

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



31 octobre 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
- « 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.

← 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.

- ← Apimail (Apicrypt) d'APICEM, dit « Apicrypt »,
- ← Apimail (S/MIME) d'APICEM,
- ← Docteur Net CPS de Medsys,
- ← EASYCRYPT.net d'Enovacom,
- ← MMUA d'Etiam,
- ← Security Box® Mail d'Arkoon Network Security,
- ← Sermentis MMS du Réseau santé social,
- ← Sign&mail d'Ilex,
- ← S.M.M. de Cegedim Logiciels Médicaux.

← Outils déjà homologués OSM par le GIP CPS

- Apimail (S/MIME),
- Docteur Net CPS,
- EASYCRYPT.net,
- MMUA,
- Security Box® Mail,
- Sermentis MMS.

← Outils en cours d'homologation OSM par le GIP CPS

- Sign&mail,
- S.M.M.

← Outil non homologable OSM par le GIP CPS

- Apimail (Apicrypt).

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-Uinx, 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	+++	++ ¹	++ ¹	++ ¹	++ ¹
Facilité d'utilisation	+++	+++	+++	+++	+++
Conformité à la législation	Oui mais ³	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 ²	Non	Non	Oui, en émission et en réception	Oui, en émission et en réception	Non
Tarifs	<p>← Libéraux : 66 €/an, (non dégressif)</p> <p>← Hôpitaux/réseaux :</p> <ul style="list-style-type: none"> - 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) 	Non fournis (nécessite l'achat d'une licence m-secure d'Etiam)	<p>← Libéraux :</p> <ul style="list-style-type: none"> - frais d'ouverture : 40 € - abonnement annuel : 75 € <p>Tarif dégressif pour un grand nombre de licences</p> <p>← Même tarif pour les hôpitaux et réseaux par poste client</p>	<p>← Libéraux :</p> <ul style="list-style-type: none"> - frais d'ouverture : 40 € TTC - abonnement mensuel : 7 € TTC (intègre le support d'HPRIM-Net) <p>Dégressivité en fonction du nombre d'abonnements</p>	<p>← Libéraux :</p> <ul style="list-style-type: none"> - frais d'ouverture : 105 € HT - abonnement annuel : 26 € HT <p>Dégressivité en fonction du nombre d'abonnements</p> <p>← Même tarif pour les hôpitaux et réseaux par poste client</p>

Comparatif 2/2 page 1/3	EASYCRYPT.net	S.M.M.	Sign&mail	MMUA
Webmail/API/client de messagerie	Webmail	Client de messagerie	Client de messagerie	API
Plates-formes supportées	Mac, PC	PC	Mac, PC	Mac, PC
Degré d'interopérabilité avec les autres solutions	<p>Oui :</p> <ul style="list-style-type: none"> ← Avec tous les OSM et toutes les messageries supportant S/MIME et X.509 ← Avec Apicrypt pour le chiffrement uniquement 	<p>Oui :</p> <ul style="list-style-type: none"> ← Avec tous les OSM et toutes les messageries supportant S/MIME et X.509 	<p>Oui :</p> <ul style="list-style-type: none"> ← Avec tous les OSM et tout client et tout serveur compatible S/MIME/POP3 	<p>Oui : les messageries développées avec MMUA sont homologables OSM et interopérables avec les autres OSM et toutes les messageries S/MIME et X.509</p>
Facilité d'installation	++ ¹	++ ¹	++ ¹	++ ¹
Facilité d'utilisation	+++	+++	Non testé	Dépend des messageries ayant intégré le kit
Conformité à la réglementation/législation	Oui	Oui	Oui	Oui

Comparatif 2/2 page 2/3	EASYCRYPT.net	S.M.M.	Sign&mail	MMUA
Intégration dans les LGC	EASYCRYPT.net utilise les interfaces existantes des LGC sachant importer des flux au format HPRIM médecin	<ul style="list-style-type: none"> ↳ Intégré aux logiciels CLM : Crossway Ville, Doc'Ware, Cardiolite et la nouvelle version de MédiClick, ↳ En cours d'intégration dans RM Medi+ 4000 (octobre 2007), ↳ Intégration dans Eglantine et Medigest (début 2008) 		<ul style="list-style-type: none"> ↳ 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.
Signature électronique	Oui	Oui	Oui	Oui
Validé HPRIM-Net ²	Oui, en émission et en réception	Oui, en réception	Non	Oui, en émission et en réception

