

## SYNTHESE DE L'ETUDE COMPARATIVE DES PRINCIPAUX OUTILS D'ECHANGE DE DONNEES A L'USAGE DES PROFESSIONNELS DE SANTE



2 septembre 2007

## Les textes juridiques et réglementaires\*

← **La Loi n°2004-810 du 13 août 2004 relative à l'assurance maladie** (repris de l'Article L.1110-4 de la loi n°2002-303 du mars 2002, dite « loi Kouchner »)

Afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique, comme leur transmission par voie électronique entre professionnels, sont soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la Commission nationale de l'informatique et des libertés. Ce décret détermine les cas où l'utilisation de la **carte de professionnel de santé** mentionnée au dernier alinéa de l'article L. 161-33 est obligatoire.

\* : liste non exhaustive

### ← **L'ordonnance n°2005-1516 du 8 décembre 2005**

Citons la Direction générale de la modernisation de l'Etat :

« Cette ordonnance... introduit la notion de **Référentiel Général d'Interopérabilité** (RGI) dont l'objet est de fixer les règles techniques permettant d'assurer l'interopérabilité de tout ensemble de moyens destinés à **élaborer, traiter, stocker ou transmettre** des informations faisant l'objet d'échanges par voie électronique avec une autorité administrative. »

Article 9-I : Un **référentiel général de sécurité** fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions **d'identification, de signature électronique, de confidentialité et d'horodatage...**

### ← **Le « décret confidentialité » n°2007-960 du 15 mai 2007**

**L'utilisation de la carte CPS est obligatoire** (Art. R. 1110-3) pour tout accès aux informations médicales à caractère personnel conservées sur support informatique ou pour leur transmission par voie électronique.

- il s'agit bien *stricto sensu* de la carte CPS (ou CPx) et non pas d'une carte hébergeant des certificats CPS.
- la CPS doit être utilisée pour accéder aux données de santé personnelles, immédiatement à partir de la publication du décret (15 mai 2007) pour les libéraux. Un délai de 3 ans est consenti aux établissements de santé.

Tous les professionnels de santé doivent se **mettre en conformité avec des référentiels de sécurité** définis par arrêtés ministériels dans **un délai d'un an après la publication desdits arrêtés**. (Art. R. 1110-1 et R.1110-2).

## ← Le RGI

- Est déjà publié.
- L'utilisation de S/MIME est obligatoire pour la sécurisation de la messagerie électronique.

## ← Le RGS

- [http://synergies.modernisation.gouv.fr/rubrique.php?id\\_rubrique=159](http://synergies.modernisation.gouv.fr/rubrique.php?id_rubrique=159)
- « Une version de travail du RGS est en cours de consultation dans les Ministères. La consultation sera élargie pendant le 2ème semestre 2007. »
- « Liste des documents référencés par le RGS : PRIS, FEROS types, etc... »
  - La PRIS V2.1 précise que la **signature** des données de Niveau \*\*\* doit être basée sur les **clés asymétriques** et les **certificats X.509 V3**.
  - Concernant l'**authentification** : « Les certificats, et les listes correspondantes de certificats révoqués (LCR),... doivent être conformes à la norme [X.509]. »

## ← Client de messagerie

- logiciel que l'on installe sur son poste de travail pour gérer ses courriers électroniques (création, envoi, réception, manipulation...).

## ← Webmail

- interface Web qui permet d'envoyer, de recevoir et de consulter ses messages à partir d'un navigateur.

## ← « Mode relais » ou « mode intégré »

- Mode relais : un dispositif s'intercale entre le logiciel de messagerie et Internet afin de contrôler l'émission et la réception de l'ensemble des messages de la boîte aux lettres sécurisée.
- Mode intégré : c'est le client de messagerie qui assure l'émission et la réception des messages à destination ou en provenance d'Internet. Les fonctions de sécurité sont directement intégrées dans le client de messagerie.

## ← API

- Interface normalisée permettant à un logiciel de faire appel aux fonctions d'un autre programme

### ← OSM : Outil de Sécurisation des Messageries

- Nom dédié aux messageries sécurisées qui utilisent la carte CPS et qui ont passé avec succès les tests du référentiel d'homologation du GIP CPS.
- [https://editeurs.gip-cps.fr/index.php?page=homologation\\_OSM](https://editeurs.gip-cps.fr/index.php?page=homologation_OSM).

