ENSP
ÉCOLE NATIONALE DE LA SANTÉ PUBLIQUE
RENNES

**Directeur d'hôpital**

*Date du Jury :* **décembre 2000**

# L'utilisation de la cryptographie dans les échanges de données médico-sociales

**Christophe FIGLAREK**

# S O M M A I R E

**REMERCIEMENTS**

Il n'aurait pas été possible pour moi d'écrire ce mémoire sans l'aide de l'équipe de la Direction des Systèmes d'Information et des Coopérations Sanitaires (DSIC) du Centre Hospitalier de la Région d'Annecy (CHRA) et je tiens à remercier tout particulièrement Madame Anne-Marie Fabretti pour son appui documentaire et sur l'expérience qu'elle a bien voulu partager avec moi sur la constitution des réseaux de soins ainsi que Monsieur François Meusnier-Delaye pour le temps qu'il a bien voulu m'apporter pour m'expliquer les différents choix des techniques et les problématiques qui se présentent lors de la mise en place de réseaux sécurisés de télémédecine.

Je tiens à remercier également mon encadrant mémoire, Monsieur Eric Larcher, chargé de la sécurité des systèmes d'information chez Accor, auteur de guides informatiques et de *L'internet sécurisé*, pour ses corrections, sa très grande pédagogie pour expliquer simplement les ressorts de la cryptographie et son aide importante sur l'aspect technique et juridique de mon mémoire.

De nombreux médecins de la FULMEDICO (Fédération des Utilisateurs de Logiciels MEDIcaux COmmunicants) et de l'AMGIT (Association des Médecins Généralistes pour l'Informatisation et la Transmission des données) m'ont donné d'importantes informations concernant leurs pratiques et leurs interrogations quant àl'avenir de l'informatique médicale, notamment dans le cadre des réseaux. Leurs commentaires ont été appréciés.

*" Dans le contexte d'une société où les échanges d'informations numériques se développent, il est indispensable de pouvoir bénéficier de systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel, assurer la sécurité des transactions financières et commerciales, passer des contrats en l'absence de support papier. Les technologies cryptographiques sont, de nos jours, reconnues comme étant des outils essentiels de la sécurité et de la confiance dans les communications électroniques."*

**(Extrait du rapport pour le Conseil d'Etat, 1997)**

## INTRODUCTION

La plus grande partie des transactions et des échanges dans un hôpital est encore réalisée avec un support papier mais la facilité de traitement des informations électroniques, leur vitesse de transmission et la simplicité d'emploi de données numérisées sont autant d'éléments qui plaident aujourd'hui en faveur de la généralisation de l'usage de réseaux électroniques permettant une interconnexion entre les différents acteurs de la santé publique. Pour l'instant, la consultation de sites Internet, le courrier électronique et la télétransmission des feuilles de soins des patients vers la Caisse Primaire d'Assurance Maladie sont les applications les plus répandues à côté des expériences de télémédecine en plein développement. Alors que cette utilisation de la voie électronique pour transmettre des informations se généralise progressivement, un besoin de protection se fait sentir et s'impose dans les esprits, renforcé par des textes juridiques et par l'action de la CNIL. Pour Gérard Worms, ancien président du Conseil Supérieur des Systèmes d'Information de Santé, "*dans cinq ans, la télétransmission sera devenu un réflexe naturel*"[1] et la cryptographie sera devenue une priorité pour protéger le patient. Pour éviter qu'un dossier médical ne soit lu par exemple par une personne non autorisée, la sécurisation des communications est un préalable. Pour accéder à une banque de données médicales nominatives, pour transmettre des informations médicales concernant un malade, le secret est exigé et il est donc essentiel que les identités de l'émetteur et du récepteur des messages soient garanties. Tous ces besoins sont couverts par une partie bien spécifique de la sécurité des systèmes d'information : la cryptographie.

Pour beaucoup, "*la cryptographie est un sujet de roman d'espionnage*"[2]. Elle est en effet historiquement liée au domaine militaire et au monde du renseignement. En tant que science, elle est considérée comme une branche de la mathématique et de l'informatique chargée de modéliser et de créer des algorithmes afin de coder des informations. C'est surtout une technologie utile pour tous ceux qui veulent protéger des données confidentielles, notamment lorsque celles-ci sont amenées à être transmises par des voies sécurisées ou non. Aujourd'hui, depuis les textes de mars 1999[3] sur la libéralisation de son usage en France, l'utilisateur est quasi maître de son choix de cryptage et il est le seul responsable de l'usage qu'il en fait. Si pour des directeurs d'hôpital ou des médecins parfaitement rompus à l'utilisation de ces techniques, conscients des contraintes qu'elles imposent, des limites de leur efficacité et des pièges qu'elle recèle, cette tâche et cette

[1] Gérard WORMS, in *Le Quotidien du Médecin* N°6629, 24 janvier 2000, pages 8 et 10
[2] Première phrase d' *Introduction à la cryptographie*, Network Associates, pour PGP Version Internationale 6.5.1, 24 décembre 1999.
[3] Cf. décrets n° 99-199 et n° 99- 200 du 19 mars 1999 analysés en pages 30 et 31 de ce mémoire

responsabilité ne posent guère de problème mais qu'en est-il pour le profane qui a juste découvert la cryptographie dans *Que sais-je ?*[4] ou mieux, s'il est curieux, dans le livre de Bruce Schneier[5]. Ce cryptologue reconnu internationalement a récemment révélé une multitude de malfaçons dans les produits des plus grands éditeurs, et que rien ne ressemblait plus à un bon procédé qu'un mauvais ! De plus, depuis la révélation dans la presse généraliste au début de l'année 2000 des failles importantes du système choisi par le GIE Carte Bleue[6] pour les cartes bancaires de paiement automatique, on sait que la cryptographie n'est pas la panacée à tous les maux et qu'elle n'est pas simple à mettre en œuvre. La sélection et surtout l'organisation d'un tel dispositif s'intégrant dans un système d'informations communiquant et partagé, répondant à des besoins réels, exige un travail rigoureux et un certain niveau d'expertise. Le choix d'une solution de cryptographie s'intègre donc dans un processus de construction d'échanges qu'il faut aujourd'hui bâtir.

C'est pourquoi, à l'heure où les cabinets médicaux s'informatisent (avec des niveaux très inégaux), quand les hôpitaux développent de nouveaux réseaux de coopération, lorsqu'ils installent dans leurs murs des systèmes d'information parfois très sophistiqués, il est important de réfléchir sur la mise en place concomitante de solutions de cryptographie. Dans les faits, un grand nombre de médecins ne se soucie pas du degré de sécurité lorsqu'ils transmettent un dossier par courrier électronique. Comment peut-il en être autrement alors que ces informations ont longtemps circulé par simples courriers voire par fax ? De nombreuses entreprises ont saisi l'enjeu en proposant des logiciels de gestion médicale devenus communicants, de grands groupes comme France Télécom et Cégétel ont créé des réseaux sécurisés, des sociétés ou des associations ont proposé des solutions clés en main de cryptographie… La situation est devenue très complexe et réussir à faire communiquer l'ensemble des professionnels de santé entre eux avec les mêmes outils semble malheureusement devenue une mission quasi impossible. Il n'empêche que la cryptographie est devenue dans tous ces systèmes un point commun obligatoire. Même s'il l'ignore, le praticien utilise des solutions de cryptage avec sa CPS, envoie des messages cryptés en télétransmettant des FSE ou échange des fichiers plus ou moins codés avec son collègue utilisant le même logiciel. Mais la situation est souvent loin d'être claire et c'est à l'hôpital peut-être de servir d'exemple, avec la télémédecine, en montrant qu'il est possible de bâtir des solutions simples de transmission de fichiers ou d'échanges de données complètement sécurisées.

---

[4] *Que sais-je ? La cryptographie*

[5] Bruce SCHNEIER : *Cryptographie appliquée, seconde édition* International Thomson Publishing France, 1997

[6] L'essentiel des informations relatives à la vulnérabilité des cartes bancaires est disponible sur le site Web http://parodie.com/monetique/vulnerabilite.htm

Le but de ce mémoire est d'exposer ces solutions de cryptographie mais comme chaque problème est unique dans ce domaine, il est difficile de proposer un remède miracle qui réunirait la totalité des acteurs du monde de la santé et leur permettrait des échanges de données nominatives en respectant les règles du secret et de la confidentialité. L'objectif est, pour un directeur d'hôpital chargé de rendre plus communicant son système d'informations, par exemple par le biais d'un réseau de télémédecine, de lui donner les clés nécessaires pour résoudre de manière efficace la problématique de la sécurité de données nominatives transmises par voie électronique. Lorsqu'on connaît la place du droit de l'information du patient dans le système public de soins hospitaliers, on saisit beaucoup plus rapidement peut-être les enjeux de la sécurité de ces transmissions. L'idée majeure est de montrer que, dans la constitution de réseaux de santé, les aspects juridiques et techniques demeurent certes incontournables, que les choix en la matière doivent respecter la loi et des normes techniques pour être efficaces mais que l'essentiel des problèmes aujourd'hui (et peut-être plus qu'avant) est surtout lié à des soucis d'organisation et d'interopérabilité entre les différents acteurs du système de santé en France.

Il s'agit de voir que la cryptographie est une science longtemps restée centrée sur des problématiques de sécurité nationale (**I.1**) mais dont l'évolution des technologies (**I.2**) et de la réglementation (**I.3**) permet désormais plus facilement son application dans le milieu médico-social. L'usage de la cryptographie devenant fondamental dans le domaine de la santé (**II.1**), plusieurs outils cherchent à devenir incontournables aujourd'hui (**II.2**) laissant encore entière la question de la sécurisation des données médicales nominatives (**II.3**). Face à la libéralisation de la cryptographie et au renouvellement de certains outils (**III.1**), plusieurs systèmes d'organisation de réseaux sécurisés de télémédecine peuvent servir de modèle comme celui du Centre Hospitalier de la Région Annecienne (**III.2**) ou d'autres à vocation locale ou nationale (**III.3**).

## I) LA CRYPTOGRAPHIE EST UNE SCIENCE LONGTEMPS RESTEE CENTREE SUR DES PROBLEMATIQUES DE SECURITE NATIONALE MAIS DONT L'EVOLUTION DES TECHNOLOGIES ET DE LA REGLEMENTATION PERMET DESORMAIS PLUS FACILEMENT SON APPLICATION DANS LE DOMAINE MEDICO-SOCIAL :

### 1) Principales fonctions de la cryptographie à travers son histoire :

Même si l'utilisation de la cryptographie est devenue transparente et quotidienne aujourd'hui, le vocabulaire qui lui est lié demeure encore mystérieux, à commencer par l'opération elle-même. On entend ainsi parler d'algorithme, de cryptage, d'authentification, de clés asymétriques, de gestion de clés… et l'aspect juridique actuel est souvent mal connu.

*a) Définition et utilisations de la cryptographie :*

Le mot "cryptographie" vient du grec kruptos signifiant *caché* et de graphein *écrire*. *Le Larousse* donne comme définition générale "*Ensemble des techniques permettant de protéger une communication au moyen d'un code graphique secret*".[7]

Très succinctement, la **cryptographie** est une technique qui permet de "*convertir un message clair et intelligible en un message chiffré inintelligible à l'aide d'un algorithme (formule mathématique) et d'une clé*"[8]. En fait, cette définition ne correspond qu'à l'une des applications les plus connues de la cryptographie, à savoir le **chiffrement**. Les données lisibles et compréhensibles sans intervention spécifique sont considérées comme du **texte en clair**. Cette méthode qui permet de transformer un texte en clair en charabia inintelligible est également appelé le **cryptage**. Elle permet de s'assurer que seules les personnes auxquelles les informations sont destinées pourront y accéder. Le processus inverse consistant à retrouver le texte d'origine à partir du texte chiffré s'appelle le **déchiffrement** lorsqu'on possède la clé et lorsqu'on connaît l'algorithme utilisé pour crypter. Lorsqu'il s'agit de récupérer le message original à partir du message chiffrer sans connaître la clé, on parle de **décryptage**. Souvent, par abus de langage, déchiffrement et décryptage sont confondus. Le décryptage requiert une certaine compétence en informatique et en mathématique.

