demandes exprimées par les PS, par l'intermédiaire de leurs instances comme les Conseils de l'Ordre, sur des fonctionnalités particulières 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 leur organisation
- mode de fonctionnement dégradé, permettant là encore de prendre connaissance des messages, même en cas de perte ou de défaillance de la carte CPS.

LES DELAIS

La première version a été livrée aux opérateurs fin janvier 2001 après recette chez le fournisseur. Une campagne de test sera organisée par les opérateurs et par Sagem : nous prévoyons d'effectuer ces tests tout au long du premier semestre 2001 : ces campagnes nous permettront de vérifier le fonctionnement de la solution, le fonctionnement entre utilisateurs des deux réseaux, le fonctionnement entre postes clients équipés de différents systèmes d'exploitation et enfin, le fonctionnement avec des postes clients équipés d'autres solutions, pourvu qu'elles respectent les standards exigés.

Une première expérimentation terrain, entre utilisateurs des deux réseaux, devrait se mettre en place après le Médec 2001.

La première commercialisation interviendra à partir du deuxième semestre 2001.

LES COUTS ET LA COMMERCIALISATION

Le développement de cette solution implique pour les deux opérateurs des investissements significatifs, de plusieurs millions de francs. Ces développements concernent en particulier :

- la mise en place des fonctionnalités correspondant à l'intégration de la CPS (2 et 2 bis),
- le développement de fonctionnalités que l'on ne trouve pas dans les produits existants (délégation, portabilité, existence de modes particuliers),
- le support d'un certain nombre de plates-formes et systèmes d'exploitation, ce qui n'est pas toujours le cas des outils existants,
- le financement des opérations d'homologation,
- le prix d'acquisition des licences,

Une fois terminée la phase de développement initiale, cette solution devra évoluer, que ce soit pour suivre les modifications de l'environnement ou pour enrichir ses fonctionnalités lorsque cela paraîtra nécessaire, au vu de l'expérience en exploitation.

Il est donc clair que cette solution a un coût comme tout service élaboré demandant des développements. Elle aura donc pour les clients un prix, qui est encore à l'étude.

Il faut simplement remarquer que la collaboration des deux principaux opérateurs a pour résultat de faire jouer les facteurs d'échelle et que le prix de la solution, pour les PS, en sera donc optimisé.

Le service de messagerie sécurisée sera proposé, sous forme payante, par chacun des deux opérateurs à l'ensemble de ses clients professionnels de Santé, abonnés soit au RSS soit à une solution France Télécom (Wanadoo Santé, Liberalis, Oléane Santé).

Les conditions tarifaires précises seront déterminées par chaque opérateur.

Les deux opérateurs pourront passer des accords de distribution avec d'autres acteurs : en effet, notre souhait commun est bien entendu de faire disposer ce produit de canaux de distribution aussi larges que possible.

Les professionnels de Santé qui utilisent les services d'un autre opérateur devront s'adresser à celui-ci pour savoir s'il distribue ce service, et dans ce cas, pour connaître ses modes de distribution et ses conditions tarifaires.

CONCLUSION

Au moment où les échanges électroniques de données confidentielles se développent dans le domaine de la santé, France Télécom et Cegetel.rss, en proposant à leurs abonnés une solution commune, performante et sûre, apportent une réponse à la mesure des enjeux de ce secteur.

France Télécom et Cegetel.rss partagent l'objectif d'aider les Professionnels de Santé à mieux exploiter le fort potentiel de l'Internet au service de leur pratique. La messagerie sécurisée est apparue comme le socle de cette démarche, dans la mesure où elle permet d'ores et déjà d'échanger des avis médicaux, des résultats d'analyse, des parties de dossiers patients.

A la lumière de ce premier résultat concret, France Télécom et Cegetel.rss pensent être en mesure d'apporter à leurs clients d'autres solutions favorisant les échanges et le partage en toute sécurité dans le monde de la Santé : les deux opérateurs examinent ensemble ces possibilités.

Le succès de ces actions dépend certes d'opérateurs comme France Télécom et Cegetel.rss, qui maîtrisent ces sujets, mais aussi du contexte réglementaire, qui doit favoriser ces orientations, et du comportement des utilisateurs eux-mêmes, qui doivent comprendre l'intérêt de partager des normes et des règles communes.

Contact presse Cegetel.rss
Patrice Delefosse – 01 71 77 21 85
patrice.delefosse@cegetel.fr
www.cegetel.rss.fr

Contact presse France Télécom
Jean-Claude Turbant – 01 55 54 00 72
jeanclaude.turbant@francetelecom.com
www.francetelecom.com