La feuille de soins électronique : Un exemple de système d'information en santé

Pr. F. Kohler, Pr F. Paulus

Nancy-Université
Université Henri Poincaré

ministère éducation nationale enseignement supérieur recherche

Le système de santé en France

- Dualité du système de santé
  - Libéral : en cabinet, en établissement de santé
  - Publique et privé participant au service public dont le système de santé des armées
- Liberté de choix du patient
- Paiement à l'acte
- Liberté d'installation
- ….

Un exemple avant 1997 :

- Mme X a de la température, tousse… Elle consulte son médecin traitant le Dr Y, à son cabinet libéral.
  - Le Dr Y :
    - Pose le diagnostic et prescrit des médicaments (rédige une ordonnance).
    - Remplit la feuille de soins « papier »
    - Fait payer à Mme X le prix de la consultation.
- Mme X va à la pharmacie
  - Le pharmacien :
    - Vérifie l'ordonnance
    - Donne les conseils d'utilisation
    - délivre les médicaments
  - Mme X paie les médicaments

Un exemple avant 1997

- Mme X rentre chez elle :
  - Elle se soigne…
  - Elle « colle » les vignettes des médicaments sur la feuille de soins
  - Elle vérifie le remplissage des rubriques personnelles de la feuille de soins
  - Elle envoie à sa caisse d'assurance maladie la feuille de soins

Un exemple avant 1997

- La caisse d'assurance maladie :
  - Reçoit la feuille de soins
  - Vérifie les prestations
  - Procède au remboursement
- Mme X est remboursée de la part des dépenses couvertes par l'assurance maladie.
- Le délai entre le paiement et le remboursement est de l'ordre de 3 à 4 semaines.

En 1997 : La Feuille de soins électronique

- Dématérialisation des flux entre assurés-professionnels de santé (médecins, pharmaciens, infirmiers….) et assurance maladie.
- Objectifs :
  - Accélérer le remboursement
  - Faciliter la tache de l'assuré
  - Faciliter le tiers payant
  - Eviter la fraude

Les contraintes

- Les échanges doivent impérativement être sécurisés
  - Risque pour le secret médical
  - Risques financiers

Qu’est ce que la sécurisation des échanges électroniques

- Toutes les organisations et techniques mises en œuvre pour garantir :
  - L’intégrité physique (feu, inondation, sauvegarde…)
  - La qualité
  - L’accessibilité et la disponibilité
  - La traçabilité
  - La rapidité de la transmission

Qu'est ce que la sécurisation des échanges électroniques ?

- **Authentification de l'émetteur et du destinataire:**
  - Quand l'auteur du message est le Dr Y, on doit être sur que le message vient bien du Docteur Y.
  - Signature électronique, certificat
- **Non répudiation :**
  - Si j'ai reçu le message du Dr Y, je ne doit pas pouvoir dire que je ne l'ai pas reçu
- **Intégrité :**
  - Le message ne doit pas pouvoir être modifié notamment par quelqu'un qui pourrait l'intercepter
- **Confidentialité :**
  - Le message ne doit être lisible que par son destinataire.

Sécurité et chiffrement : cryptologie

- Cryptologie par substitution
  - Substitution simple
  - Le carré de Polybe
- Cryptologie par clé
  - Le chiffre de Vigenère
  - Les méthodes à clés secrètes
  - Les méthodes à clés publiques

Substitution simple

- Le codage par substitution mono-alphabétique (on dit aussi les alphabets désordonnés) est le plus simple à imaginer.
- Dans le message clair, on remplace chaque lettre par une lettre différente.

- `Texte clair` `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
- `Texte codé` `WXEHYZTKCPJIUADGLQMNRSFVBO`

Le carré de Polybe

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

- Polybe : historien grec 205 – 125 avant JC.
- Il dispose les lettres dans un tableau 5*5 (nous sommes ici obligés d'identifier le i et le j de manière identique) :

Le carré de Polybe

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

- On remplace chaque lettre par ses coordonnées dans le tableau, en écrivant d'abord la ligne, puis la colonne.
- Par exemple, le A est remplacé par 11, le B est remplacé par 12, le F par 21, le M par 32....
- Si nous codons :
  LONGTEMPS JE ME SUIS COUCHE DE BONNE HEURE
- Nous obtenons
  3134332244153235432415 3215 133445132315 1415 1234333152315454215

Le chiffre de Vigenère

Pour coder un message, on choisit une clé qui sera un mot de longueur arbitraire.

On écrit ensuite cette clé sous le message à coder, en la répétant aussi souvent que nécessaire pour que sous chaque lettre du message à coder, on trouve une lettre de la clé.

Pour coder, on regarde dans le tableau l'intersection de la ligne de la lettre à coder avec la colonne de la lettre de la clé.

Exemple : On veut coder le texte "CRYPTOGRAPHIE DE VIGENERE" avec la clé "MATHWEB". On commence par écrire la clef sous le texte à coder :

C	R	Y	P	T	O	G	R	A	P	H	I	E		D	E		V	I	G	E	N	E	R	E
M	A	T	H	W	E	B	M	A	T	H	W	E		B	M		A	T	H	W	E	B	M	A

Pour coder la lettre C, la clé est donnée par la lettre M. On regarde dans le tableau l'intersection de la ligne donnée par le C, et de la colonne donnée par le M.

Le chiffre de Vigenère

- Cet algorithme de cryptographie comporte beaucoup de points forts.
  - Il est très facile d'utilisation, et le décryptage est tout aussi facile si on connait la clé.
  - En outre, l'exemple précédent fait bien apparaitre la grande caractéristique du code de Vigenère : la lettre E a été codée en I, en A, en Q, et en E. Impossible par une analyse statistique simple de retrouver où sont les E.
  - Dernière chose, on peut produire une infinité de clés, il est très facile de convenir avec quelqu'un d'une clé donnée.