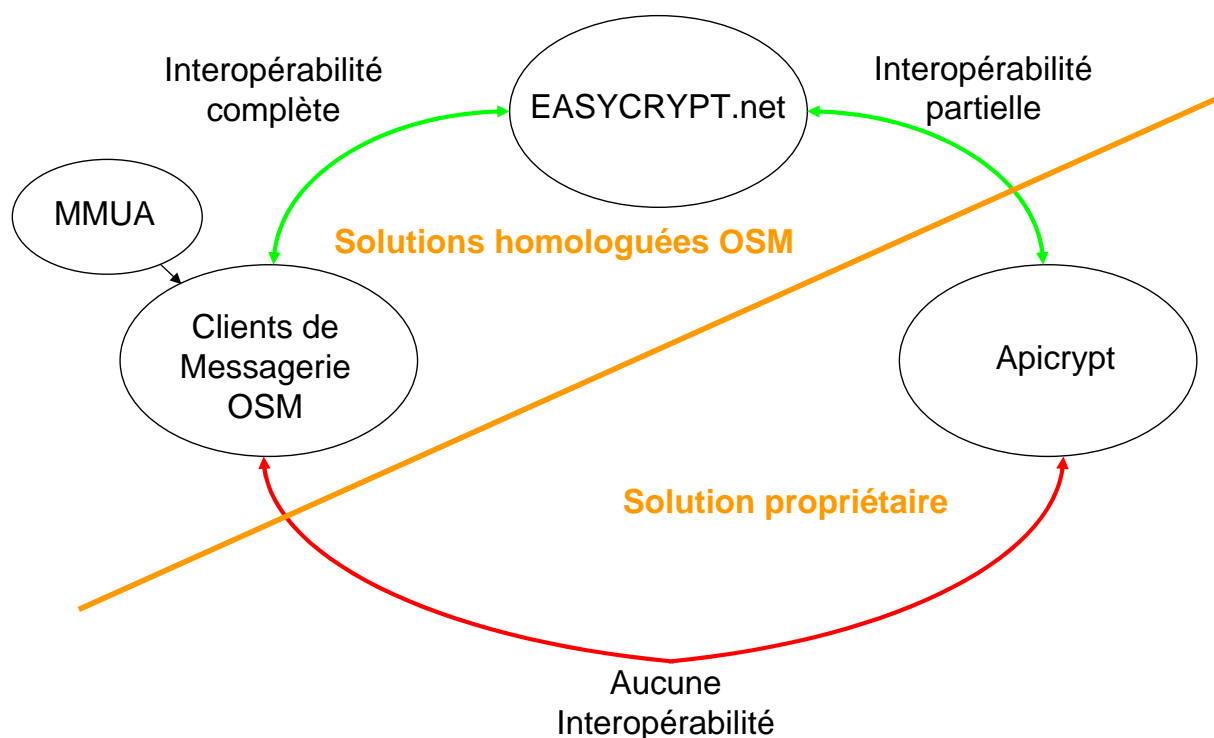
Comparatif 2/2 page 3/3	EASYCRYPT.net	S.M.M.	Sign&mail	MMUA
Tarifs	<ul style="list-style-type: none"> ↳ 60 € TTC/an : inclut la réception en HPRIM-Net. ↳ En option, 40 € TTC pour les frais de mises en œuvre incluant le support téléphonique lors de la première utilisation, l'enregistrement et la formation par téléphone 	<ul style="list-style-type: none"> ↳ La version « autonome » de la messagerie est gratuite si elle est packagée avec des écrans de veille publicitaires, ↳ Intégrée aux logiciels du groupe, S.M.M. est gratuite dans les mêmes conditions Sinon c'est environ 60 €/an 	Non disponible	Se renseigner auprès d'Etiam

- 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.