C'est pourquoi la définition générale de la cryptographie est avant tout celle d'une science. Son objectif est de concevoir des formules mathématiques permettant de transformer des messages clairs en messages inintelligibles pour tous ceux qui ne connaissent ni la formule, ni la clé. Elle permet ainsi de stocker des informations

[7] *Le Petit Larousse 2000,* version électronique
[8] Eric LARCHER : *L'Internet sécurisé,* Editions Eyrolles, Annexe A, page 349, 2000

confidentielles et de les faire circuler sur des réseaux sécurisés ou non (tels que l'Internet) afin qu'aucune autre personne ne puisse les lire. C'est un moyen d'assurer une certaine protection. En fait, la confidentialité sur un réseau peut être assurée soit en sécurisant le réseau (on sécurise en fait le "tuyau" avec une infrastructure permettant de limiter l'accès), soit en sécurisant les données qui circulent (en les cryptant), soit les deux. Par abus de langage, on dit souvent qu'on **décrypte** un fichier **crypté** (ou **encrypté**). En fait, cette activité est l'œuvre des **cryptanalystes** qui cherchent à découvrir le message d'origine sans connaître la clé en utilisant les failles des algorithmes afin de les "casser" pour "décrypter" un contenu. Les **cryptographes** sont ceux qui élaborent les algorithmes les plus sûrs. La **cryptanalyse** classique implique une combinaison intéressante de raisonnement analytique, d'application d'outils mathématiques, de recherche de modèle, de patience, de détermination et de chance. On regroupe sous le terme de **cryptologie**, la **cryptographie** associée à la **cryptanalyse**. Sémantiquement proches, ces termes sont aussi souvent confondus.

La cryptographie peut être **vulnérable** ou " **invulnérable"**. Cette vulnérabilité se mesure en terme de temps et de ressources nécessaires pour récupérer le texte en clair. Bruce Schneier l'a très bien résumé en disant qu' *"il existe deux types de cryptographie dans le monde : celle qui protège vos documents de la curiosité de votre petite sœur et celle qui empêche les gouvernements les plus puissants de lire vos fichiers"*[9]. La cryptographie "invulnérable" correspond au second, on notera cependant qu'elle est relative : une révolution dans les mathématiques peut toujours intervenir afin de faciliter certaines opérations aujourd'hui encore trop complexes pour être traitées rapidement par une formulation scientifique théorique. Tout le débat juridique des années 1990 en France a porté sur ce degré de vulnérabilité à relier avec l'une des fonctions de la cryptographie : la **confidentialité**. Il s'agit de garantir le secret de l'information transmise ou archivée. Tout courrier électronique transmis est ainsi protégé sous une forme chiffrée. Dans les esprits, la cryptologie est souvent résumée à cette seule fonction sans doute pour des raisons historiques car ce fut longtemps son seul usage. Une autre fonction est celle de l'**identification** : l'identité et la qualité d'une personne souhaitant accéder à des informations et des ressources sont vérifiées (c'est le principe de la gestion par mot de passe crypté). Cette fonction est à relier au **principe d'authentification** : il s'agit de garantir l'origine d'une information en permettant la reconnaissance d'une personne afin de lui délivrer un accès à un contenu pas forcément chiffré. C'est l'exemple de la signature numérique qu'on utilise avec un couple de clés (l'une est secrète et permet de chiffrer, l'autre est publique et permet de vérifier la signature). Une bonne solution de cryptographie doit aussi permettre un contrôle d'**intégrité** des données transmises : toute modification d'une information chiffrée au

[9] Bruce SCHNEIER, *Cryptographie appliquée*, seconde édition, International Thomson Publishing France, 1997

départ et envoyée sur le réseau est détectée. Finalement, la cryptographie permet également l'application du **principe de non-répudiation** : un expéditeur d'un message ne peut pas nier l'avoir envoyé (une fois chiffré avec sa propre clé, l'individu ne peut pas refuser d'admettre que le message est bien de lui).

Cet aperçu rapide des fonctions de la cryptographie permet d'emblée de voir les applications qu'on peut en tirer dans le milieu médical : bien crypter des données médicales concernant un patient permet d'éviter une lecture par une personne non autorisée, de s'assurer de l'identité des lecteurs, de veiller au respect des informations transmises (puisque toute modification est visible, le cryptage ayant changé) et de prouver qu'un fichier a bien été envoyé par la bonne personne. Toutes ces possibilités sont encore loin d'être exploitées dans le milieu hospitalier : l'objectif reste celui de se conformer à la loi, c'est à dire d'assurer la sécurité du contenu des informations et de l'expédition vers la bonne personne, ce qui, il faut l'admettre, nécessite d'importants efforts au sein des Directions des Systèmes d'Information et de l'Organisation d'hôpitaux (**DSIO**) décidés à rendre communicant leur établissement. Il ne faut pas oublier qu'avant de se positionner sur la constitution d'un réseau de santé et sur les choix techniques qui en découlent, le réseau interne de l'hôpital doit lui-même être sécurisé. Il s'agit d'un préalable nécessaire avant tout échange avec l'extérieur. Il n'est donc pas étonnant que la constitution de réseaux de santé ait été si lente et que les enjeux du cryptage des données n'aient pas été immédiatement perçus.

*b) Les origines de la cryptographie :*

Pour comprendre ce retard dans la perception des avantages de la cryptographie, il est nécessaire d'avoir un éclairage historique, assez révélateur de la vision qui a longtemps dominé les esprits et la réglementation en France sur le sujet.

La Grèce, avec Sparte, la plus guerrière des cités grecques, a conçu le premier procédé de chiffrement militaire. Dès le 5ème siècle avant Jésus Christ elle employait un instrument appelé *"scytale"*, le premier utilisé en cryptographie et fonctionnant selon le principe de transposition (les lettres sont mélangées). Il consistait en un axe de bois autour duquel on enroulait, en spires jointives, un ruban de papyrus, cuir ou parchemin. Le texte était écrit (en lignes droites successives parallèles à l'axe) sur le ruban qui était ensuite déroulé tel quel par le destinataire. Ce dernier réenroulait la bande sur le bâton de même diamètre que le premier. Les mots chevauchaient alors les spires et le texte se reformait. Des historiens grecs tels que Thucydide ou Plutarque mentionne l'utilisation de ce procédé par les Spartes vers 475 avant Jésus Christ pour ordonner à un général trop ambitieux de s'allier ou même 100 ans plus tard quand un général spartiate répond à une accusation d'insubordination. Les

Grecs sont aussi à l'origine de procédés stéganographiques tels que des trous représentant les lettres de l'alphabet sur un disque. Le chiffrement consistait à passer un fil de façon aléatoire dans les différents trous. Un autre procédé était de marquer d'une piqûre d'épingle dans un livre ou tout autre document les lettres dont la succession fournit le texte secret (notamment utilisé par les Allemands pendant le premier conflit mondial). Polybe, écrivain grec, est à l'origine du premier procédé de chiffrement par substitution. [10]

Pendant le Moyen-Age la cryptologie évolue faiblement. Seuls les moines en Europe utilisent cette science plus par jeu que par nécessité. Alors que la féodalité du Moyen-Age n'avait que peu fait avancer la cryptographie, l'Italie en 1467 a réussi avec Léon Batista Alberti, à faire fortement évoluer la science des écritures secrètes. Il inventa la substitution polyalphabétique, procédé permettant la correspondance de nombreux alphabets cryptés en un seul clair. Ce système sera amélioré au 16ème siècle par l'utilisation d'un procédé "*autoclave*" (le message lui-même est la clé). C'est Cardan, médecin et mathématicien milanais qui invente ce procédé. L'inventeur du second procédé *"autoclave",* plus performant, est un français du nom de Blaise de Vigenère. Pendant la Renaissance, la cryptographie devient un art, *ars occulte scribendi* et elle acquiert une certaine importance dans les correspondances des princes avec leurs ambassadeurs. Très vite, les cryptologues insistent sur l'importance de la cryptanalyse dans la politique. Un homme, Antoine Rossignol intervient pour la royauté contre les huguenots assiégeant la ville de Réalmont en 1628. Il décrypte un message destiné aux Protestants en une heure annonçant la fin de munitions très proche des huguenots. Surprise, l'armée royale fit capituler la ville malgré les remparts imposants. Avec ce haut fait, commença la carrière de celui qui allait devenir le premier cryptologue professionnel de France. Une des plus grandes contributions de la famille Rossignol (car cette science plus proche d'un art fut transmise sur plusieurs générations) fut de démontrer de façon éclatante à ceux qui gouvernaient la France l'importance du décryptage dans la détermination de leur politique. Cela aboutit à la création d'un bureau spécialisé au 18ème siècle, le Cabinet Noir. D'autres s'édifièrent dans toute l'Europe. En France, il n'a cessé de dépérir à partir de la Révolution pour totalement disparaître.

Mais simultanément allait naître une invention qui révolutionnera la cryptographie : le télégraphe. Cette nouvelle innovation dans les flux d'information suscita de nouvelles vocations à la cryptologie. Il n'est donc pas étonnant de voir aujourd'hui le même développement avec la généralisation des Nouvelles Technologies de l'Information et de la Communication. Dans le domaine militaire, le télégraphe allait offrir aux généraux et autres

[10] Cf. l'ouvrage de Jacques STERN : *La science du secret*, Odile Jacob

officiers l'occasion d'exercer un contrôle continu et instantané des forces armées. Dans *La cryptographie militaire*[11], publié en février 1883, Auguste Kerckhoffs von Nieuvenhof décline les principes fondamentaux de cette science. Cet ouvrage continue de guider les cryptologues contemporains. Il affirme notamment que toute méthode de chiffrement peut être connue de l'ennemi et que la sécurité du système ne dépend que du choix des clés. Ce principe dit "de Kerckhoffs" sera à mettre en relation avec l'évolution de l'encadrement juridique du chiffrement en France que nous verrons un peu plus loin dans le mémoire.

*c) Histoire récente de la cryptographie :*

A l'aube du 20ème siècle, le savoir en cryptographie et cryptanalyse est important[12]. L'apport de Kerckhoffs a été important : il a synthétisé les différentes méthodes de chiffrage des données (principe de la transposition, principe de la combinaison du chiffre avec une interversion de l'alphabet et principe de la représentation symbolique de groupes de lettres). C'est dans le domaine militaire que l'on verra le plus cette science des écritures secrètes. On y enseigne les systèmes à simple, à double clé et à clé variable… La France, meilleure nation cryptologique, aborde le premier conflit mondial avec de l'avance sur l'Allemagne qui pense toujours être la nation suprême par excellence et qui reste sur ses acquis. En effet, ils ne se sont pas rendu compte de l'importance de la cryptanalyse mettant à l'épreuve la cryptographie. Des hauts faits historiques ont été imprégnés par la cryptologie comme la résolution de l'affaire Dreyfus. Le bureau 40 a été crée suite au désir de décrypter les messages allemands. C'est un organisme composé de plusieurs passionnés de cryptologie, installé en Angleterre. Leur première découverte fut la méthode de la substitution simple, qui consiste à remplacer chaque même lettre en clair par une seule unité cryptographique, toujours la même. L'un des moyens utilisés pour le décryptement fut le repérage radiogoniométrique. Ils déchiffrèrent les messages des *U-boote,* (sous-marins), qui étaient chiffrés avec un code à quatre lettres de la flotte de surface et surchiffrés par une transposition à tableau. Les Allemands appelaient *"Gamma epsilon"* le surchiffrement pour les sous-marins classiques et *"Gamma-u"* celui des sous-marins à grand rayon d'action. Le mot clé était différent. Environ quinze mille télégrammes secrets allemands furent décryptés par le Bureau 40 d'octobre 1914 à février 1919. La première Guerre Mondiale fut une suite de véritables batailles sur le plan technique. Avant, l'importance de la cryptologie était secondaire ; après, elle était primordiale. La cause directe de ce développement était l'accroissement énorme du volume des communications radio.