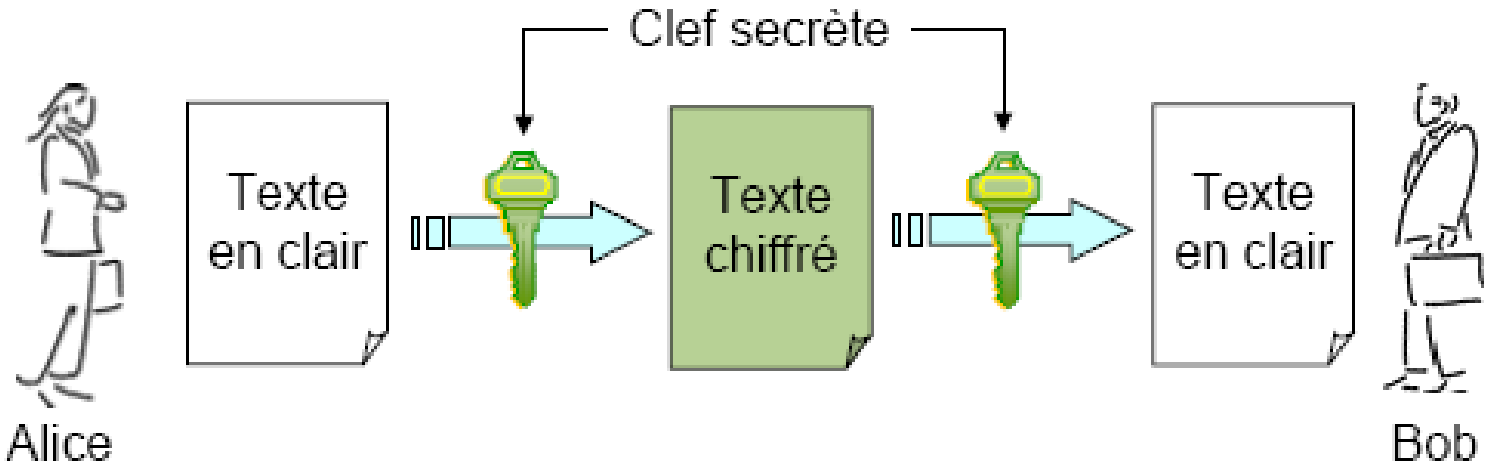
Les méthodes actuelles

- Les méthode à clés sécrètes
- Les méthodes à clés publiques

Méthodes à clé secrète

- Il existe un algorithme de chiffrement parfaitement sûr (il est unique, Shannon 1949).
- Mis au point par Gilbert Vernam en 1917
  - chiffre de Vigenère, où la clé est de la taille du message à envoyer, et où les lettres de cette clé sont choisies totalement aléatoirement.
- Si la clé ne sert qu'une fois (chiffre à usage unique), ce système est absolument sûr : il n'y a aucune corrélation entre le message de départ et sa version codée (voir les détails d'implémentation en annexe).
- Inconvénients de ce mode de chiffrement
  - La génération et le transport des clés.
  - Cette clé doit être parfaitement aléatoire, et sa longueur est énorme....
  - Tout cela pour une seule utilisation!
  - Tout le monde ne dispose pas de la valise diplomatique pour pouvoir échanger la clé.

Le chiffrement symétrique



Le chiffrement symétrique

- Assure le service de confidentialité des données
- Nombreux protocoles y associent les services d'authentification des partenaires ou d'intégrité des données
- Les deux partenaires doivent partager la même clé
- La gestion des clés devient rapidement complexe (création, distribution, modification et destruction)
  - *4 personnes Alice, Bob, Carole et David : Alice doit posséder une clé différente pour chacune des 3 autres personnes, Bob qui possède maintenant une clé pour Alice doit en posséder 2… Soit au total 16 clés*
  - Pour N partenaires il faut N*(N-1)/2 soit pour 50 personnes 1225 clés !!!!

Quelques algorithmes

- Algorithmes de chiffrements en continu (stream cipher)
  - RC4 le plus courant (longueur de clé variable généralement 128bits
- Algorithmes de chiffrement par bloc
  - Opèrent sur le texte en clair par blocs (64 bits)
  - **DES** (clé de 56 bits)
  - Triple DES
  - IDEA
  - CAST
  - Blowfish
  - **AES**

La Saga du DES

- Devant l'émergence de besoins civils, le NBS (*National Bureau of Standards*) lança le 15 mai 1973 un appel d'offres dans le Federal Register (l'équivalent du Journal Officiel américain) pour la création d'un système cryptographique.
- Le cahier des charges était le suivant :
  - l'algorithme repose sur une clé relativement petite, qui sert à la fois au chiffrement et au déchiffrement.
  - L'algorithme doit être facile à implémenter, logiciellement et matériellement, et doit être très rapide.
  - le chiffrement doit avoir un haut niveau de sûreté, uniquement lié à la clé, et non à la confidentialité de l'algorithme.
- Les efforts conjoints d'IBM, qui propose Lucifer fin 1974, et de la NSA (*National Security Agency*) conduisent à l'élaboration du DES (*Data Encryption Standard*), l'algorithme de chiffrement le plus utilisé au monde durant le dernier quart du XXiè s.

Le DES cassé

- Ce qui a signé l'arrêt de mort du DES est l'extraordinaire progression de la puissance des ordinateurs.
- Le 17 juin 1997, le DES est cassé en 3 semaines par une fédération de petites machines sur Internet.
- On estime très officiellement (dans un rapport présenté au Sénat Américain) à cette date à quelques secondes le temps nécessaire à un état pour percer les secrets d'un message chiffré avec le DES.

Le chiffrement asymétrique

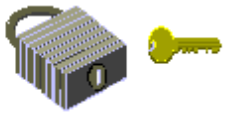
- Appelé à clé publique parce que basé sur l'existence de deux ensembles
  - Les valeurs qui sont conservées privées par leur propriétaire : clé privée ou clé secréte
  - Les valeurs qui sont rendues publiques
- Chaque partenaire d'un réseau possède un couple unique clé publique/clé privée
- Les clés publiques doivent être communiquées à l'ensemble des partenaires

SANTE

Cryptographie à clé publique :

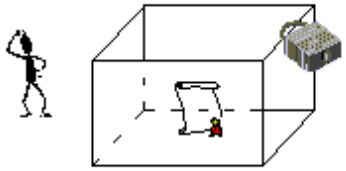

Alice Bob

Etape 1 : Fabrication des clés. Bob fabrique une clé publique qui permet de sceller le message codé dans la boite (ici : le cadenas), et une clé privée qui permet d'ouvrir le cadenas.