Outils d'échange en santé	Les points forts	Les points faibles
Les clients de messagerie OSM	<ul style="list-style-type: none"> ← Conformes à la législation française, ← Conformes aux normes techniques publiques, internationales, ← Interopérables, ← Homologués GIP CPS et audités par un organisme indépendant 	<ul style="list-style-type: none"> ← Potentiellement difficiles à installer, ← Pas toujours intégrés aux logiciels¹, ← Pas multiplate-forme², ← Encore peu déployés sur le terrain
Apicrypt	<ul style="list-style-type: none"> ← Expérience terrain, ← Facilité de déploiement, ← Intégration aux LGC, ← Service médical rendu, ← Nombre d'utilisateurs, ← Multiplate-forme 	<ul style="list-style-type: none"> ← Pas de signature électronique CPS « S/MIME », ← Interopérabilité partielle avec EASYCRYPT.net, ← Pas d'interopérabilité avec les clients de messageries homologuées, ← Conforme à la législation à voir³
Le Webmail OSM	<ul style="list-style-type: none"> ← Conforme à la législation française, ← Conforme aux normes techniques publiques, internationales, ← Interopérable, ← Homologué GIP CPS et audité par un organisme indépendant ← Nombre d'utilisateurs 	<ul style="list-style-type: none"> ← Non intégré aux logiciels métier, ← Nécessité d'être connecté pour accéder aux données d'où une connexion permanente recommandée

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

Sociétés ou Association

- Axilog,
- Cegedim Logiciels Médicaux,
- Groupe SEPHIRA,
- IMAGINE Editions,
- Prokov Editions,
- Association @medulo.

Les Logiciels de Gestion de Cabinet

Développements en cours (ou terminés)

Editeur de LGC	Proposera à terme une messagerie homologable OSM par le GIP CPS
Axilog	Oui , intégrée à AxiSanté
Cegedim Logiciels Médicaux	Oui , déjà développée. En cours d'homologation. Messagerie autonome ou intégrée aux principaux LGC de CLM
Groupe SEPHIRA	Oui . Docteur Net CPS est déjà commercialisé par SEPHIRA et EASYCRYPT.net le sera bientôt
IMAGINE Editions	Oui , en cours de développement. Cette nouvelle version d>HelloDoc Mail sera intégrée à HelloDoc
Prokov Editions	Oui , en cours de développement. Ce sera la nouvelle version de PeriCollect
Association @medulo	Non . Choix de la messagerie sécurisée entièrement laissé à l'utilisateur

Situation actuelle

- ← Vous utilisez un LGC d'**Axilog**, de **Sephira** ou **@medulo**
 - la facilité d'importer/exporter des messages dans votre LGC est identique quelle que soit la solution choisie, client de messagerie homologué OSM, Webmail homologué OSM, Apicrypt.
- ← Vous êtes équipé d'un logiciel de **CLM** ayant intégré **S.M.M.**, par exemple **Crossway**
 - il y a moins de manipulations (pas de « copier/coller ») à utiliser S.M.M. qu'Apicrypt ou n'importe quelle autre messagerie. La solution la plus conviviale est dans ce cas-là S.M.M.
- ← Vous êtes utilisateur d'**HelloDoc** ou **MédiStory**
 - à l'heure actuelle, Apicrypt est très bien intégré à ces LGC et est donc plus convivial que les autres messageries.
 - Mais, n'oubliez pas que ces deux éditeurs sont en cours de développement d'une messagerie homologable OSM qui sera intimement intégrée à leur logiciel et qui ne nécessitera alors aucune manipulation supplémentaire pour envoyer/recevoir des messages sécurisés.

- ← Les différents formats **H.PR.I.M.**
- ← **HPRIM-Net**
- ← **Sécurisation des messages de biologie**
- ← **Bioserveur**

← HPRIM santé

- V 2.2. Communication entre laboratoires

← HPRIM médecin

- Communication entre les laboratoires et les médecins. Versions 1, 2 et 3 actuellement utilisées

← HPRIM-Net

- Recommandation 1.0 : permet l'échange de n'importe quel type de fichiers HPRIM par messagerie sécurisée respectant

- S/MIME,
- Certificats X509 V3,
- Origine des certificats non imposée : opérateur tiers de confiance, voire l'utilisateur lui-même.