[11] Auguste Kerckhoffs : La cryptographie militaire, Journal des sciences militaires, volume IX, pages 5 à 38, janvier 1883 et pages 161 à 191 février 1883

[12] Cf. le livre de David KHAN *The Codebreakers* très complet pour la partie pré-informatique contemporaine et qui a contribué à faire sortir la cryptographie du domaine militaire

En 1939, peu avant la seconde Guerre Mondiale, le Capitaine Baudoin, un français, fait paraître son ouvrage marquant la transition entre la cryptologie classique et la cryptologie moderne. Durant la Seconde Guerre Mondiale, la cryptographie connût un développement considérable notamment avec l'utilisation de la machine ENIGMA. Il y eu en fait plusieurs modèles de cette célèbre machine, première à produire automatiquement du texte crypté. Le modèle A d'ENIGMA est lourd et volumineux, un clavier de machine à écrire (de type QWERTY) est utilisé pour la saisie des messages. Dans les faits, la machine pouvait être utilisée comme une machine à écrire standard et cela même en plein milieu de l'encodage d'un texte. Les modèles C et D étaient portables et cryptographiquement différents des modèles précédents. L'armée allemande redessine la machine et c'est en juin 1930 que la version standard finale, nommée ENIGMA I commence à être utilisée par l'armée. Tous les niveaux du gouvernement et de la défense se servent d'ENIGMA pour communiquer. Ils sont tellement convaincus que leur codes ne peuvent être brisés, qu'ils transmettront au vu et su de tous. Malgré le haut niveau de cryptage, les secrets transmis via ENIGMA furent régulièrement et dans le détail, déchiffrés par les cryptanalystes alliés comme Alan Turing.

Depuis, les services secrets ont utilisé toutes sortes de codages et de moyens cryptographiques pour communiquer entre agents et gouvernements, de telle sorte que les "ennemis" ne puissent pas comprendre les informations échangées. La cryptologie a alors évolué dans ces milieux fermés qu'étaient les gouvernements, les services secrets et les armées. Ainsi, très peu de gens, voire personne n'utilisait la cryptographie à des fins personnelles. C'est pourquoi, pendant tant d'années, la cryptologie est restée une science discrète. De nos jours en revanche, il y a de plus en plus d'informations personnelles qui doivent rester secrètes ou confidentielles. En effet, les informations échangées par les banques ou un mot de passe ne doivent pas être divulgués et personne ne doit pouvoir les déduire. C'est pourquoi ce genre d'informations est crypté. L'algorithme de cryptographie DES[13] par exemple, est utilisé massivement par les banques pour garantir la sécurité et la confidentialité des données circulant sur les réseaux bancaires. Le système d'exploitation Unix, lui aussi, utilise ce procédé pour crypter ses mots de passe. C'est pour des mêmes raisons de sécurité sur Internet, et par un besoin humain d'intimité que la cryptographie à des fins purement personnelles s'est développée. En effet, lorsque l'on envoie un message électronique par Internet, on peut préférer qu'il reste discret vis à vis de la communauté Internet, voire qu'il ne soit compréhensible que par le destinataire du message. En d'autres termes, la cryptographie peut servir si l'on veut envoyer un message confidentiel à quelqu'un. Cela est aujourd'hui possible grâce à la formidable distribution de logiciels gratuits

[13] Les principaux algorithmes utilisés aujourd'hui comme RSA seront détaillés dans la partie technique à partir de la page 15 de ce mémoire

permettant d'utiliser de la cryptographie "forte" très facilement. C'est le cas du logiciel PGP (Pretty Good Privacy) développé par Philip R. Zimmerman en 1991 longtemps interdit en France malgré son utilisation mondiale. Ce sont pour toutes ces raisons que la cryptologie s'est énormément renforcée, et que finalement, elle est passée d'un monde fermé comme les armées ou les services secrets à un monde ouvert à tout utilisateur. Elle tend désormais à se généraliser dans toutes les transmissions de données nominatives, relatives à un patient par exemple, entre médecins ou entre différents hôpitaux.

Mais ce cheminement a été rendu difficile en France à cause de la position des gouvernements qui sont longtemps restés sur une interprétation rigide et stricte de la cryptographie, souhaitant préserver un certain contrôle sur cette technologie qui devait avant tout servir au monde du renseignement et lutter contre les agissements criminels dont le chiffrement peut effectivement faciliter la dissimulation. Ce qui n'a pas empêché depuis une vingtaine d'années cette technologie d'évoluer sur le plan technique et d'aboutir à certains standards qu'il peut être utile de connaître, ou tout du moins d'en comprendre le concept.

## 2) Une évolution des techniques permettant un renforcement de la sécurité :

Aborder l'aspect purement technique de la cryptographie n'a qu'un intérêt professionnel très limité pour un directeur d'hôpital (à moins d'être curieux et de vouloir comprendre ce que signifient les spécifications techniques d'un logiciel[14]). Ce qui est essentiel, c'est de comprendre que cette science, en se détachant du domaine purement militaire, a fait d'importants progrès pour renforcer la sécurité et que certains concepts simples et certaines normes reconnues doivent être intégrés dans la réflexion concernant la protection des données. L'idée est de montrer que parler de "messagerie ou d'échanges de données sécurisées" ne signifie pas grand chose en soi et que cette simple indication sur l'emballage d'un produit ou dans la présentation d'un réseau n'évacue la réflexion sur la sécurité.

### *a) Clés symétriques et asymétriques :*

Les petites structures hospitalières partent souvent du principe qu'à partir du moment où le réseau de l'hôpital est sécurisé (soit par l'installation de firewalls ou pare-feux réputés), les solutions de cryptographie ne s'imposent pas. La réflexion est identique lorsque le système d'information est complètement fermé (pas de rattachement à l'Internet ou à tout autre réseau). En fait, ce type d'organisation consiste simplement à se prémunir d'une attaque extérieure et ne permet en aucun cas de bénéficier des avantages déclinés précédemment.

[14] Les lecteurs férus de mathématiques apprécieront notamment l'ouvrage de A.MENEZES, P.VAN OORSCHOT et S.VANSTONE *Handbook of Applied Cryptography*, CRC Press Inc. 1997

Mais si la cryptographie se conjugue avec la sécurité, les deux ne sont pas substituables. De plus, de par la généralisation du Réseau de Santé Social et de la multiplication des réseaux ville-hôpital, il est devenu quasi impossible d'ignorer le problème du cryptage des données. Ou bien il est intégré dans des solutions "clé en main" (un peu à l'image du RSS) ou bien il faut étudier concrètement les apports réels de la cryptographie et organiser des solutions efficaces dans l'établissement. Pour cela, il est indispensable de comprendre comment on peut être amené à juger de l'efficacité d'un logiciel de cryptographie dont la force réside dans le type d'algorithme utilisé. La compréhension du détail n'est pas nécessaire surtout dans ses fondements mathématiques mais un aperçu donne clairement une idée des enjeux et des problématiques actuelles liées à la qualité du chiffrement.

Un **algorithme de cryptographie** ou un **chiffrement** est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une *clé* (un mot, un nombre ou une phrase), afin de crypter le texte en clair. Avec des clés différentes, le résultat du cryptage variera également. La sécurité des données cryptées repose entièrement sur deux éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clé. Un **système de cryptographie** est constitué d'un algorithme de cryptographie ainsi que des clés et des protocoles nécessaires à son fonctionnement.

En **cryptographie conventionnelle**, également appelée **cryptage à clé secrète** ou de **cryptage à clé symétrique**, une seule clé suffit pour le cryptage et le décryptage. Les algorithmes à clé secrète sont surtout utilisés pour assurer la confidentialité d'une information grâce à l'algorithme de chiffrement : la clé doit être connu par le destinataire. La norme de cryptage de données (**DES**) est un exemple de système de cryptographie conventionnelle largement utilisé par le gouvernement fédéral des Etats-Unis.

Mais l'exemple le plus célèbre dans l'histoire de la cryptographie est celui de **l'algorithme de César**[15]. Il combine les deux opérations mathématiques de base que sont la substitution et la transposition. Le chiffrement de substitution est un exemple extrêmement simple de cryptographie conventionnelle. Il substitue une information par une autre. Cette opération s'effectue généralement en décalant les lettres de l'alphabet. Dans le cas code secret de Jules César, l'algorithme constitue à décaler les lettres de l'alphabet et la clé correspond au nombre de caractères de décalage. On ne peut pas évoquer la cryptographie sans citer cet exemple : si l'on code le mot SECRET à l'aide de la valeur 3 de la clé de César, l'alphabet est décalé de manière à commencer à la lettre D. Ainsi, D = A, E = B, F = C, etc. Avec ce procédé, le texte en clair SECRET est crypté en VHFUHW. On effectue alors une opération de *transposition*. Pour autoriser un autre utilisateur à lire le texte chiffré, il faut donner la valeur de la clé (égale

[15] On retrouve cet exemple dans absolument tous les ouvrages sur la cryptographie.

à 3 ici) et l'algorithme. Evidemment, ceci est considéré comme une cryptographie extrêmement vulnérable de par les standards actuels. Le cryptage conventionnel comporte des avantages. Il est très rapide et s'avère particulièrement utile pour les données véhiculées par des *moyens de transmission* sécurisés. Toutefois, il peut entraîner des coûts importants en raison de la difficulté à garantir la confidentialité d'une clé de cryptage lors de la distribution. Mais cette méthode convenait à César et illustre le mode de fonctionnement de la cryptographie conventionnelle.

Les problèmes de distribution des clés sont résolus par la **cryptographie à clé publique**. On parle aussi de **cryptographie à clé asymétrique**. Ce concept a été introduit par Whitfield Diffie et Martin Hellman en 1975. La cryptographie à clé publique est un procédé asymétrique utilisant une *paire* de clés pour le cryptage : une **clé publique** qui crypte des données et une **clé privée** ou **secrète** correspondante pour le décryptage. On peut ainsi publier sa clé publique tout en conservant sa clé privée secrète. Le principe est que tout utilisateur possédant une copie de votre clé publique peut ensuite crypter des informations que vous êtes le seul à pourvoir lire. Même les personnes que vous ne connaissez pas personnellement peuvent utiliser votre clé publique. D'un point de vue informatique, il est impossible en l'état actuel des connaissances mathématiques et de la puissance de calcul des processeurs, de deviner la clé privée à partir de la clé publique. Tout utilisateur possédant une clé publique peut crypter des informations, mais est dans l'impossibilité de les décrypter. Seule la personne disposant de la clé privée correspondante peut les décrypter. La cryptographie à clé publique présente un avantage majeur : en effet, elle permet d'échanger des messages de manière sécurisée sans aucun dispositif de sécurité. L'expéditeur et le destinataire n'ont plus besoin de partager des clés secrètes via une voie de transmission sécurisée. Les communications impliquent uniquement l'utilisation de clés publiques et plus aucune clé privée n'est transmise ou partagée. **Elgamal** (d'après le nom de son inventeur, Taher Elga-mal), **RSA** (d'après le nom de ses inventeurs, Ron Rivest, Adi Shamir et Leonard Adleman) et **DSA,** l'algorithme de signature numérique élaboré par David Kravitz, sont des exemples de systèmes de cryptographie à clé publique. **DH** ou **Diffie-Hellman** (du nom de ses inventeurs) est un système qui résout le problème de l'échange de clés pour les algorithmes symétriques, mais il ne fonctionne pas avec des clés en lui-même.

La cryptographie conventionnelle étant auparavant la seule méthode pour transmettre des informations secrètes, les coûts de transmission et de distribution sécurisées des clés ont relégué son utilisation aux institutions disposant de moyens suffisants, telles que des gouvernements et des banques. Le cryptage à clé publique représente une révolution technologique qui offre à tout citoyen la possibilité d'utiliser une cryptographie invulnérable.

C'est évidemment une solution à base de chiffrement à clé publique qui doit être privilégiée dans les Systèmes d'Informations Hospitalières.[16]

*b) Principales utilisations des algorithmes de cryptographie et la garantie de la sécurité :*

L'un des principaux avantages de la cryptographie à clé publique est qu'elle offre une méthode d'utilisation des **signatures numériques**. Celles-ci permettent au destinataire de vérifier leur authenticité, leur origine, mais également de s'assurer qu'elles sont intactes. Ainsi, les signatures numériques à clé publique garantissent l'**authentification** et l'**intégrité** des données, principes vus précédemment.

Elles fournissent également la fonctionnalité de **non répudiation** (afin d'éviter que l'expéditeur ne prétende qu'il n'a pas envoyé les informations). Ces fonctions jouent un rôle tout aussi important pour la cryptographie que la confidentialité, sinon plus. Une signature numérique a la même utilité qu'une signature manuscrite. Cependant, une signature manuscrite peut être facilement imitée, alors qu'une signature numérique est pratiquement infalsifiable. De plus, elle atteste du contenu des informations, ainsi que de l'identification du signataire. Certains systèmes d'informations privilégient l'utilisation des signatures par rapport au cryptage.