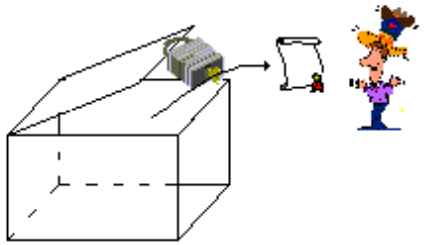


Etape 2 : Distribution des clés. Bob fait parvenir à Alice le cadenas, mais garde la clé pour lui.

Etape 3 : Envoi du message. Alice met son message dans une boite qu'elle ferme à l'aide du cadenas.



Etape 4 : Réception du message. Bob ouvre la boite a l'aide de sa clé, et récupère le message. Personne n'a pu l'intercepter puisque lui seul pouvait ouvrir la boite.



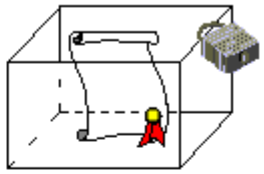
Le RSA

- Inventée en 1977 par Ron Rivest, Adi Shamir et Len Adleman, à la suite de la découverte de la cryptographie à clé publique par Diffie et Hellman.
- Le RSA est encore le système cryptographique à clé publique le plus utilisé de nos jours.
- Repose sur des problèmes mathématiques complexes
- 2 clés distinctes : clé publique et clé privée
- Algorithme lent réservé à l'échange de clé et à la signature

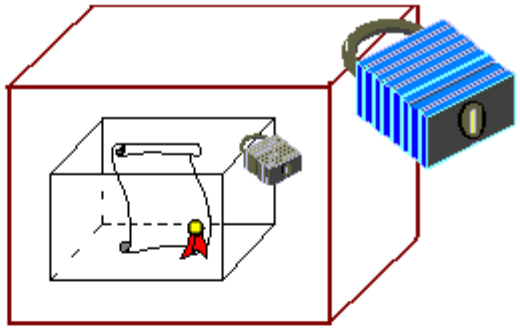
Etre sur de l'expéditeur : La signature électronique

- La cryptographie à clé publique permet de s'affranchir du problème de l'échange de la clé, facilitant le travail de l'expéditeur.
- Mais comment s'assurer de l'authenticité de l'envoi? Comment être sûr que personne n'usurpe l'identité d'Alice pour vous envoyer un message? Comment être sûr qu'Alice ne va pas nier vous avoir envoyé ce message?
- La cryptographie à clé publique peut résoudre ce problème.
  - Alice veut envoyer un message crypté à Bob, mais Bob veut s'assurer que ce message provient bien d'Alice. Ils se sont mis d'accord sur un système de cryptographie à clé publique commun, Alice possédant le couple clé publique/clé privée (PA,SA), et Bob le couple (PB,SB). Alice veut envoyer M.
  - **Phase d'envoi :** Alice calcule SA(M), à l'aide de sa clé secrète, puis PB(SA(M)), à l'aide de la clé publique de Bob.
  - **Phase de réception :** A l'aide de sa clé privée, Bob calcule SB(PB(SA(M)))=SA(M). Seul lui peut effectuer ce calcul (=sécurité de l'envoi). Puis il calcule PA(SA(M))=M. Il est alors sûr que c'est Alice qui lui a envoyé ce message, car elle-seule a pu calculer SA(M).

Alice

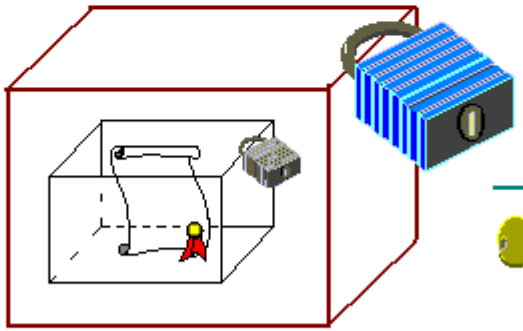


enferme le message dans une boite à l'aide de sa clé privée (authentification de l'expéditeur)

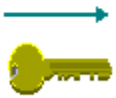


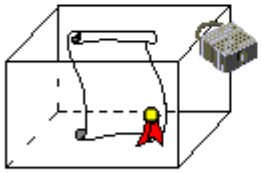
enferme cette boite dans une autre boite avec la clé publique de Bob (chiffrement, seul Bob peut ouvrir)