### ← Intérêt de l'homologation

- Garantir l'**interopérabilité** entre les produits (utilisation de S/MIME V3)...
- En s'appuyant sur les certificats du GIP (Autorité de Certification reconnue pour le monde de la santé en France)

### ← Les OSM

- Garantissent l'identité et la qualité du signataire
- Garantissent l'inaltérabilité du message
- Ainsi que la confidentialité du message
- Permettent la continuité de service (possibilité de déchiffrer un message en cas d'urgence). La clé de confidentialité est partageable sur un même poste par délégation à des personnes habilitées qui doivent utiliser leur carte CPx.

- ← Apicrypt et Apimail d'APICEM,
- ← Docteur Net CPS de Medsys,
- ← EASYCRYPT.net d'Enovacom,
- ← MMUA d'Etiam,
- ← PEPS du GCS SIS-RA,
- ← Security Box® Mail d'Arkoon Network Security,
- ← Sermentis MMS du Réseau santé social,
- ← Sign&mail d'Ilex,
- ← S.M.M. de Cegedim Logiciels Médicaux.

Comparatif 1/2 page 1/2	Apimail (Apicrypt)	Apimail (S/MIME)	Docteur Net CPS	Sermentis	Security Box® Mail
Webmail/API/client de messagerie	Client de messagerie et Webmail (avec Apiwebmail)	Client de messagerie	Client de messagerie	Client de messagerie	Client de messagerie
Plates-formes supportées	Mac, PC, linux AIX, SCO-Unix, Open VMS, AS 400	PC	PC	PC	PC
Degré d'interopérabilité avec les autres solutions	← Avec Easycrypt pour le chiffrement uniquement, ← Aucun avec les OSM	Oui : avec tous les OSM et toutes les messageries supportant S/MIME et X.509	Oui : avec tous les OSM et toutes les messageries supportant S/MIME et X.509	Oui : avec tous les OSM et toutes les messageries supportant S/MIME et X.509	Oui : avec tous les OSM et toutes les messageries supportant S/MIME et X.509
Facilité d'installation	+++		++ <sup>1</sup>	++ <sup>1</sup>	++ <sup>1</sup>
Facilité d'utilisation	+++		+++	+++	+++
Conformité à la législation	Oui mais <sup>3</sup>	Oui	Oui	Oui	Oui
Intégration dans les LGC	Intégré à une trentaine de LGC dont Hellodoc, Médistory, Mégabaze	Non	HPRIM-Net : interface fine et spécifique à la biologie avec les LGC	HPRIM-Net : interface fine et spécifique à la biologie avec les LGC	Non

Comparatif 1/2 page 2/2	Apimail (Apicrypt)	Apimail (S/MIME)	Docteur Net CPS	Sermentis	Security Box® Mail
Signature électronique	Oui, avec CPS mais signature propriétaire	Oui	Oui	Oui	Oui
Validé HPRIM-Net <sup>2</sup>	Non	Non	Oui, en émission et en réception	Oui, en émission et en réception	Non
Tarifs	← Libéraux : 66 €/an, (non dégressif) ← Hôpitaux/réseaux : - mensuel : 220 € par établissement et 44 € par poste si clients lourds individuels - annuel : 264 € en mode Proxy, coût du proxy 2 600 € HT (achat, installation, maintenance 2 ans sur site comprise)		← Libéraux : - frais d'ouverture : 40 € - abonnement annuel : 75 € Tarif dégressif pour un grand nombre de licences ← Même tarif pour les hôpitaux et réseaux par poste client	← Libéraux : - frais d'ouverture : 40 € TTC - abonnement mensuel : 7 € TTC (intègre le support d'HPRIM-Net) Dégressivité en fonction du nombre d'abonnements	← Libéraux : - frais d'ouverture : 105 € HT - abonnement annuel : 26 € HT Dégressivité en fonction du nombre d'abonnements ← Même tarif pour les hôpitaux et réseaux par poste client