L'utilisation de la CPS n'est pas obligatoire

← Brouillage

- les données peuvent être brouillées : elles sont compactées puis chiffrées par un algorithme très léger suivant un mot de passe connu uniquement du laboratoire et du médecin.

← Apicrypt

- Les fichiers HPRIM sont chiffrés avec le moteur de chiffrement Apicrypt puis envoyés par messagerie aux médecins prescripteurs. Les fichiers HPRIM sont envoyés directement dans le corps du message et non en pièce jointe du message.

← HPRIM-Net

- Les fichiers sont envoyés par messagerie sécurisée utilisant des certificats X.509.

Echanges entre laboratoires et prescripteurs sans Bioserveur : les laboratoires doivent connaître avant l'envoi et pour chaque prescripteur, le format de fichier demandé et le mode de sécurisation utilisé par le PS.

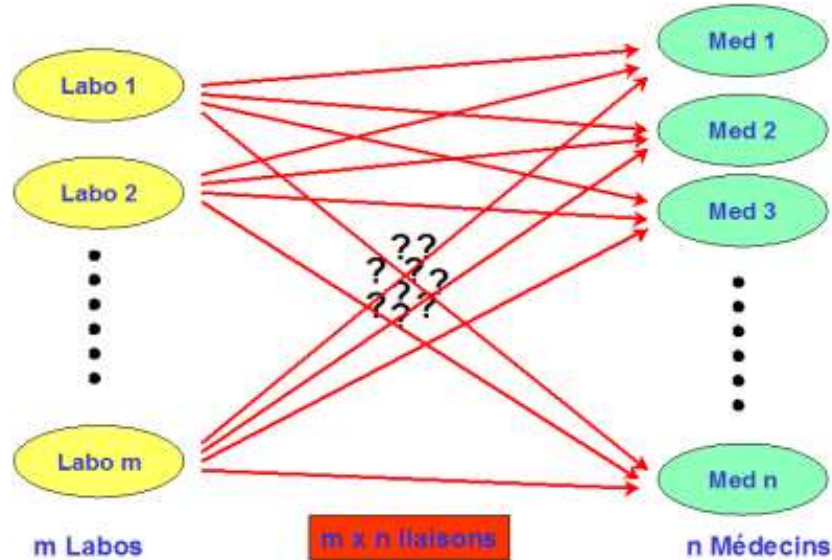
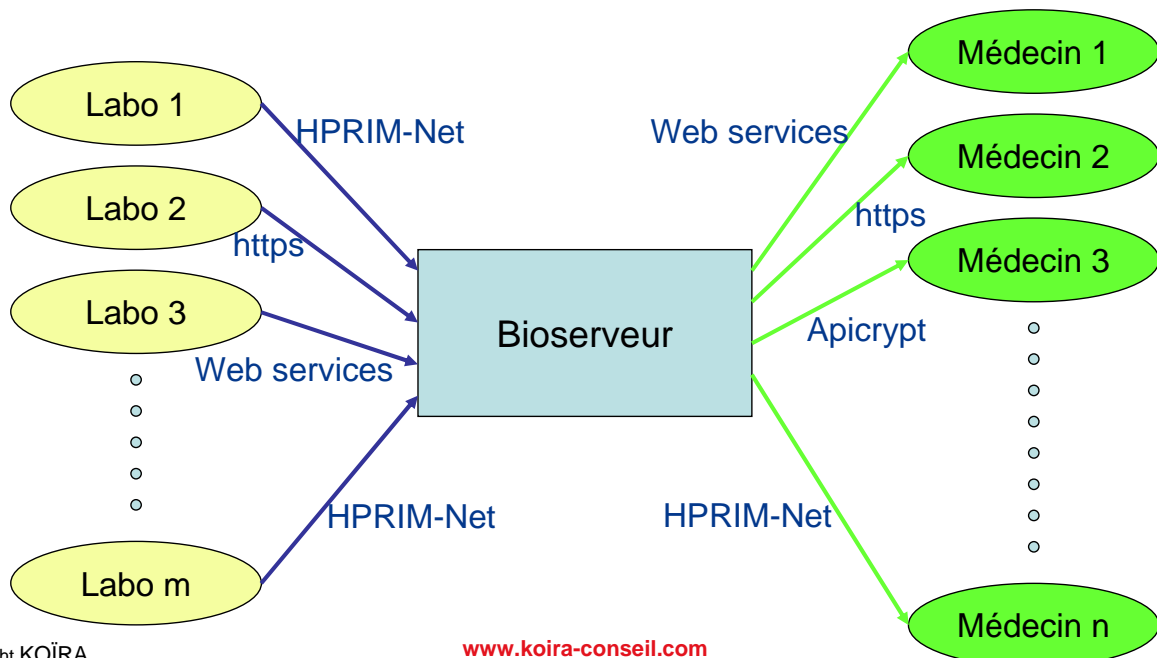