Bob



recoit le message chiffré et authentifié





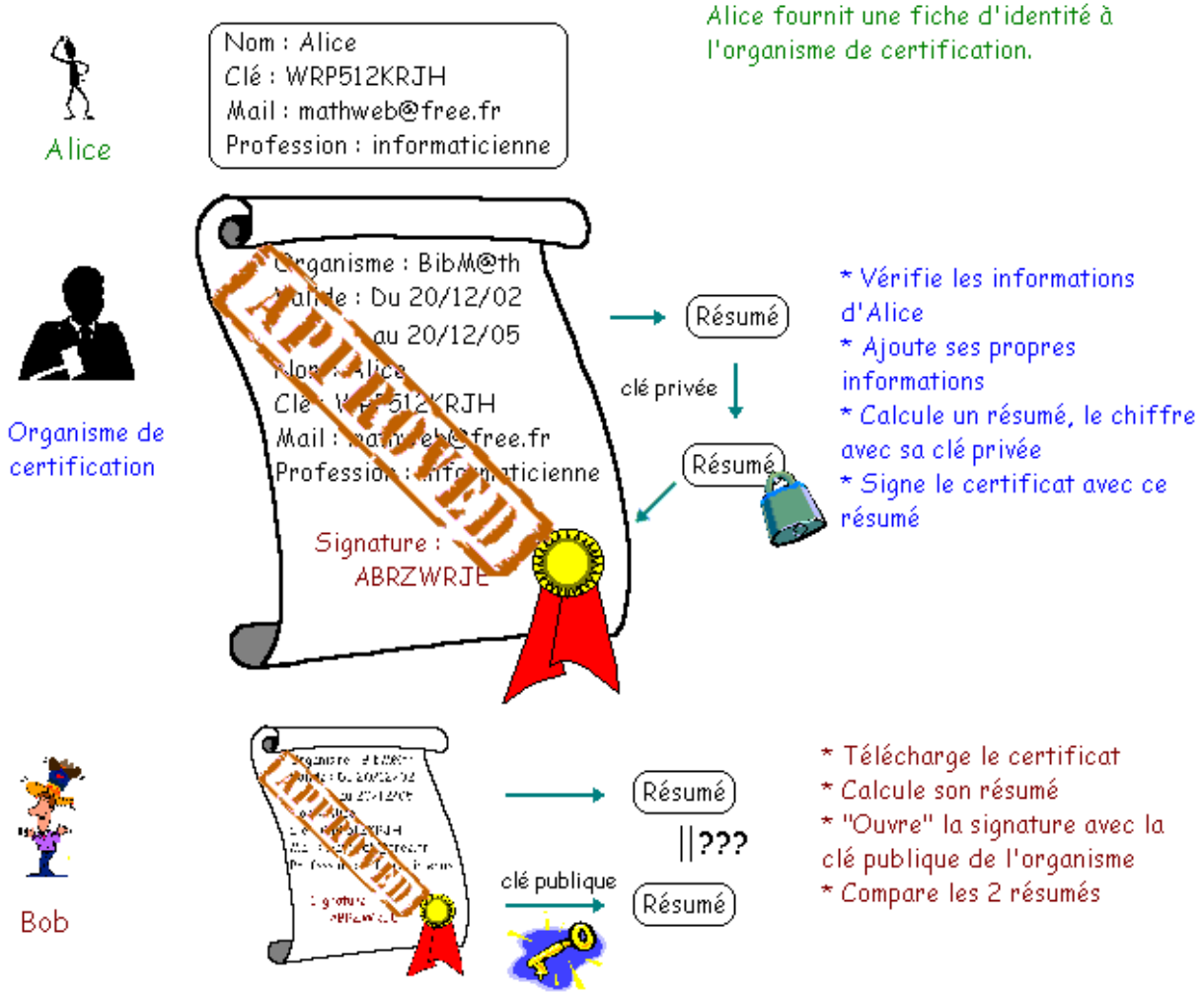
ouvre la premičre botie avec sa clé privée (déchiffrement)

ouvre la deuxičme boite avec la clé publique d'Alice (authentification)

Etre sur du destinataire ?

- Le problème des certificats numériques est à l'opposé de celui de la signature électronique : si vous commandez des Cds sur Internet, comment être sûr que vous envoyez bien votre numéro de carte bleue au commerçant, et non à un pirate qui aurait usurpé son identité et donné sa propre clé publique. Cette fois, c'est donc du Destinataire que l'on veut être sûr, et non de l'Expéditeur.
- Comme dans la vie courante, on a recours à des certificats. Pour passer un examen, il vous faut prouver votre identité : fournir une carte d'identité, passeport ou permis de conduire. Un organisme supérieur (l'Etat) a signé ces certificats, s'assurant auparavant (par un acte de naissance,...) qu'il s'agit bien de vous.
- Les certificats numériques fonctionnent sur le même principe.
  - Alice veut certifier que sa clé publique lui appartient. Elle envoie sa clé à un organisme de certification, ainsi que différentes informations la concernant (nom, email, etc...).
  - Cet organisme vérifie les informations fournies par Alice, et ajoute au certificat son propre nom, une date limite de validité, et surtout une signature numérique.
  - Cette signature est calculée de la façon suivante : à partir des informations du certificat, l'organisme calcule un résumé en appliquant une fonction de hachage connue, comme MD5. Puis il signe ce résumé en lui appliquant sa clé secrète.

- Lorsque Bob veut envoyer son message à Alice,
  - il télécharge le certificat de celle-ci sur un serveur de certificat (on parle de PKI, *Public Key Infrastructure*).
  - Il calcule le résumé du certificat, puis applique la clé publique de l'organisme auteur du certificat à la signature électronique.
  - Si cette quantité est égale au résumé, il est sûr qu'il a bien affaire à Alice.



Certification numérique d'une clé publique

Le chiffrement et la Loi en France

- Rôle de la direction centrale de la sécurité des système d'information

Synthèse du nouveau cadre législatif et réglementaire				
Finalités	**Fonctions offertes**			
	Authentification, signature, intégrité, non répudiation	Confidentialité		
		$L \leq 40$ bits	40 bits $< L \leq$ 128 bits	$L >$ 128 bits
Utilisation	Libre	Libre	Libre ou Déclaration (1)	Autorisation
Fourniture	Déclaration simplifiée	Déclaration	Déclaration	Autorisation
Importation	Libre	Libre	Libre ou Déclaration (1)	Autorisation
Exportation	Libre	Autorisation	Autorisation	Autorisation

Le chiffrement en santé

- Applications actuelles
  - La feuille de soins électronique
  - Messagerie sécurisée
  - PMSI : numéro anonyme chaînable par la Fonction d'Occultation de l'Information Nominative (FOIN)
  - Dans l'avenir le DMP
- Utilisent pour certaines des cartes à puces
  - CPS et CP
  - SESAM - VITALE

La Carte « Professionnel de Santé »

- La CPS est une carte à microprocesseur, un support personnalisé permettant à son porteur, le professionnel de santé
  - de s'identifier,
  - de s'authentifier pour accéder à des données ou des services réservés,
  - d'attester de sa qualité de professionnel de santé et de sa situation conventionnelle,
  - d'accéder à des informations ou des services dans le respect des droits liés à sa fonction,
  - de signer électroniquement les opérations effectuées et d'accéder au réseau « santé social ».
- La CPS permet :
  - l 'accès sécurisé à l 'information médicale,
  - la sécurité des messageries électroniques,
  - l 'accès exclusif à des réseaux spécifiques et à des informations ciblées (réseau santé - social).