A ces algorithmes de signature, s'ajoute de manière quasi générale une fonction de **hachage** (ou fonction de **condensation**). Elle permet de transformer un message de longueur quelconque en un condensé de longueur fixe (160 bits pour le logiciel PGP par exemple). Cette fonction est dite à sens unique car il est impossible (a priori) de retrouver le message original à partir de ce condensé. Dans la pratique, on applique déjà la fonction de hachage au message et ensuite l'algorithme de signature.

La garantie de la sécurité est également liée à la **clé** (c'est l'un des principes de Kerckhoffs[17]). Une clé est une valeur utilisée dans un algorithme de cryptographie, afin de générer un texte chiffré. Les clés sont en réalité des nombres extrêmement importants. La taille d'une clé se mesure en bits et le nombre correspondant à une clé de 1024 bits est gigantesque. Dans la cryptographie de clé publique, plus la clé est grande, plus la sécurité du texte chiffré est élevée. Cependant, la taille de la clé publique et de la clé secrète de cryptographie conventionnelle sont complètement indépendantes. Une clé conventionnelle de 80 bits est aussi puissante qu'une clé publique de 1024 bits. De même, une clé

[16] Attention, on n'utilise jamais le chiffrement à clé publique pour chiffrer d'importantes quantités de données (tel qu'un fichier). PGP par exemple n'utilise pas RSA pour chiffrer mais le Triple DES ou IDEA afin de chiffrer le fichier, la clé Triple DES ou IDEA étant elle-même chiffrée avec RSA ou équivalent

[17] Cf. la partie historique et militaire de la cryptographie de ce mémoire, notamment la page 13

conventionnelle de 128 bits équivaut à une clé publique de 3000 bits. Encore une fois, plus la clé est grande, plus elle est sécurisée, mais les algorithmes utilisés pour chaque type de cryptographie sont très différents. Même si les clés publiques et privées sont liées par une relation mathématique, il est très difficile de deviner la clé privée uniquement à partir de la clé publique. Cependant, la déduction de la clé privée est toujours possible en disposant de temps et de puissantes ressources informatiques.

Ainsi, il est très important de sélectionner des clés de tailles correctes, suffisamment grandes pour être sécurisées, mais suffisamment petites pour être utilisées assez rapidement. Plus la clé est grande, plus sa durée de sécurisation est élevée. Si les informations que l'on souhaite crypter doivent rester confidentielles pendant plusieurs années, il faut utiliser une clé correspondant à un nombre de bits extrêmement élevé. Il fut un temps où une clé symétrique de 56 bits était considérée comme extrêmement sûre. En janvier 2000, le collectif d'internautes Distributed.net a fait voler en éclats la clé à 56 bits du spécialiste de la sécurité Communication & Systèmes (ex Compagnie des Signaux). Distributed.net, constitué de plus de 38 000 internautes dans plus de 140 pays a mis deux mois à réaliser cet exploit. Yazid Sabeg, président du groupe CS expliquait que "*si le groupe Distributed.net s'était attaqué au même défi, crypté avec une clef à 128 bits, en utilisant la même méthode de la recherche exhaustive, il aurait mis 2 72 fois plus de temps pour trouver la solution. Ce qui représente plusieurs milliards de millions d'années !*". On verra que la législation française a très longtemps limité le nombre de bits des clés de chiffrement et la libéralisation de l'utilisation des solutions de cryptographie dite "forte" (c'est à dire 128 bits) n'est effective que depuis les décrets de mars 1999. Ainsi, le Réseau Santé Sociale (RSS) développe enfin des clés de chiffrement à 128 bits alors qu'elles n'étaient que de 40 bits au départ.[18]

Pour un directeur d'hôpital chargé de mettre en place des solutions de cryptographie, il est également nécessaire d'évoquer rapidement les différents algorithmes utilisés sur le marché qu'on retrouve dans la plupart des logiciels. Le but est seulement de démystifier un peu des termes trop souvent ésotériques. L'évolution de la cryptographie dans les années à venir dépendra du choix des prochains standards parmi ceux évoqués ci-dessous.

L'**algorithme de chiffrement symétrique** le plus utilisé est le **DES** (Data Encryption Standard), choisi par le gouvernement américain comme standard en 1976 après examen par les spécialistes de la célèbre NSA (National Security Agency). La taille de la clé est de 56 bits et cet algorithme n'est plus efficace aujourd'hui pour protéger avec efficacité des informations sensibles (l'Electronic Frontier Foundation a développé en 1998 des systèmes

[18] Au moment où ce mémoire est écrit, le RSS n'avait pas encore adopté de chiffrement avec des clés de 128 bits.

permettant de "casser la clé" en quelques heures seulement). Le DES, au cours des années, a été amélioré avec un chiffrement à 2 clés de 56 bits.

On utilise désormais le **triple DES** (soit on utilise 3 clés successivement d'où un cryptage avec une clé équivalente à 168 bits, soit on utilise 2 clés de 56 bits avec triple application du DES, soit un cryptage avec une clé résultante de 112 bits).

Mais, l'avenir appartient à d'autres algorithmes. Le NIST (National Institute of Standards and Technology) a lancé un appel d'offre le 12 septembre 1997 afin de remplacer le DES par une nouvelle norme l'**AES** qui deviendra un standard en 2001. Pour le moment, les algorithmes plus efficaces que le DES sont l'**IDEA** (International Encryption System) fonctionnant avec une clé de 128 bits, le **RC6** de la société RSA Data Security et **CAST** (Carlisle Adams et Stafford Tavares de Northern Telecom (Nortel)).[19]

L'**algorithme de chiffrement asymétrique** (ou **à clé publique**) le plus couramment rencontré est le **RSA** évoqué précédemment. Il permet de faire de la cryptographie à clé publique ainsi que de la signature. Il repose sur le problème de la factorisation des grands nombres. Dans la réglementation américaine, la valeur de la clé pour un logiciel voué à l'exportation a longtemps été limitée à 512 bits et il s'avère qu'il est plutôt conseillé aujourd'hui, afin de garantir une réelle sécurité avec le RSA, une longueur minimale de 768 bits voire 1024 bits. On peut signaler l'existence d'autres algorithmes de chiffrement asymétrique comme **ElGamal**.

En ce qui concerne les algorithmes de signature, à côté de **RSA**, se trouve le **DSA** avec une clé dont la taille varie de 512 à 1024 bits. Pour la fonction de hachage, on rencontre, dans les spécifications techniques des logiciels, **MD5** (Message Digest version 5) déconseillé malgré un risque minime et surtout **SHA** (Secure Hash Algorithm) encore inviolé. Ce rapide aperçu des algorithmes utilisés couramment en cryptographie est à relier avec la problématique juridique de l'utilisation de ces solutions, qui sera évoquée ultérieurement.

*c) Les Infrastructures de Gestion de Clés (IGC) ou Public Key Infrastructures (PKI) :*

Pour clore l'aspect technique de la cryptographie, il est important d'aborder, dans le cadre d'une vision prospective, les IGC[20]. Quand les réseaux de santé se seront généralisés à très grande échelle en France, l'organisation des IGC sera peut-être le nouveau casse-tête du Directeur du SIH même si ce paragraphe, qui résume l'essentiel des utilisations de la cryptographie, se veut porteur d'une solution miracle.

[19] Tous ces acronymes sont cités dans une vision prospective. Le triple DES l'algorithme le plus connu et le plus utilisé mais l'IDEA risque de lui succéder.

[20] Cf. le rapport de J.GOTTEL, E.LARCHER, G.LEBRETON, R.NGUYEN : *Public Key Infrastructures (PKI)*, mastère Ecole Nationale Supérieure des Télécommunications, mai 1999

Jusqu'à la fin des années soixante-dix, la cryptologie ne connaissait que les systèmes à clé symétrique. Mais, en novembre 1976, Diffie et Hellman ont émis l'idée de systèmes à clé non-symétrique. Il s'agissait là d'une révolution conceptuelle, dont l'exemple le plus connu est l'algorithme **RSA**. Dans ces systèmes, les clés de chiffrement et de déchiffrement sont différentes. La connaissance de l'une ne doit pas permettre en pratique de retrouver l'autre. Une des deux clés peut être publiée sans nuire au secret de l'autre. Avec un tel système, n'importe qui peut envoyer à A un message chiffré. Il suffit pour cela d'utiliser la clé publique de A. Seul ce dernier, ayant sa clé privée, aura la capacité de le déchiffrer. Par ailleurs, si A veut signer un message, il lui suffit cette fois d'utiliser sa clé privée pour chiffrer un condensé du message. Alors toute personne pourra déchiffrer la signature à l'aide de la clé publique et vérifier qu'il s'agit bien du condensé du message signé.

Ces principes ainsi résumés paraissent au premier regard quasi miraculeux, mais ils ont aussi un coût. Tout d'abord, les clés et les blocs élémentaires de chiffrement sont en général plus longs. La complexité de calcul d'un chiffrement est beaucoup plus grande que dans les systèmes symétriques. De plus, les systèmes asymétriques reposent sur des problèmes mathématiques, comme la factorisation des grands nombres, où aucune solution radicale n'a été encore trouvée. Tout le problème est dans le "encore", car chaque jour la recherche mathématique fait des progrès dans ces domaines qui deviennent l'enjeu de compétitions.

Enfin la notion de clé publique ouvre d'autres horizons et appelle certaines questions dont la principale est : comment être sûr que la clé publique de A est bien celle que je trouve dans l'annuaire ? On arrive alors au problème épineux de la gestion, de la certification des clés dans les **Infrastructures de Gestion de Clés** ou **IGC**. On rencontre plus souvent le terme anglais de **PKI** (**Public Key Infrastructures**). Les nouveaux types d'applications comme les messageries électroniques transitant sur des réseaux ouverts, les nouvelles configurations de réseaux (réseaux ouverts, apparition de routeurs, firewalls, etc.) ont fait évoluer les besoins de sécurité des systèmes d'information. Aujourd'hui, les utilisateurs mettent en oeuvre des opérations de plus en plus complexes à partir de leur propre poste de travail et souhaitent voir la sécurité au plus près de leurs applications. La cryptographie symétrique, qui implique une gestion contraignante de clés, s'adapte difficilement aux réseaux ouverts où un utilisateur ne connaît pas forcément son interlocuteur, utilise un canal de communication publique, ou échange des informations avec une communauté d'utilisateurs importante. La cryptographie asymétrique, quant à elle, on l'a vu, facilite la gestion des clés puisqu'elle permet de sécuriser des communications sans qu'aucun échange de secret préalable ne soit nécessaire. Dans un modèle d'intégrité, la fonction de

sécurité est mise en oeuvre par l'initiateur de l'échange par signature d'un document grâce à sa propre clé privée, de sorte que son interlocuteur puisse vérifier la signature en utilisant la clé publique correspondante. Dans un modèle de confidentialité, un premier correspondant utilise la clé publique de son interlocuteur de sorte que seul cet interlocuteur puisse déchiffrer le message sécurisé grâce à sa propre clé privée.

Grâce à ces systèmes asymétriques, divers types d'applications peuvent être sécurisés, comme, par exemple, la messagerie électronique, l'accès à des serveurs d'informations (Web), la gestion d'infrastructures réseaux etc. Selon l'utilisation faite de la cryptographie asymétrique, il est possible d'assurer des fonctions de sécurité d'authentification de l'origine d'un message, de détection de perte d'intégrité, de non-répudiation d'une action et de protection de la confidentialité. Mais ces fonctions de sécurité ne peuvent être garanties que si l'auteur est bien le seul détenteur du secret qu'est la clé privée. De même, la sécurité du système fait appel à la confiance dans la relation qui lie l'utilisateur à un bi-clé. Un bi-clé est caractérisé par des paramètres cryptographiques (longueur de clé, période de validité, algorithme) tandis que l'utilisateur dispose d'une identité propre ou d'une fonction pour une période donnée. L'ensemble de ces paramètres relatifs au bi-clé et à l'utilisateur est contenu dans un fichier appelé **certificat de clé publique**. Pour que la relation entre l'utilisateur et le bi-clé soit de confiance, il est indispensable que le certificat soit signé par un tiers qui cautionne la véracité des informations contenues dans le certificat. Cette autorité appelée **autorité de certification** (notée **AC**) signe avec sa propre clé privée le certificat de clé publique. L'ensemble des ressources mises en oeuvres pour sécuriser des bi-clés par la génération et la gestion complète de certificats de clés publiques est appelé **infrastructure de gestion de clés** (**IGC**). Une IGC est un système distribué constitué de :

– ressources informatiques (matérielles, logicielles, réseau),
– ressources cryptographiques,
– ressources humaines (personnels de l'infrastructure).