Comparatif 2/2 page 1/3	EASYCRYPT.net	S.M.M.	Sign&mail	MMUA	PEPS
Webmail/API/client de messagerie	Webmail	Client de messagerie	Client de messagerie	API	Webmail
Plates-formes supportées	Mac, PC	PC	Mac, PC	Mac, PC	Mac, PC
Degré d'interopérabilité avec les autres solutions	Oui : ↳ Avec tous les OSM et toutes les messageries supportant S/MIME et X.509 ↳ Avec Apicrypt pour le chiffrement uniquement	Oui : ↳ Avec tous les OSM et toutes les messageries supportant S/MIME et X.509	Oui : ↳ Avec tous les OSM et tout client et tout serveur compatible S/MIME/POP3	Oui : les messageries développées avec MMUA sont homologables OSM et interopérables avec les autres OSM et toutes les messageries S/MIME et X.509	Non
Facilité d'installation	++ <sup>1</sup>	++ <sup>1</sup>	++ <sup>1</sup>	++ <sup>1</sup>	+++
Facilité d'utilisation	+++	+++	Non testé	Dépend des messageries ayant intégré le kit	+++
Conformité à la réglementation/législation	Oui	Oui	Oui	Oui	Oui

Comparatif 2/2 page 2/3	EASYCRYPT.net	S.M.M.	Sign&mail	MMUA	PEPS
Intégration dans les LGC	EASYCRYPT.net utilise les interfaces existantes des LGC sachant importer des flux au format HPRIM médecin	↳ Intégré aux logiciels CLM : Crossway Ville, Doc'Ware, Cardiolite et la nouvelle version de MediClick, ↳ En cours d'intégration dans RM Medi+ 4000 (octobre 2007), ↳ Intégration dans Eglantine et Medigest (début 2008)		↳ Editeurs cliniques (B2) : Actibase, Cegi Santé, Hospéa, etc., ↳ Editeurs laboratoires (HPRIM-Net) : Selarl Interlabo, ORNIS, Euro-sys, Institut Pasteur de Lille, etc., ↳ Divers : SNR, Logicmax, Corwin, Micro 6, Institut Gustave Roussy, etc.	↳ Possibilité d'alimentation en automatique via API et service web sécurisé, ↳ Intégré à Hellodoc et à des systèmes hospitaliers (coordination ville – hôpital)
Signature électronique	Oui	Oui	Oui	Oui	Non
Validé HPRIM-Net <sup>2</sup>	Oui, en émission et en réception	Oui, en réception	Non	Oui, en émission et en réception	Non

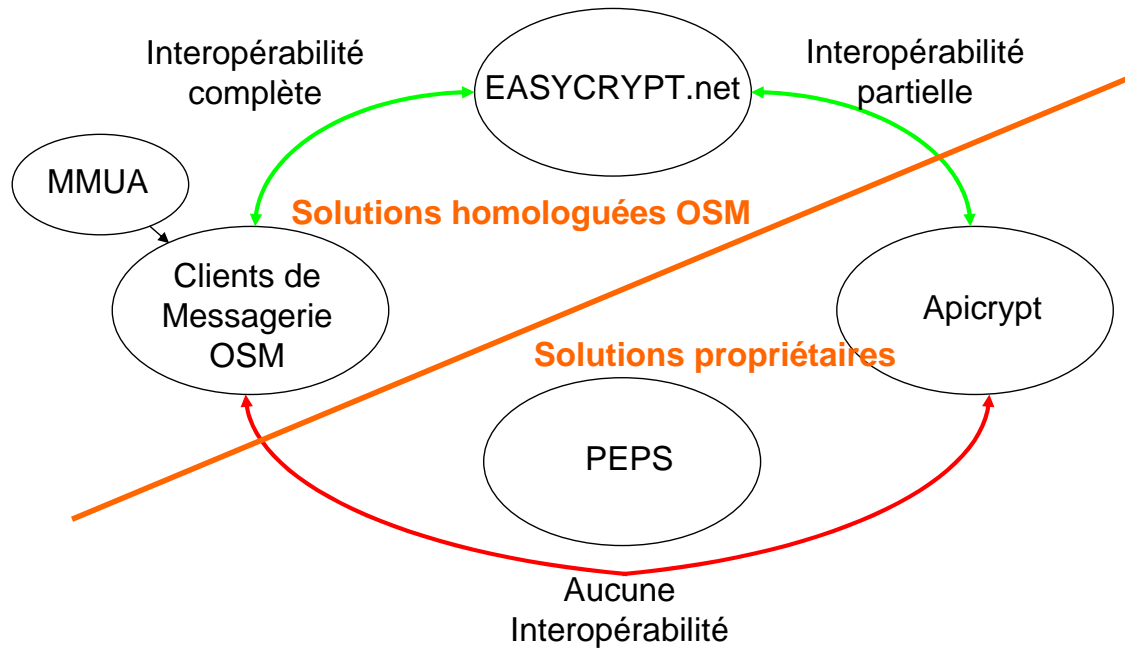
Comparatif 2/2 page 3/3	EASYCRYPT.net	S.M.M.	Sign&mail	MMUA	PEPS
Tarifs	<p>← 60 € TTC/an : inclut la réception en HPRIM-Net.</p> <p>← En option, 40 € TTC pour les frais de mises en œuvre incluant le support téléphonique lors de la première utilisation, l'enregistrement et la formation par téléphone</p>	<p>← La version « autonome » de la messagerie est gratuite si elle est packagée avec des écrans de veille publicitaires,</p> <p>← Intégrée aux logiciels du groupe, S.M.M. est gratuite dans les mêmes conditions Sinon c'est environ 60 €/an</p>	Non disponible	<p>A Titre indicatif, le tarif de vente du Kit MMUA à un éditeur de logiciel de cabinet de médecins généralistes est de 1000 € HT (correspondant au support de second niveau à l'intégration) et de 150 € HT par poste installé. Pour tout autre contexte, consulter Etiam.</p>	<p>← Un forfait de maintenance annuelle pour l'ensemble des utilisateurs d'un réseau ou d'un établissement (1 000 € HT),</p> <p>← Pas de licence individuelle</p>