La CPS

- La CPS est émise par un Groupement d'intérêt public qui a rejoint l'ASIP (agence des systèmes d'information partagés de santé) qui réunit les ordres professionnels, des associations professionnelles, les hôpitaux, l'état, les assurances complémentaires et l'assurance maladie.
- Dotée d'un système de reconnaissance « carte à carte », la CPS et elle seule, donne accès aux informations contenues dans la carte VITALE .

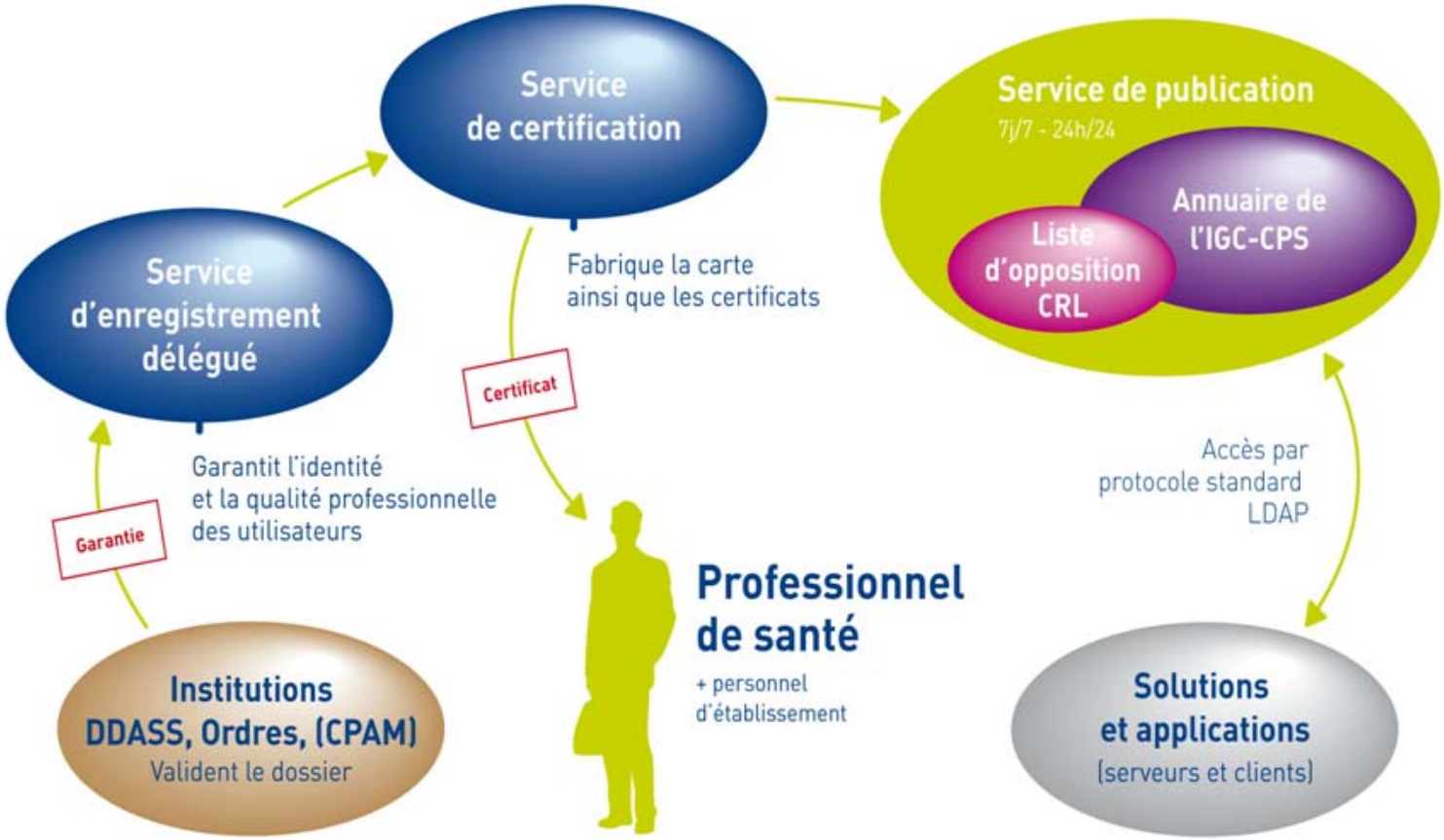
La CPS

- **La carte CPS est réservée aux professionnels de santé réglementés par le Code de la Santé Publique :**
  - Les professionnels de santé régis par un Ordre : médecins, chirurgiens-dentistes, sages-femmes, pharmaciens, masseurs-kinésithérapeutes, pédicures-podologues,
  - Les auxiliaires médicaux : infirmiers, orthophonistes, orthoptistes, opticiens-lunetiers, audioprothésistes, ergothérapeutes, psychomotriciens, manipulateurs d'électroradiologie médicale,
  - Les professionnels de santé du Service de Santé des Armées.
- **La CPS contient :**
  - **Les données relatives à l'identification du professionnel de santé**
    - numéro d'identification ADELI,
    - nom patronymique et nom d'exercice du professionnel de santé,
    - profession et spécialité
  - **Les informations relatives à chaque activité**
    - la CPS peut contenir plusieurs situations d'exercice différentes et autant de situations de facturation différentes pour les feuilles de soins, mode d'exercice, identification du lieu d'exercice, données de tarification de l'assurance maladie.
  - **Les éléments techniques nécessaires aux fonctions de sécurité**
    - authentification du professionnel de santé, signature électronique.