Ces ressources agissent pour le compte d'utilisateurs finaux pouvant être des personnes, des organismes, des matériels ou d'autres composantes d'une infrastructure. Différents types de composantes tels que des autorités de certification, des autorités d'enregistrement, un service de publication, éventuellement un horodateur, interagissent pour offrir aux utilisateurs finaux des services de confiance. Les prestations réalisées par une IGC sont l'enregistrement d'un utilisateur, la génération de certificats, la publication et la révocation de certificats, ainsi que d'autres services qui peuvent varier selon les besoins.

L'enregistrement, service rendu par une autorité d'enregistrement, consiste en la vérification d'informations propres au demandeur de certificat, avant la génération de son certificat. Après l'enregistrement, le gabarit d'un certificat est transmis pour signature à l'autorité de certification. Cette dernière génère le certificat et le transmet au service de publication, afin de le rendre disponible aux utilisateurs potentiels de la clé publique qu'il contient. Les certificats sont publiés par le biais d'un vecteur de publication pouvant être une disquette, un document papier, un serveur d'information ou un annuaire. Lorsqu'un utilisateur perd ou divulgue sa clé privée ou que les informations contenues dans son certificat sont ou deviennent fausses (falsification de l'identité, perte d'intégrité de la clé publique contenue dans le certificat), alors le certificat n'est plus de confiance et son utilisation ne peut plus garantir aucune fonction de sécurité. Il est alors révoqué par l'autorité de certification et son nouveau statut est transmis au service de publication. Un utilisateur n'accorde sa confiance à une signature numérique que s'il a confiance dans le certificat qu'il utilise pour la vérifier et, par extension, dans le générateur de certificat, c'est-à-dire à l'ensemble de l'infrastructure.

La question future pour les hôpitaux sera de savoir, lorsque le réseau mis en place sera très important, s'il faudra internaliser cette masse de travail ou bien, à l'image du privé, de l'externaliser. Toute la problématique des IGC réside en effet dans :

– l'adéquation des services rendus par l'IGC aux besoins réels des utilisateurs. Les spécification techniques doivent couvrir les besoins des applications sécurisées grâce à l'IGC et répondre aux attentes des utilisateurs finaux. D'autre part, les solutions opérationnelles mises en oeuvre doivent tenir compte de l'existant et proposer des solutions réalistes du point de vue des coûts et des ressources humaines disponibles.

– le niveau de confiance généré par l'IGC et la possibilité de fournir des indicateurs de confiance aux utilisateurs finaux et aux partenaires de l'hôpital.

En tant que générateur de confiance, une IGC doit disposer des procédures de fonctionnement interne, de politiques de certification, de déclarations quant aux services effectivement rendus et de spécifications techniques précises. Pour cela, des documents doivent décrire l'IGC en termes opérationnels, techniques, organisationnels, ainsi qu'en termes de services rendus à l'utilisateur. La reconnaissance de l'IGC par un organisme de confiance, un schéma d'accréditation national ou propre à une application représentent également un élément de confiance plus formel qui peut résulter d'une étude de l'ensemble des autres indicateurs. Dans le cadre des communications avec d'autres partenaires, des accords doivent être conclus, sous l'égide d'une autorité compétente. Cette autorité doit être capable de déterminer si les modalités de gestion mises en oeuvre par deux IGC sont équivalentes et si leur coopération dans le cadre d'une ou plusieurs applications peut être envisagée.

Les infrastructures de gestion de clés sont des systèmes émergents qui répondent aux besoins de sécurité des systèmes d'information. Elles offrent des moyens techniques, organisationnels et humains au service de la génération de la confiance. Des acteurs issus de domaines de compétences des plus divers et notamment la santé s'adonnent aujourd'hui à cette nouvelle activité de gestion de certificats, dans le but de sécuriser leurs applications. Ils se positionnent soit en tant qu'opérateurs de service, soit en proposant un produit matériel ou logiciel de déploiement d'IGC, soit en déployant une infrastructure au sein même de leur activité. Les enjeux liés au développement des IGC désormais identifiés, les efforts commerciaux, nationaux et internationaux tendent aujourd'hui à se fédérer pour assister et accélérer le développement des IGC.

## 3) Une évolution juridique attendue permettant aujourd'hui de crypter librement:

Cette évolution permettra sans nul doute d'offrir un peu plus de confort pour les responsables de réseaux communicants de santé. Mais à l'heure actuelle, cette préoccupation sur la gestion des PKI n'est qu'émergente et beaucoup d'hôpitaux choisiront vraisemblablement alors des solutions "clés en main".

Pour le moment, c'est surtout le revirement récent (et donc tardif) du droit français encadrant l'usage de la cryptographie qui va peut-être susciter un nouvel attrait pour le renforcement de la sécurité des données médicales télétransmises. Il est donc forcément intéressant de retracer cette évolution afin de voir quelles sont les nouvelles marges de manœuvres offertes par l'Etat.[21]

### *a) Un cadre juridique longtemps resté très restrictif en France :*

Dans le **décret du 18 avril 1939**, le contrôle cryptologique est rattaché à la notion de *matériel de guerre de 2ème catégorie*. Tout commerce, fabrication ou utilisation de moyens de cryptologie est totalement prohibé et seules des dérogations ponctuelles sont possibles. Ce régime est bien adapté au contexte diplomatique et militaire de l'époque et trouve toute sa légitimité pendant la Guerre Froide, mais rapidement des limitations se font sentir. De multiples difficultés apparaissent avec l'accroissement de la demande privée en produits de sécurité. La lourdeur administrative est de moins en moins compatible avec les besoins industriels et commerciaux modernes, surtout à partir de 1957 avec la création de la Communauté Economique Européenne. Dès lors le problème se pose : comment concilier les impératifs de sécurité de l'état avec les nécessités du commerce international ?

[21] Cf. Géraud LAC et Cédric VIEAU *Les Aspects Légaux de la Cryptographie en France et dans le Monde*, rapport ENSIMAG option SDTR mars 1999

Dans **le décret de février 1986 (86-250)**, les cartes à puce, qui ne font que de l'authentification, sont déclassées. Mais les appareils de chiffrement restent des armes de guerre. Deux organismes sont créés pour gérer et suivre l'évolution de la cryptographie : le DISSI (Délégation Interministérielle pour la Sécurité des Systèmes d'Information) qui sert d'observatoire pour le gouvernement, et le Service Central de la Sécurité des Systèmes d'Information (SCSSI) qui joue un rôle dans les deux types d'autorisation qui sont mises en place. Pour la fabrication et le commerce des moyens de cryptologie, il faut faire une demande accompagnée d'un dossier aux P&T et à la Direction de la Réglementation Générale (DRG) ; pour le déclassement des matériels, le dossier est examiné par le CNET, le SCSSI et par le contrôle général des armées ; pour les importations, une enquête sur la société est menée par la Direction des Relations Internationales (DRI). Quant à l'utilisation des moyens de cryptologie, une demande doit être faite aux P&T et au Service de Défense de la Sécurité Civile (SDSC). Tout produit, même déclassé, reste considéré comme un matériel de guerre et son utilisation est soumise à une demande à la DRI et à la Direction Générale des Armées (DGA). Cette pluralité des interlocuteurs rend les textes de 1986 restrictifs et très difficiles à mettre en oeuvre.

La **loi du 29 décembre 1990 (90-1170 article 28)** tente de répondre à ces difficultés. La nouvelle réglementation a pour but d'élargir et de simplifier les procédures précédentes. Ainsi le nombre d'interlocuteurs est limité à un seul : le SCSSI. Le législateur a comme volonté d'imposer le minimum de restrictions nécessaires pour assurer la défense et la sécurité de l'état. Deux régimes de contrôle sont ainsi mis en place : la déclaration préalable et l'autorisation préalable. Une liste exhaustive des prestations ou moyens de cryptologie ne nécessitant qu'une déclaration préalable est crée. Cette liste comprend entre autres les moyens qui permettent l'authentification d'une communication ou encore ceux qui permettent d'assurer l'intégrité des messages transmis. Tout ce qui n'est pas dans la liste est soumis à l'autorisation préalable. Pour l'autorisation préalable, la demande d'utilisation, qu'elle soit générale ou personnelle, est faite au SCSSI. C'est lui qui instruit le dossier, mais l'accord est donné par le Premier Ministre. Les demandes d'exportation sont soumises au même régime.
La loi du 26 juillet 1996 (96-659) loi tente d'atténuer la rigueur des précédentes. Elle autorise la libre utilisation des moyens de cryptologie permettant d'authentifier mais aussi d'assurer l'intégrité des messages (ce qui signifie que le cryptage des mots de passe n'est plus hors la loi). Mais la vraie nouveauté est la libéralisation des moyens permettant d'assurer la confidentialité du message lui-même, à condition que les conventions secrètes utilisées (clés de cryptage) soit remises à un organisme agréé. Cet organisme, aussi appelé tiers de confiance ou tiers de séquestre ou encore *notaire électronique*, est le seul habilité à gérer et à certifier les conventions secrètes. Il doit faire une demande d'agrément au SCSSI, mais

c'est le premier ministre qui, lui seul, peut l'accepter ou la refuser après concertation avec les ministres concernés.

Publiés tardivement[22], les **décrets d'application** de la loi de 1996 **du 24 février 1998 (98-101 et 98-102)** définissent les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie. Ils définissent aussi les conditions dans lesquelles sont agréées les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie. Ce sont en fait les conditions de fonctionnement du SCSSI puisqu'il est le seul organisme agréé.

Dans les **décrets du 23 mars 1998 (98-206 et 98-207)**, se trouve la liste concrète des libertés définies par la loi de 1996. Les décrets définissent les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable (totalement libres d'utilisation ou de commercialisation) ainsi que les catégories de moyens et de prestations de cryptologie pour lesquelles il suffit de faire une déclaration au SCSSI, la demande d'autorisation n'étant plus nécessaire. Ce sont ces décrets qui fixent la taille des clés de cryptage librement utilisables à 40 bits. Ce nombre est à ramener au temps qu'il fallait en 1996 pour casser une telle clé : 1 semaine avec un simple PC alors qu'il faut 0.0002 secondes pour la CIA ou la DST (*Rapport de Matthew Blaze présenté au Sénat américain en juin 1996*). Une clé de 56 bits devient impossible à casser avec un PC, et prend 12 secondes pour les organismes gouvernementaux. Mais le général Desvignes, directeur du SCSSI, estimait en 1998 que le passage aux 56 bits ne présentait guère d'intérêt, car les centres de décryptage (officiels) seraient plus coûteux pour le contribuable, alors que la confidentialité forte est devenue accessible par le séquestre des clés par les tiers de confiance...[23] Pourtant, à l'époque, le choix du Centre Hospitalier de la Région Annecienne s'était porté sur une solution de cryptographie avec une clé de 56 bits beaucoup plus sûre que celle retenue par exemple dans le cadre du Réseau Santé Social resté dans le cadre de la loi sécurisé avec une clé de 40 bits.

En **janvier 1999** a eu lieu le bilan d'un an de travail du Comité interministériel pour la société de l'information. A cette occasion M. Lionel Jospin, Premier Ministre, a déclaré lors de sa conférence de presse du **19 janvier 1999** que "*la législation de 1996 n'est plus adaptée*". Le Gouvernement, en accord avec le Président de la République, a décidé de s'orienter vers

[22] Cf. rapport juin 1998 du Service Central de la Sécurité des Systèmes d'Information *La réglementation française en matière de cryptologie*
[23] *Le Monde Informatique,* 27 février 1998

une "*liberté complète dans l'utilisation de la cryptologie*" et ainsi "*supprimer le caractère obligatoire du recours au tiers de confiance pour le dépôt des clefs de chiffrement*".