- 1 :** difficile d'attribuer autre chose qu'une « note médiane ». Les OSM sont faciles à installer sur un poste vierge. L'installation peut être plus délicate sur un poste sous-dimensionné ou sur un poste ayant déjà beaucoup de choses d'installées, en particulier en matière de télétransmission de feuille de soins, par exemple des API CPS obsolètes. Cette remarque est également vraie pour des solutions non homologuées OSM par le GIP CPS mais qui utilisent la carte CPS (pour l'authentification, pour la signature...). La facilité d'installation peut donc varier de « + » à « +++ ».
- 2 :** attention, depuis la publication du décret « confidentialité » du 15 mai 2007, les professionnels de santé libéraux ne devraient utiliser que les solutions qui supportent la recommandation HPRIM-Net et avec la carte CPS. Ils devraient refuser l'utilisation avec des certificats autocertifiés ou des certificats X.509 hors CPS. De même, ces solutions ne devraient plus accepter d'authentification autre que celle réalisée avec la carte CPS (sauf en mode secours).
- 3 :** Apicrypt n'est pas actuellement, à proprement parler, non-conforme à la législation. Car si le décret « confidentialité » publié le 15 mai dernier indique bien ce vers quoi il faut tendre en terme de sécurité, les décrets incorporant les référentiels ne sont pas encore sortis. Mais l'on peut, dès à présent, se référer à ce qui a déjà été publié comme la PRIS V2.1.

En revanche, le RGI (Référentiel Général d'Interopérabilité) est déjà paru. Il est en cours d'adaptation pour le secteur de la santé. Il rend déjà obligatoire le support de standards comme S/MIME et son adaptation à la santé ne pourra aller à l'encontre des recommandations actuelles.

Nous pensons que l'APICEM sera amenée, tout en gardant ce qui fait sa force (c'est-à-dire des produits qui rendent un réel service médical) à faire évoluer son offre pour être conforme à la législation quand celle-ci sera officiellement publiée, comme l'APICEM l'a fait en prenant en compte les évolutions DMP.

Nous sommes en ce moment dans une phase transitoire : le décret « confidentialité » est publié, mais les décrets annexes (ceux des référentiels), ne le sont pas encore.