La famille des cartes CP

- Cartes de professionnel de santé
- Cartes de professionnel en formation
- Cartes de directeur d’établissement
- Cartes de personnel d’établissement
- Cartes de personnel autorisé

Infrastructure de gestion de Clés (IGC)



Accès sécurisé ›› | Quitter

Accueil | Autorités de Certification

Recherche rapide

Nom ou Identifiant:
maire

Département:
Vosges (88)

- (•) Professionnels de santé
- ( ) Structures
- ( ) Serveurs

RECHERCHER

Recherche avancée

- Professionnels de santé
- Structures
- Serveurs

INFOS TITULAIRE | LIEU D'EXERCICE | CERTIFICATS

Identité

Identification :	0441032323
Civilité :	Monsieur
Nom :	MAIRE
Prénom :	BERNARD
Mail(s) :	- non renseigné -
Type de carte :	CPS
Numéro de carte :	2200183014
Historique ADELI :	- non renseigné -

Profession

Profession :	Médecin
Spécialité :	Médecine générale (polyvalente en milieu hospitalier)
Qualif d'exercice RPPS :	- non renseigné -
Rôle dans la structure :	Titulaire cabinet

SANTE

Accès sécurisé ›› | Quitter

Accueil | Autorités de Certification

Recherche rapide

Nom ou Identifiant:
maire

Département:
Vosges (88)

- (•) Professionnels de santé
- ( ) Structures
- ( ) Serveurs

RECHERCHER

Recherche avancée

- Professionnels de santé

INFOS TITULAIRE	LIEU D'EXERCICE	CERTIFICATS

Certificat d'authentification

Numéro de série : 21b617
Date de début : Sep 15, 2009 2:00:01 AM
Date de fin : Nov 1, 2012 12:59:59 AM

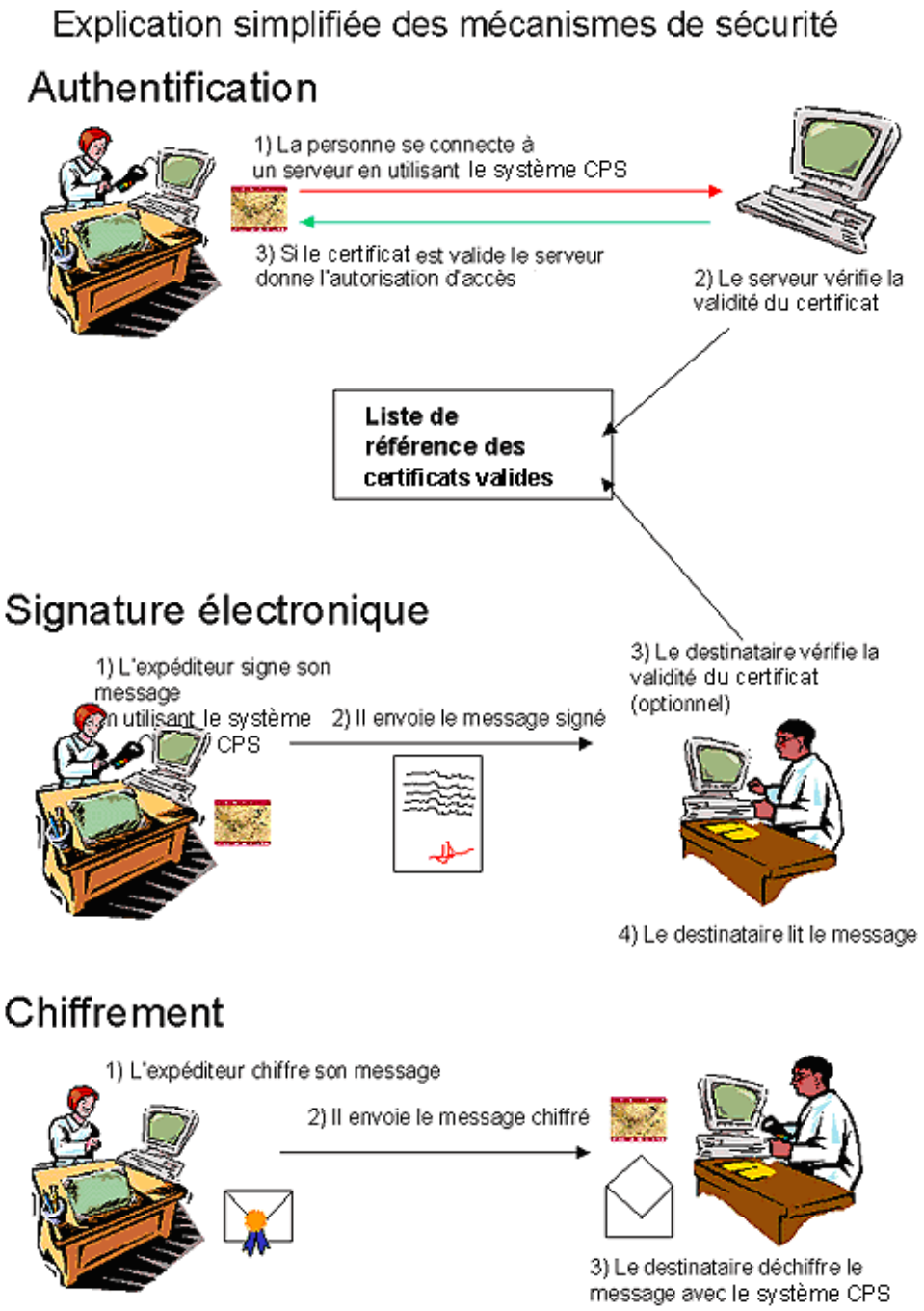
Télécharger...

Certificat de signature

Numéro de série : 21b615
Date de début : Sep 15, 2009 2:00:01 AM
Date de fin : Dec 1, 2012 12:59:59 AM

Télécharger...

La messagerie sécurisée à l'aide de la CPS



La carte Vitale

- La carte Vitale est une carte d'assuré social. Elle atteste de l'affiliation et des droits à l'Assurance Maladie.
- La carte Vitale est une carte à microprocesseur, de la taille d'une carte bancaire.
- Elle contient tous les renseignements administratifs nécessaires au remboursement des soins.
- Elle peut être présentée à tout professionnel ou établissement de santé, équipé du matériel informatique lui permettant de la "lire".
- La carte Vitale est attribuée à toute personne de 16 ans et plus.
- *A noter*
  - *la carte Vitale ne contient aucune information d'ordre médical ;*
  - *la carte Vitale n'est pas une carte de paiement.*