Mais un changement de loi prend du temps, et devant le retard qu'a pris la France dans le domaine de la sécurité informatique, et le retard que cela entraîne dans le développement de son commerce électronique (ce qui constitue une priorité politique pour le gouvernement actuel), ce n'est qu'en **mars 1999** que "*le Gouvernement a décidé de relever le seuil de la cryptologie dont l'utilisation est libre, de 40 bits à 128 bits, niveau considéré par les experts comme assurant durablement une très grande sécurité*".

*b) Faiblesses de la libéralisation de 1996 et 1998 :*

La loi française du 27 juillet 1996 avait été présentée comme une véritable libéralisation alors qu'en fait, après une analyse soigneuse des textes, rien n'avait changé de manière radicale. Il s'agissait simplement d'un assouplissement[24]. Son analyse est importante sur un plan historique mais elle reste d'actualité car elle a introduit des concepts et des pratiques qu'on retrouve aujourd'hui et qui seront développés plus tard dans ce mémoire.

La seule réelle nouveauté de la loi était la mise en place de **tiers de séquestre**, système purement français dont on peut s'interroger sur le degré de libéralisation. Il s'agit d'une **tierce partie de confiance**, organisme qui a la confiance de l'utilisateur et qui effectue, pour le compte de celui-ci, certaines opérations liées à la gestion des clés de confidentialité et/ou de signature numérique. Il convient de distinguer les fonctions de **tiers de séquestre** (des clés servant à la confidentialité) et les fonctions d'**autorités de certification** (**AC**) pour des clés publiques n'intervenant que dans des applications liées à la signature. Certains mécanismes sont communs aux deux fonctions, comme la certification de clés publiques, et rien n'empêche un organisme de remplir les deux fonctions (séquestre et AC).

Cette confiance repose sur plusieurs éléments, notamment les compétences de l'organisme, l'obtention éventuelle d'un agrément, le contenu du contrat liant l'organisme à l'utilisateur et les mesures mises en place par l'organisme pour assurer la protection des données et clés de l'utilisateur. Le tiers de séquestre est un organisme agréé par le Premier ministre après instruction de son dossier de demande d'agrément par le SCSSI. La fonction du tiers de séquestre consiste à conserver les clés secrètes des utilisateurs mises en œuvre

[24] Cf. entretiens de décembre 1998 intitulé *L'exception française* par Maître Valérie Sédaillan reproduits sur le site Web http://www.juriscom.net/espace2/crypto3.htm

à des fins de confidentialité afin de les remettre à ces mêmes utilisateurs s'ils les demandent et aux autorités judiciaires ou de sécurité. Dans cette seule fonction de séquestre, il n'intervient pas directement dans les échanges entre utilisateurs. Ainsi l'utilisateur peut-il s'appuyer sur un professionnel de la cryptologie qui lui permet d'utiliser librement des produits de cryptologie forte, tandis que l'État peut, dans le cadre des procédures prévues par la loi, accéder à une information. Le tiers de séquestre est soumis à deux types d'obligations :

- Le tiers de séquestre doit pouvoir **fournir des garanties de bon fonctionnement** à ses clients. La sécurité apportée par l'usage de la cryptologie repose sur le secret des clés. Il est donc nécessaire que le tiers de séquestre garantisse à ses clients un très haut niveau de sécurité, tant pour le stockage des clés secrètes que pour leur génération, dans les cas où il assure cette génération. Des audits destinés à vérifier les dispositions mises en œuvre pour assurer ce haut niveau de sécurité peuvent être effectués par le SCSSI.
- Le tiers de séquestre est soumis à des obligations légales de **remise ou de mise en œuvre des clés à la demande des autorités judiciaires ou de sécurité**. Ces obligations conduisent le tiers de séquestre à mettre en place un service permanent de remise ou de mise en œuvre des conventions secrètes assuré par du personnel présentant un niveau d'habilitation suffisant. Il n'est pas explicitement prévu qu'une entité gère directement ses propres clés (notion "*d'autrui*" citée dans la loi), mais une société ou un groupe peut tout à fait créer une filiale indépendante qui devra se faire agréer comme tiers de séquestre et agira pour ses propres besoins.

Le rôle de l'autorité de certification est de produire et de gérer des **certificats de clés publiques** utilisées pour la signature numérique. L'objectif d'un certificat est de garantir à une personne qui utilise une clé publique pour vérifier une signature que cette clé publique appartient bien à qui elle est censée appartenir (non usurpation d'identité). Pour ce faire, un certificat garantit le lien entre la clé publique et le détenteur de la clé secrète correspondante utilisée pour fabriquer la signature numérique. L'AC vérifiera l'identité du demandeur, ou le pouvoir, et veillera à la non réutilisation de clé publique, par exemple en s'assurant que le demandeur détient bien la clé secrète. Ses tâches principales sont la création du certificat pour le détenteur d'une clé secrète, la publication de certificats, la révocation de certificat et l'interface avec les autres AC (reconnaissance mutuelle des certificats).

La France est le seul pays à avoir mis en place ce système de tiers de séquestre. Cette singularité avait été soulignée par le Conseil d'Etat dans son rapport. Cette solution était inadaptée aux échanges internationaux, chaque Etat voulant se réserver l'accès aux clés privées de chiffrement dans le domaine de la sécurité nationale où il est peu réaliste

d'envisager des accords internationaux. Le Conseil d'Etat soulignait qu' "*il ne sera possible de conserver durablement un dispositif de tiers de séquestre, relativement contraignant pour les entreprises, que si la réglementation française parvient à inspirer celle mise en œuvre par les autres pays développés*". Or, en Amérique du Nord et dans les autres pays européens, il n'existe pas de législation restreignant le libre usage et la fourniture de logiciels. Seuls existent des contrôles à l'export qui varient selon les pays. Les entreprises françaises se trouvaient donc face à une législation qui encadrait non seulement l'exportation mais également l'importation, la fourniture et l'utilisation de produits de cryptographie. Le décret 98-101 du 24 février 1998 réglementait même l'utilisation par un fournisseur de procédés de cryptographie à des fins de développement.

Devant la rapidité de l'évolution de la puissance des machines, il est vite apparu que la barrière des 40 bits était dépassée et qu'une clé d'une telle longueur ne permettait pas un chiffrement fort. Le dispositif français visait à ce que les entreprises, pour effectuer du chiffrement fort, étaient plus ou moins obligées de passer par le système de tiers de confiance. Ce système avait été critiqué par **l'Agence de Régulation des Télécommunications** (**ART**) qui avait rendu un avis réservé sur les projets de décrets et le rapport du Conseil d'Etat soulignait les difficultés soulevées par le système. De plus, ce système de tiers de confiance supposait le recours à une technologie propriétaire spécifique qui risquait de ne pas être toujours compatible avec les standards internationaux. Les produits commercialisés par les tiers de confiance étaient forcément destinés au seul marché français, marché plus restreint avec des contraintes de développement et d'exploitation plus lourdes avec un coût plus élevé. Largement critiqué par les experts, ce système continuait encore aux premiers mois de 1999 de faire de la France un des pays où la cryptographie était le plus sévèrement contrôlée au monde.

Ce début de libéralisation était somme toute assez paradoxal sur certains points puisqu'on pouvait par exemple légalement sécuriser un accès en chiffrant par exemple les données d'authentification telles que les mots de passe mais qu'il n'était pas question de crypter librement (dans la limite d'un chiffrement avec une clé supérieur à 40 bits) les contenus et les données d'un message. Pour poursuivre cette idée, l'utilisation de tout système qui avait pour vocation d'assurer l'authentification de l'échange et des correspondants ainsi que des moyens permettant d'assurer l'intégrité des messages d'un bout à l'autre de la chaîne de diffusion était libre, mais pas celle d'un système cryptant les contenus diffusés.

C'est dans ce contexte que se sont développées dans le milieu hospitalier les premières expériences de télémédecine avec transmissions de données protégées ainsi que le Réseau Santé Social, initialement sécurisé avec des clés de chiffrement d'une longueur de 40 bits.

*c) La libéralisation de 1999 :*

Le **19 janvier 1999**, le Premier Ministre, M. Lionel Jospin, annonçait dans un discours resté célèbre, une proche libéralisation de l'usage de la cryptologie.

"*Nous avions, il y a un an, franchi un premier pas vers la libéralisation des moyens de cryptologie. J'avais annoncé alors que nous en franchirions un autre ultérieurement. Le Gouvernement a, depuis, entendu les acteurs, interrogé les experts et consulté ses partenaires internationaux. Nous avons aujourd'hui acquis la conviction que la législation de 1996 n'est plus adaptée*. *En effet, elle restreint fortement l'usage de la cryptologie en France, sans d'ailleurs permettre pour autant aux pouvoirs publics de lutter efficacement contre des agissements criminels dont le chiffrement pourrait faciliter la dissimulation*."

Pour changer l'orientation de la législation, le Gouvernement a donc retenu les orientations suivantes avec l'aval du Président de la République :
– offrir une liberté complète dans l'utilisation de la cryptologie
– supprimer le caractère obligatoire du recours au tiers de confiance pour le dépôt des clefs de chiffrement
– compléter le dispositif juridique actuel par l'instauration d'obligations, assorties de sanctions pénales, concernant la remise aux autorités judiciaires, lorsque celles-ci la demandent, de la transcription en clair des documents chiffrés. De même, les capacités techniques des pouvoirs publics seront significativement renforcées et les moyens correspondants dégagés.

Le Gouvernement a voulu que les principales entraves qui pèsent sur les citoyens pour protéger la confidentialité de leurs échanges et sur le développement du commerce électronique soient levées sans attendre. Ainsi, dans l'attente des modifications législatives annoncées, le Gouvernement a décidé de relever le seuil de la cryptologie dont l'utilisation est libre, de 40 bits à 128 bits, niveau considéré par les experts comme assurant durablement une très grande sécurité."

Dans la suite logique de cette déclaration et de l'**arrêté du 17 mars 1999**[25], les **décrets du 17 mars 1999 n° 99-199** et **n° 99-200** passant le seuil de 40 bits à 128 bits sortirent le **19 mars 1999**[26]. Ils établissent, entre autres :

[25] Cf. Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie (J.O. numéro 66 du 19 mars 1999 page 4052)

– que l'utilisation des produits "offrant un service de confidentialité mis en oeuvre par un algorithme dont la clé est d'une longueur inférieure ou égale à 40 bits" est libre
– que l'utilisation des produits entre 40 et 128 bits est libre, sans condition dans le cas d'un usage purement privé, et après une unique déclaration du producteur, d'un fournisseur, d'un importateur ou même à défaut d'un utilisateur dans les autres cas. Dans le cadre de l'utilisation à des fins privés d'une personne physique, il n'est même pas nécessaire d'obtenir une quelconque déclaration d'utilisation ou d'importation, n'importe quel logiciel utilisant une clé d'une longueur inférieure à 128 bits peut légalement être importé.

Au-dessus de cette limite, il faut soit utiliser les services d'un tiers de séquestre agréé, soit demander une autorisation auprès du SCSSI dépendant toujours du Premier Ministre. On retrouve la démarche juridique décrite précédemment qui reste donc toujours d'actualité.

Par conséquent, la question de la cryptographie ne soulève plus autant de débats que par le passé sur son encadrement juridique puisque la règle est devenue la liberté. La facilité d'installation d'un module de cryptographie dans n'importe quelle solution logicielle permet de s'affranchir de la connaissance des données techniques à partir du moment où la CNIL (et le SCSSI le cas échéant) a donné son aval. Il s'agit de voir désormais de voir quels dispositifs de sécurité ont été prévus sur les outils apparemment incontournables que sont entre autres le RSS, la CPS et la carte SESAM VITALE et à quelles fins.

[26] Cf. Décret n°99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation (J.O. numéro 66 du 19 mars 1999 page 4050)

## II) L'USAGE DE LA CRYPTOGRAPHIE DANS LE DOMAINE MEDICO SOCIAL DEVENANT FONDAMENTAL, PLUSIEURS OUTILS CHERCHENT A DEVENIR INCONTOURNABLES, LAISSANT ENCORE ENTIERE LA PROBLEMATIQUE DE LA SECURISATION DES DONNEES MEDICALES NOMINATIVES :

### 1) La télétransmission des feuilles de soins avec le Réseau Santé Social et ses concurrents:

La télétransmission des feuilles de soin est le premier exemple "grandeur nature" d'échanges de données liées à un patient. Il permet d'analyser les questions de sécurité dans ces échanges et d'introduire les principaux outils et acteurs qu'un directeur d'hôpital rencontrera forcément lorsqu'il aura à construire un réseau de télémédecine, à savoir des partenaires éventuels comme Cégétel-RSS et des outils courants comme la Carte Professionnel de Santé (CPS) ou la carte SESAM VITALE nouvelle génération qui contiendra le dossier du patient.