Schéma de principe de Bioserveur

Avec Bioserveur, le laboratoire envoie à Bioserveur dans le mode qui lui convient, hors Apicrypt (non autorisé), sans se soucier des demandes des prescripteurs. C'est Bioserveur qui se charge de mettre dans le bon format et d'envoyer au prescripteur avec la sécurisation que ce dernier aura choisie.



- ↳ Actuellement, seuls les comptes rendus d'imagerie sont envoyés aux médecins prescripteurs
- ↳ Les envois se font majoritairement par Apicrypt
- ↳ L'Avenant 24 de la Convention va inciter les radiologues à investir dans des solutions d'archivage d'images médicales
- ↳ L'intérêt
 - Avoir des images numériques « normalisées » et « sécurisées »
 - Pouvant être transmises à des correspondants
 - Pouvant alimenter le DMP

- ↳ Critères pertinents de choix
 - Interopérabilité,
 - Conformité à la réglementation,
 - Solutions propriétaires ou non,
 - Mode d'exercice,
 - Intégration dans les LGC,
 - Facilité d'installation,
 - Facilité d'utilisation,
 - Support de la plate-forme Macintosh ou pas,
 - Configuration minimum du poste.

	Apimail (Apicrypt)	Apimail (S/MIME)	Docteur Net CPS	Sermentis	Security Box® Mail	EASYCRY PT.net	S.M.M.	Sign&mail
Interopérabilité	Partielle	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Conformité à la réglementation	Oui mais	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Solutions propriétaires	Oui	Non	Non	Non	Non	Non	Non	Non
Support du Macintosh	Oui	Non	Non	Non	Non	Oui	Non	Oui
Intégration dans les LGC	Relais et intégré	Relais	Relais	Relais	Relais et intégré	Intégré	Intégré	Relais
Facilité d'installation	+++	++	++	++	++	+++	++	++
Facilité d'utilisation	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Configuration minimum du poste (RAM, place disque)	Sobre	Sobre	Sobre	Sobre	Sobre	Très sobre	Gourmand en RAM (512 Mo) et espace disque (100 Mo)	Nécessite 128 Mo de RAM

← Exercice en monoposte

- Tous les choix sont possibles,
- Privilégiez les solutions intégrées à votre LGC,
- Vérifier que votre plate-forme est supportée (Mac OS),
- L'homologation OSM peut être importante.

← Exercice sur plusieurs sites

- Privilégiez les solutions de type Webmail accessible de n'importe quel endroit.

← Choix en fonction de votre LGC (confer diapositive 21)

- Axilog, Sephira, @medulo : import/export de messages identique quelle que soit la solution choisie,
- CLM : privilégiez S.M.M. quand il est intégré à votre LGC,
- HelloDoc et MédiStory : meilleure intégration actuellement d'Apicrypt. Mais les 2 éditeurs développent actuellement leur propre messagerie intégrée à leur LGC et homologable OSM.

- ← **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) : 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.
- ← **PS** : Professionnel de Santé
- ← **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.