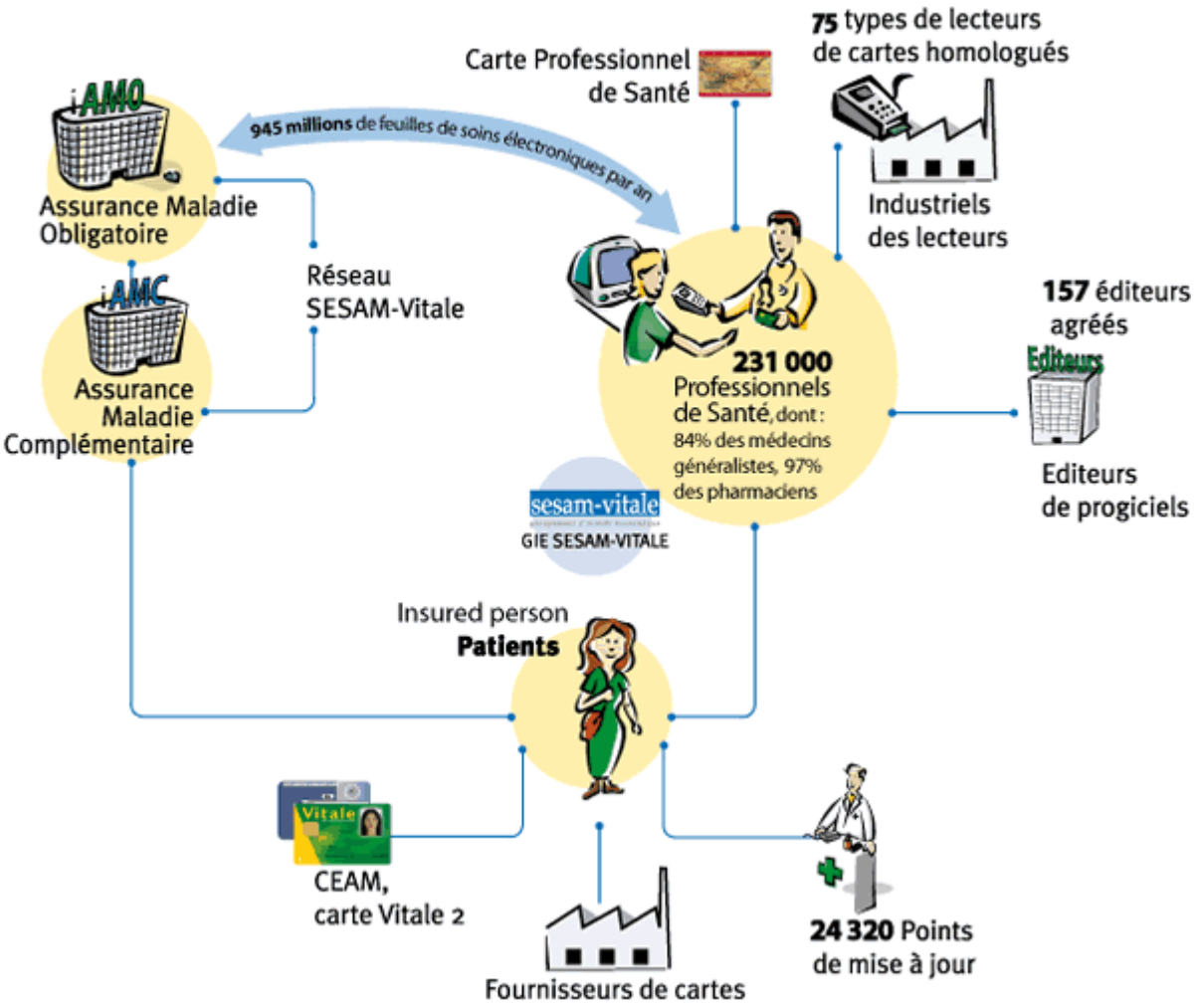
Informations contenues dans la carte

- **Informations inscrites sur le visuel de la carte Vitale**
  - n° de sécurité sociale de l'assuré ;
  - nom et prénom du titulaire de la carte.
- **Informations contenues dans la puce de la carte Vitale :**
  - n° de sécurité sociale de l'assuré ;
  - régime d'assurance maladie ;
  - caisse d'Assurance Maladie et centre de rattachement ;
  - nom et prénom du titulaire de la carte ;
  - nom et prénom des bénéficiaires ;
  - et, éventuellement : exonération ou modulation du ticket modérateur, droit à la CMU complémentaire.
- *A noter : la carte Vitale ne contient pas de dossier médical.*

La carte VITALE 2

- Carte individuelle, véritable carte d'identité de santé
  - données d'urgence afin de connaître le plus rapidement possible si nécessaire, la personne à contacter ou le médecin traitant d'une personne inanimée par exemple.
  - données médicales comme par exemple les allergies ou les traitements réguliers.
- Ces informations pourront être synchronisées avec le dossier médical personnel
- La carte vitale 2 sera également la clé d'accès au dossier médical personnel ou à d'autres dossiers de prestation de l'assurance-maladie (articles 2 & 12 de la loi)
- Mise en service : 2006
- Chaque carte aura une durée de validité de 5ans

Schéma général du système SESAM-Vitale - décembre 2006



Le système SEAM VITALE

- Le système SESAM-Vitale met en œuvre de nombreux composants matériels et logiciels :
  - La **carte Vitale**
  - La **carte CPS**.
  - **L'équipement informatique** du Professionnel de Santé : équipement informatique "classique" (ordinateur, lecteur de cartes homologué, progiciel agréé CNDA, etc) ou Solution Intégrée.
  - **Des réseaux informatiques** de transmission de Feuilles de Soins Electroniques et d'échanges de données professionnelles.
  - **Des systèmes informatiques spécifiques** à l'Assurance Maladie (frontaux et Centres de Traitement Informatiques), chargés du traitement des Feuilles de Soins Electroniques.

SESAM VITALE et Réseau

- En 1997 deux options :
  - Réseau propriétaire de l'assurance maladie
  - Réseau utilisant les normes de l'internet
    - Protocoles de l'internet :
      - TCP/IP
      - POP/FTP
      - …
    - Intranet : le réseau santé social

La création d'une Feuille de soins Electronique

- A votre arrivée au cabinet, vous mettez en marche votre équipement, insérez votre carte de professionnel de santé (CPS) dans le lecteur Vitale (bi-fente) et saisissez votre code confidentiel pour vous identifier.
- Vous pouvez laisser votre carte dans le lecteur toute la journée.