*a) Le RSS :un réseau unique pour l'acheminement des feuilles de soins électroniques :*

Le **RSS** ou **Réseau de Santé Social** est un **réseau de transport de l'information**, basé au départ, sur le réseau téléphonique commuté. Il doit permettre le traitement sans papier des feuilles de soins, puis du carnet médical. Pour l'avenir, il devrait favoriser un échange des informations entre professionnels de santé et leur proposer d'autres prestations que celles rendues obligatoires par les ordonnances Juppé relatives à la réforme de la Sécurité sociale (accès à Internet, par exemple). Ces autres prestations ne constituent pas un monopole.


Le RSS a démarré en Bretagne le **2 avril 1998**. Le Morbihan a été le premier département où le RSS a été déployé. A la fin du mois de mai 2000, on comptait 20 727 abonnés au RSS. Un appel d'offres pour l'opérateur de ce réseau avait été lancé en février

1997. L'appel d'offres fut bouclé le 15 septembre 1997. Les candidats en lice étaient France Télécom, La Poste, Cap Gemini, Cégétel et Cegedim. Le choix de l'opérateur fut entériné après plusieurs reports le **31 décembre 1997**. Cégétel, filiale du groupe Générale des Eaux, est alors devenu concessionnaire du RSS. Le marché qui confie à Cégétel une concession de cinq ans ouvre à la société trois sources de rémunération : un abonnement forfaitaire payé par les médecins pour leur raccordement au réseau, un forfait payé par tous les hôpitaux et les institutions de santé et une facturation à la Sécurité Sociale par feuille de soins transmise.

L'appel d'offres gouvernemental portait sur un réseau propriétaire sécurisé. Certains se sont rendu compte que les FSE allaient générer un trafic faible, mais concentré à certaines heures et proposaient un Internet sécurisé. La technologie finalement retenue a été un Intranet (utilisant les protocoles TCP/IP) reliant le réseau Ramage de l'Assurance Maladie, les régimes complémentaires et les gros établissements de soins (3000 sites), associé à un Extranet les professionnels de santé (300 à 400 000 sites). Le RSS est réservé aux professionnels de santé et supporte d'abord les transferts de la Feuille de Soins Electronique et de multiples autres services (accès aux bases de données). Ne peuvent utiliser le RSS que les porteurs de carte CPS. Dans un souci de normalisation et de sécurité des flux, le législateur a prévu que les transferts entre les professionnels de santé, d'une part, et les organismes d'assurance maladie, d'autre part, se fassent via ce réseau. Sur ce réseau seront connectés, les médecins et leurs serveurs professionnels, mais aussi les autres professionnels de santé, les établissements de santé, les institutions (ANAES, Agence du médicament…), les régimes d'assurance maladies obligatoires et complémentaires, des prestataires de services, avec la possibilité d'avoir une passerelle avec le réseau Internet. Des réseaux associés (SIAMUC, MEDSYN, UNIONS…) sont autorisés à se brancher sur le RSS pour proposer aux professionnels de santé des services complémentaires.[27]

L'architecture du réseau repose sur la société Télécom Développement, filiale commune de Cégétel (40 %) et de la SNCF (60 %), dont le réseau de 10 000 km en fibre optique (le long des voies) assurera la transmission des données du RSS. Depuis la mi 1998, Cégétel a mis en chantier des kits de connexion qui ont été être mis à la disposition du GIE SESAM-VITALE, du GIP CPS et des éditeurs de logiciels. Le RSS propose ainsi en pratique une messagerie électronique médicale sécurisée, permettant d'envoyer et de recevoir des courriers électroniques (e-mails), une adresse de courrier électronique personnelle (e-mail) de professionnel de santé et la transmission des feuilles de soins

[27] Cf. site Web du RSS sur http://www.cegetel.rss.fr/HTML/Index.htm

électroniques avec le retour des **Accusés de Réception Logiques** (**ARL**). Lorsque le professionnel de santé souhaite remplir une FSE, il ouvre le logiciel en question et remplit un formulaire électronique. A la fin de la journée, lorsque tous les formulaires sont mis en mémoire, il actionne une icône lui permettant d'envoyer les FSE. Un système d'authentification lié à la carte CPS se met alors en place, qui permet aux informations de passer sur le réseau, de façon sécurisée, jusqu'à la caisse de destination. Mais les FSE peuvent également transiter par des opérateurs intermédiaires (**concentrateurs** ou **Réseaux Associés**). Il s'agit le plus souvent de groupements professionnels (de type syndical ou associations professionnelles) ou de sociétés commerciales (France Télécom avec Libéralis, Cegedim avec Santénet) qui gèrent la connexion de leurs abonnés ou adhérents et leur proposent différents services. Le RSS est directement relié aux organismes d'**Assurance Maladie Obligatoire** (**AMO**). L'interconnexion garantit que les AMO puissent traiter sans difficulté les données issues des FSE.

*b) La sécurité sur le RSS :*

Cegetel.rss fournit avec le kit de connexion le navigateur (Netscape), l'annuaire, l'authentification par CPS, assistance en ligne et logiciel automatisant les fonctions de télétransmissions. L'accès au RSS se fait par 84 points d'entrée répartis sur le territoire. Alors que le RSS utilise des technologies Internet et qu'il existe des passerelles entre le Réseau et l'Internet, selon Cegetel.rss, en théorie, trois procédures de sécurisation autorisent la protection des données échangées sur l'Intranet du Réseau Santé Social :

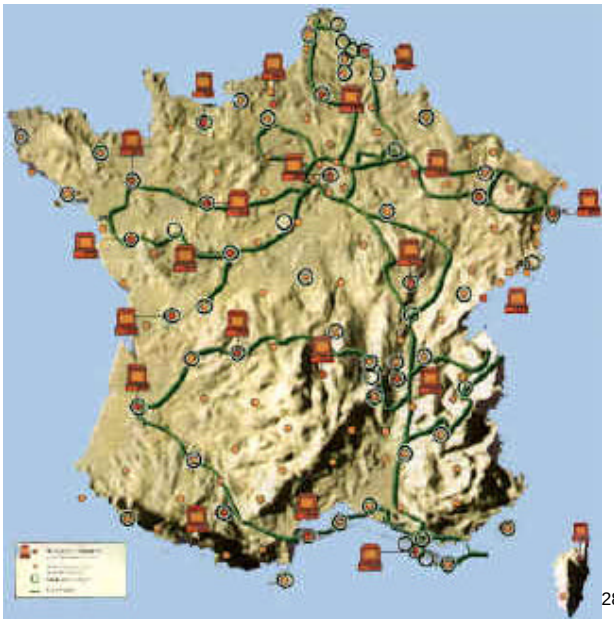
**- une authentification à la source et une signature** : toute personne pénétrant sur le RSS est identifiée par sa carte CPS. Les mécanismes permettant d'assurer la sécurisation des échanges sont directement assurés au niveau de la carte CPS. La CPS joue le rôle de certificat personnel qui permettra de signer électroniquement et de crypter/décrypter des messages de manière totalement conviviale et transparente.

**- un chiffrement SSL puis S/MIME** (*Secure / Multipurpose Internet Mail Extensions) :* standard utilisé pour chiffrer et signer numériquement les messages électroniques MIME**.** Développé par RSA, il contribue à garantir la sécurité des messages électroniques d'un utilisateur. Il comprend une signature numérique, qui permet aux utilisateurs de vérifier l'identité de l'expéditeur et l'intégrité du message, et un cryptage numérique qui protège le contenu des messages contre une éventuelle lecture par une personne autre que le destinataire. La CNIL a mis en cause dès le départ le cryptage insuffisant exposant au risque de "*divulgation, de déformation et d'intrusion*". La CNIL a toléré pour le démarrage en Bretagne une clé de chiffrement simple de type SSL. Le service S/MIME aujourd'hui permet

de crypter les informations échangées sur le RSS et d'assurer ainsi la confidentialité. Le niveau de sécurité offert (longueur de clé de cryptage de 40 bits, respectant la réglementation de 1998) devait garantir de la majorité des tentatives d'interception des échanges, mais celui-ci, on l'a vu n'est absolument plus sûr aujourd'hui.

**- des systèmes de sécurité** (firewalls ou pare-feux) sur l'ensemble des accès, garantissant la non-intrusion d'utilisateurs ne faisant pas partie des abonnés professionnels de santé et protégeant le réseau contre les virus.

Sur le RSS se connectent deux types d'utilisateurs : individuellement les professionnels de santé et les groupes d'utilisateurs reliés entre eux par un réseau. Le type d'accès est différent. La connexion des utilisateurs au RSS repose sur l'infrastructure grand public de Cegetel. Les **POP** (points de présence) constituent les points d'entrée au réseau.



[28]

- **les Points d'Accès Individuels ou PAI** :

Le **PAI** est le point d'entrée des abonnés individuels sur le RSS. Il authentifie l'utilisateur se connectant et assure l'aiguillage de la requête de l'utilisateur, en acheminant la communication vers les différents réseaux (Internet, RSS). Un PAI se compose de routeurs, de firewalls (pare-feux) et de machines serveurs. Les routeurs filtrent les communications entrantes et les dirigent vers les services demandés par l'utilisateur. Les firewalls assurent un rôle de double filtrage à la fois des accès au RSS grâce à la liaison avec les serveurs d'authentification ainsi que des données en provenance de l'Internet. Les serveurs se composent de trois types de machines : les serveurs d'authentification qui interdisent l'accès

[28] Carte *SVM Micro* reprenant l'infrastructure de Cégétel, les PRS, les PRI et les principaux nœuds de connexion en France (1999)

au RSS des utilisateurs non autorisés, les serveurs de back-office hébergeant les services de gestion et de facturation des abonnés au RSS et les serveurs proxy améliorant la performance des accès aux services.

- les **Point d'Accès Collectif (PAC)**:
Les PAI sont réservés aux groupes d'utilisateurs organisés en réseau. Le réseau du groupe d'utilisateur est raccordé au RSS par une ligne spécialisée (LS) ou via une connexion RNIS. Le raccordement est analogue à celui du PAI. Il passe par la mise en place d'un serveur d'authentification, qui permet de vérifier l'autorisation de chaque utilisateur d'accéder aux services du RSS. Comme le PAI, le **PAC** est composé de routeurs, de firewalls et de serveurs. Deux formes de raccordement sont proposées. Dans le mode "client de messagerie", le serveur de messagerie est hébergé par Cégétel et les AMO peuvent lire leur boîte aux lettres dans laquelle sont stockées les données des FSE télétransmises par les professionnels de santé. Les AMO rapatrient ces données sur un poste dédié à cette messagerie. Pour consulter sa boîte aux lettres, l'utilisateur doit être authentifié. Dans le mode serveur de messagerie, les AMO possèdent leurs propres serveurs de messagerie, vers lesquels sont dirigées les informations (FSE transmises) par le serveur du RSS.

- les **Points de Raccordement des Serveurs (PRS)** :
Les **PRS** permettent de connecter au RSS des serveurs placés sous la responsabilité des prestataires de services ou hébergés par Cegetel.rss. Le raccordement au RSS est assuré par une ligne spécialisé (LS). Les prestataires de services, eux-mêmes abonnés au RSS, mettent à la disposition des professionnels de santé des services particuliers dans le cadre du RSS. Ces services sont hébergés sur des serveurs qui doivent pouvoir accéder au RSS. Les prestataires en question n'ont donc besoin que d'accès entrants. Un firewall sera systématiquement mis en place à l'entrée du RSS afin de parer à tout risque d'intrusion et pour faire les mises àjour. Le PRS est constitué de routeurs, de pare-feux et de serveurs.

- les **Points de Raccordement Internet (PRI)**, passerelle entre le RSS et l'Internet :
Les Points de Raccordement Internet (PRI) permettent de relier le RSS et l'Internet et garantissent ainsi aux utilisateurs connectés sur le RSS l'accès au Web et aux forums de discussion. Les PRI sont constitués de routeurs, de pare-feux et de serveurs.