## Avantages-Inconvénients des outils

Outils d'échange en santé	Les points forts	Les points faibles
<b>Les clients de messagerie OSM</b>	<ul style="list-style-type: none"> <li>← Conformes à la législation française,</li> <li>← Conformes aux normes techniques publiques, internationales, Interopérables,</li> <li>← Homologués GIP CPS et audités par un organisme indépendant</li> </ul>	<ul style="list-style-type: none"> <li>← Potentiellement difficiles à installer,</li> <li>← Pas toujours intégrés aux logiciels<sup>1</sup>,</li> <li>← Pas multiplate-forme<sup>2</sup>,</li> <li>← Encore peu déployés sur le terrain</li> </ul>
<b>Apicrypt</b>	<ul style="list-style-type: none"> <li>← Expérience terrain,</li> <li>← Facilité de déploiement,</li> <li>← Intégration aux LGC,</li> <li>← Service médical rendu,</li> <li>← Nombre d'utilisateurs,</li> <li>← Multiplate-forme</li> </ul>	<ul style="list-style-type: none"> <li>← Pas de signature électronique CPS « S/MIME »,</li> <li>← Interopérabilité partielle avec EASYCRYPT.net,</li> <li>← Pas d'interopérabilité avec les clients de messageries homologuées,</li> <li>← Conforme à la législation à voir<sup>3</sup></li> </ul>
<b>Le Webmail OSM</b>	<ul style="list-style-type: none"> <li>← Conforme à la législation française,</li> <li>← Conforme aux normes techniques publiques, internationales, Interopérable,</li> <li>← Homologué GIP CPS et audité par un organisme indépendant</li> <li>← Nombre d'utilisateurs</li> </ul>	<ul style="list-style-type: none"> <li>← Non intégré aux logiciels métier,</li> <li>← Nécessité d'être connecté pour accéder aux données d'où une connexion permanente recommandée</li> </ul>
<b>La plate-forme régionale</b>	<ul style="list-style-type: none"> <li>← Plate-forme régionale dont la cible est d'être « prête » pour le DMP</li> </ul>	<ul style="list-style-type: none"> <li>← Messagerie conçue autour du partage plutôt que de l'échange,</li> <li>← Connexion permanente recommandée,</li> <li>← Manque la signature électronique,</li> <li>← Interopérable avec aucun autre outil</li> </ul>

- 1** : certaines solutions sont intégrées dans des LGC.
- 2** : l'arrivée du produit Sign&mail, en cours d'homologation OSM par le GIP CPS, va rendre, fort heureusement, ce critère non valide. En effet, il suffit d'une solution disponible sur le marché pour que ce facteur tombe, toutes les autres solutions OSM étant par nature interopérables avec cette solution. De plus, la sortie du décret « confidentialité » le 15 mai dernier a donné un signal fort au marché : il a indiqué la direction vers laquelle devaient se diriger les éditeurs. Plusieurs éditeurs d'OSM envisagent de développer une version Macintosh.
- 3** : confer Note 3, diapositive 13

- ← **Apicrypt**
- ← **Client de messagerie OSM**
  - Scénario 1 : Docteur Net CPS
  - Scénario 2 : plusieurs clients de messagerie OSM (préférés par KOÏRA pour tirer partie des avantages de chaque solution)
- ← **EASYCRYPT.net**
- ← **PEPS**
  - Ou DPPR

\* : par ordre alphabétique des produits

- ← **Autocertification** ou certificat autosigné : dans le cas de l'autocertification, c'est l'utilisateur du certificat qui est en-même temps producteur de son certificat, sans faire référence à un tiers de confiance.
- ← **CPS (Carte de Professionnel de Santé)** : carte à microprocesseur distribuée par le Groupement d'Intérêt Public "CPS". Cette carte contient dans sa puce, deux certificats, l'un de signature, l'autre d'authentification.
- ← **CPx** : sigle générique désignant une carte de la famille CPS (CDE, CPE, CPA, CPF).
- ← **GIP "CPS"** ([www.gip-cps.fr](http://www.gip-cps.fr)) : le Groupement d'Intérêt Public "Carte de Professionnel de Santé", créé en 1993, a pour mission depuis 1996 de concevoir, distribuer et promouvoir l'usage de la carte CPS et de ses services associés. Ceci, afin de garantir la sécurité et la confiance des échanges et du partage des données médicales au sein du système de santé, quels que soient le réseau utilisé, l'environnement informatique.

- ← **HPRIM-Net** : cette recommandation permet l'échange de fichiers H.PR.I.M. par messagerie sécurisée. La transmission de fichiers H.PR.I.M. se fait par échange de certificats entre correspondants.
- ← **LGC** : Logiciel de Gestion de Cabinet.
- ← **S/MIME (Secured Multipurpose Internet Mail Extension)** : c'est le protocole de messagerie sécurisée conforme à la norme X509. S/MIME v3 a été défini par l'IETF.
- ← **Spam** : remplissage délibéré d'une boîte aux lettres par l'envoi de messages électroniques non sollicités.
- ← **X.509** : la norme ITU-T (International Telecommunications Union-T) des certificats. X.509 v3 désigne les certificats comportant ou pouvant comporter des extensions. Le certificat X.509 est attaché à une seule adresse de messagerie.