Ensuite

- Pour chaque patient, vous réalisez une feuille de soins électronique (FSE) à l'aide de votre logiciel et en présence de la carte Vitale et de votre CPS insérées dans le lecteur.
- La transmission
  - La transmission des FSE peut s'effectuer à tout moment de la journée.
  - Avant de télétransmettre, le logiciel effectue le groupement des FSE en lots, permettant un envoi par organisme destinataire : caisses du régime général, de la MSA (régime agricole), etc.
  - L'opération de regroupement et d'émission ne prend que 2 à 3 minutes par jour.

Le traitement par l’assurance maladie et les retours

- Après traitement de la FSE, l'organisme vous envoie un accusé de réception logique positif (ARL) pour confirmer l'arrivée des FSE.
- Cet accusé de réception dégage votre responsabilité en terme de prise en charge des FSE.
- En cas de problème, vous êtes averti de la réception d'un ARL négatif ou d'une absence de retour. Vous disposez de deux jours ouvrés pour retransmettre vos FSE.
- En cas de tiers-payant, vous recevez également des retours RSP qui vous informent du rejet ou paiement.
- Vous devez conserver durant 3 mois une copie sauvegardée de toutes les FSE.

SESAM VITAL 1.40

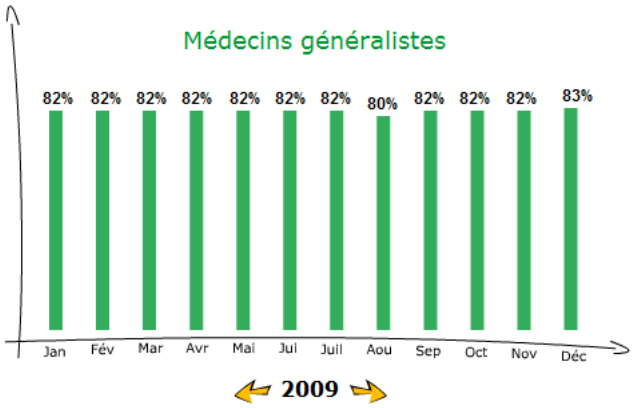
- PS Concernés : Tous
- Prise en compte de la CCAM
- Sécurisation renforcée : chiffrement
- Possibilité de signature désynchronisée : **meilleure adaptation pour l'organisation de la facturation dans les cabinets possédant un accueil (ou secrétariat), ou dans les cabinets de groupe**
- **Prise en compte de l'assurance complémentaire :** possibilité de télétransmettre dans le même temps une facture au régime obligatoire du patient (la FSE, désormais bien connue) et une facture à la complémentaire santé du patient ("DRE" ,Demande de Remboursement Electronique).

FSE : Intérêts

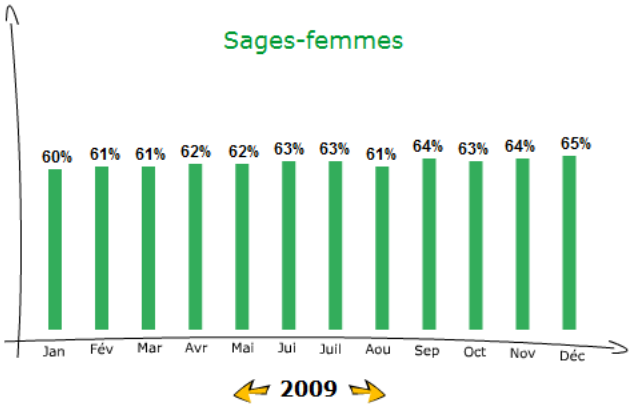
- un **système national** valable pour l'ensemble des organismes d'assurance maladie.
- des **feuilles de soins sécurisées** grâce aux cartes Vitale et CPS.
- des **remboursements plus rapides**, pour les patients et pour vous, même en cas de tiers payant.
- une simplification **d'enregistrement des fichiers clients** : l'emploi des cartes à puce permet de récupérer directement les informations administratives et les données d'exonération des assurés, évitant ainsi les erreurs de saisie.

Statistiques

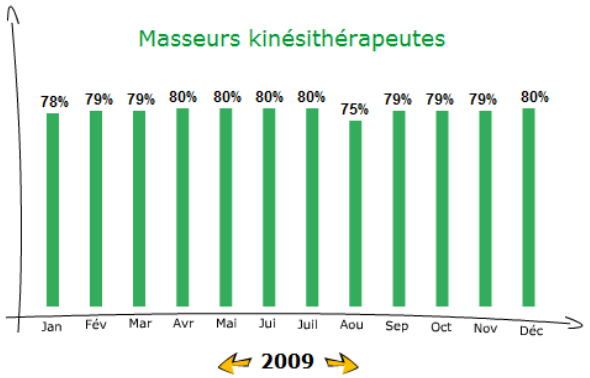
Médecins généralistes



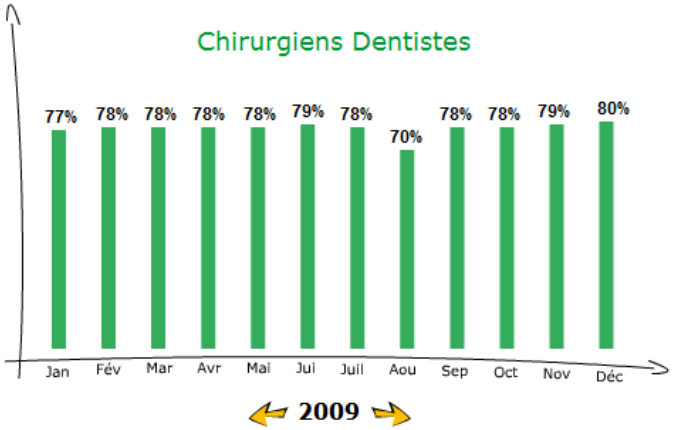
Sages-femmes



Masseurs kinésithérapeutes



Chirurgiens Dentistes



Pharmaciens