A chaque point, l'opérateur s'est donc entouré de solutions de sécurité. Malgré cette structure, le RSS a connu (et continue de connaître) moult déboires notamment un plantage national les 7, 8 et 9 mars 1999 touchant l'authentification rendant impossible toute

télétransmission et désactivant les fonctions de messagerie[29]. Une nouvelle panne de la messagerie est survenue le 16 juin 1999 avec des problèmes de connexion notables jusqu'au 25 juin 1999[30].

*c) Les concurrents commerciaux du RSS :*

Le RSS n'a pas le monopole des connexions pour le transfert des FSE. En effet, le cahier des charges de l'appel d'offres de l'Intranet Santé a prévu une passerelle sur Internet pour la transmission des FSE aux CPAM. Les seuls flux concernés par le RSS sont le transit des FSE SESAM-VITALE. Les FSE "mutuelles" ne sont pas obligatoirement transmises par le RSS, ces données peuvent très bien être transmises par un intranet ou via Internet.

Une clause garantit à Cégétel le transit exclusif des flux SESAM-VITALE vers la caisse inter-régime sur le RSS. L'opérateur doit développer des passerelles entre l'intranet RSS et les quatre points d'entrée nationaux du réseau RAMAGE de la CNAM. Pour chaque flux de FSE arrivant par un des 4 points d'entrée de RAMAGE, la Sécurité Sociale verse 20 centimes à Cégétel-rss. A partir du 500 millionième document, 10 centimes, puis 5 centimes après le premier milliard de flux de FSE acheminé. Le RSS n'a qu'un monopole, c'est celui de la réception des feuilles de soins électroniques. Le praticien peut très bien utiliser les services d'un serveur intermédiaire qui lui sera obligatoirement connecté au RSS. Le professionnel de santé, peut être adhérent à un **concentrateur de données** lui même abonné au RSS et agréé par l'Etat. Les concentrateurs sont des organismes intermédiaires dans le processus de la télétransmission des FSE, chargés de centraliser les informations de remboursement et d'en effectuer le routage vers les différents organismes d'assurance maladie concernés. Comme la CNIL l'a rappelé lors de plusieurs avis, ces organismes ne doivent assurer aucun traitement particulier pour leur propre compte, effectuer ni enrichissement, ni cession de ces informations à des tiers.

A la suite du RSS, d'autres sociétés se sont lancées à leur tour dans l'offre de réseaux sécurisés à destination des professionnels de la santé. Ces sociétés doivent être connues par un directeur d'hôpital car elles peuvent offrir des solutions alternatives au RSS pour la constitution de réseaux de télémédecine.

[29] Cf. sur le Web http://www.amgitweb.com/actualite/actualite_du_rss.htm la liste actualisée par l'AMGIT de tous les dysfonctionnements du RSS

[30] Cf. article de *Libération* du 25 juin 1999 : *Une sécurisation perfectible des réseaux de santé*

- **Libéralis (France Télécom)** :

En 1997, plusieurs Unions Régionales des Médecins Libéraux (URML) réfléchissent à la création d'un réseau Intranet destiné à leurs activités. Un appel d'offre désigne France Télécom comme opérateur chargé de la réalisation technique de celui-ci, qui est baptisé Libéralis. L'unique formule d'abonnement, fixée à 120 F par mois (hors coûts de communication téléphonique locale), permet l'accès à une large gamme de services comme la transmission sécurisée des Feuilles de Soins Electroniques et la gestion des Accusés de Réception Logiques (ARL), l'accès à une boîte aux lettres électronique sécurisée permettant, outre l'échange de courriers cryptés, la réception des résultats d'analyse au format HPRIM, des services professionnels multiples (agenda des tâches, résultats d'enquêtes de santé publique, statistiques et données épidémiologiques, actualités thérapeutiques, participation à des enquêtes et à des évaluations médico-économiques…) et un accès illimité à Internet.

- **Medsyn** :

Créé à l'initiative du syndicat MG-France, Medsyn est le seul Intranet officiellement associé au RSS depuis le début. Pour une formule unique à 145 F par mois (hors coûts de communication téléphonique), l'abonnement permet un accès au RSS permettant la transmission sécurisée des FSE qui bénéficient dès lors d'une prise en charge complète par le réseau Medsyn (archivage réglementaire, gestion des ARL, ré-émission automatique en cas de problème, traçabilité des FSE, gestion des éventuels contentieux relatifs aux télétransmissions…), l'accès à une boîte aux lettres électronique sécurisée, la consultation de l'annuaire des professionnels de santé, de nombreux services professionnels (groupes de discussion thématiques en particulier sur les différents progiciels médicaux, informations de santé publique, actualités thérapeutiques, accès au journal Osmose Médicale…), l'accès à des fonctionnalités "serveur Exchange" (communications professionnelles, agenda partagé…) et un accès illimité à Internet.

- **Santésurf (Cegedim)**:

Ex Santénet, Santésurf est destiné aux professionnels de santé, y compris ceux de l'industrie pharmaceutique. Cette formule prévoit l'accès aux services suivants: la télétransmission des FSE via le "concentrateur de données" Télépharma, une messagerie sécurisée ainsi que l'accès aux boîtes aux lettres médicales des laboratoires et un accès à Internet. Omniprésent dans le monde du logiciel médical avec Medigest, DIA, DBMed, Mediclick, Ordogest…, Cegedim couple systématiquement ses logiciels à sa plate-forme Santésurf.

- **Les fournisseurs d'accès Internet traditionnels**

Ces organismes ont la particularité d'être avant tout des fournisseurs d'accès à Internet grand public. Par la suite, au gré de l'évolution du concept de télétransmission médicale, certains d'entre eux se sont lancés dans l'offre de services à destination des professionnels de santé. Tous garantissent des niveaux de sécurité suffisants pour permettre l'acheminement des courriers sensibles et des données professionnelles, mais le recours à ces opérateurs peut réclamer quelques petites compétences techniques, notamment pour la configuration des logiciels utilisés. On peut citer **Wanadoo santé (France Télécom)** qui permet la télétransmission des FSE en coordination avec les logiciels prévus à cet effet et **Club Médical (Club-Internet)** qui propose la même chose à quelques subtilités de contenus et de services près (la possibilité de recevoir des résultats d'analyses par e-mail nécessite un abonnement particulier par exemple).

- **L'infogérance avec WebFSE**

Selon ce principe novateur, le professionnel de santé délègue une partie de ses obligations à un prestataire extérieur qui lui facture cette prise en charge de manière forfaitaire. Pour le moment, le service **WebFSE** d'**Almasanté** est le seul agréé à proposer une telle offre. Lors de son abonnement, le professionnel de santé télécharge le logiciel de saisie et de télétransmission des FSE. Dès cet instant, le praticien envoie ses FSE quotidiennes au serveur qui se charge de les transmettre aux CTI compétents, de gérer les accusés de réception logiques et de les corriger s'il y a lieu, d'effectuer la sauvegarde automatique des FSE pendant 90 jours et de présenter au praticien, lorsqu'il visite le serveur, l'état de ses transmissions. Ici, la maintenance est assurée par la simple connexion quotidienne au serveur WebFSE qui envoie automatiquement au poste émetteur les éventuelles mises à jour de son logiciel.

Malgré une volonté gouvernementale affichée de vouloir unifier le corps médical sur un seul et même réseau électronique, le résultat est plutôt à l'inverse de ce qui était attendu. *Le Quotidien du Médecin* spécial informatique des 15 et 18 juin 2000 donnaient un tableau de bord des réseaux[31] : 20 727 abonnés au RSS fin mai, 17 417 pour Wanadoo santé (dont 50 % télétransmettraient), 13 000 pour Club Médical, 1600 abonnés pour Medsyn (avec 650 télétransmetteurs), 25 000 abonnés (dont 3000 télétransmetteurs) pour Santé Surf de Cegedim et 500 pour Libéralis. Non seulement le RSS est sérieusement concurrencé mais chaque praticien libéral informatisé se retrouve avec une configuration (réseau d'accès au RSS, bases de données..) qui lui est propre. Selon Régis Giet, l'insuccès de Libéralis est

[31] A compléter avec l'annexe 2 relative aux transmissions avec le RSS

imputable à "*la disparité des configurations d'installation (80 logiciels de gestion de dossier-patients sont disponibles sur le marché)*" [32].

Afin de favoriser l'interopérabilité des différentes messageries médicales utilisées par les professionnels de santé, Cégétel.rss et les principaux éditeurs de logiciels médicaux (Alternative Soft, Axilog, Coccilog, CSK, Etiam, Everys, Hexaflux, HDMP-Eglantine, Imagine Edition, Kalamazoo, Logun, LSI Médical, Microconcept, 01 Santé, Prokov Edition, RM Informatique, Visiodent et Waid) ont signé il y a quelques mois un accord pour la création d'un standard d'échanges de données sécurisées (imagerie et résultats d'analyses) sur le RSS, le **Medical Message Format** (**MMF**)[33]. Cégétel.rss a en fait conclu début mars 2000 un accord de partenariat avec la société rennaise Etiam afin de développer une messagerie professionnelle sécurisée, capable de gérer simplement le transfert de données médicales comme des images radiologiques et des résultats d'examens biologiques. La messagerie Mediem d'Etiam[34] sera adaptée aux normes de sécurité du RSS et l'ensemble des données échangées seront chiffrées pour en assurer la confidentialité. Mediem utilise aussi le format **Medical eXchange Folder** (**MXF**). Ce format va évoluer vers le nouveau standard Medical Message Format (MMF). CegeteI.rss se porte garant du standard MMF, de ses évolutions, et de sa compatibilité avec les principaux formats de données nationaux et internationaux en usage dans le domaine médical. C'est un premier pas vers le renforcement de la sécurité des échanges de données médicales.

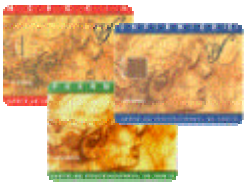
Malgré cette forte concurrence qui montre bien que le RSS n'est pas si incontournable qu'il ne le prétend, deux outils encore en évolution sont largement distribués en France et leur utilisation devient de plus en plus naturelle pour le patient comme pour le professionnel de santé : la **CPS** et la carte **VITALE**.

[32] Médecin de France, juillet 2000
[33] Cf. communiqué de presse du RSS du 10 mars 2000
[34] Cf. site Web d'Etiam sur le http://www.etiam.fr ou http://www.etiam.com

## 2) CPS et Carte VITALE : les outils pour la sécurité de demain:

*a) La CPS :*

La **CPS** est une carte à puce permettant au Professionnel de Santé d'authentifier, c'est à dire de signer la FSE et assurer la sécurité des transactions. La carte permet au titulaire de s'**authentifier** vis-à-vis du RSS. Il peut ensuite **signer** les FSE et transmettre les informations administratives et médicales. C'est la signature électronique du praticien qui a effectué l'acte. C'est aussi un **passeport qui ouvre à son détenteur un accès sécurisé au RSS**. On peut envisager la consultation de dossiers de patients hospitalisés, des liens avec les réseaux sentinelles ou le Réseau National de Santé Publique pour des alertes sanitaires... Cette carte est à insérer avec **la carte VITALE** dans **le lecteur bifente SESAM-VITALE.**



Sur le plan technique, on distingue 2 versions de la CPS : la **CPS 1** qui supportait 3 fonctions, l'identification, l'authentification et la signature électronique du professionnel de santé et la **CPS 2**, une nouvelle version enrichie du chiffrement. Toutes ces fonctions sont permises grâce aux procédés de cryptographie évoqués en première partie. Le gouvernement avait demandé que soit implantée un service supplémentaire de sécurité **ITSEC** (***ITSecurity***, norme européenne évaluant la sécurité d'un système). C'est cette version qui a été distribuée et non la CPS 1. Le **décret N°98-271 du JO du 9 avril 1998** fixe les informations contenues sur cette carte**. Sur la partie visible de la carte,** figurent la date de fin de validation, le nom sous lequel l'utilisateur pratique, son prénom usuel, sa profession. Au recto est indiqué le numéro ADELI (le répertoire DDASS des professions médicales et paramédicales) du titulaire et au verso la mention "strictement personnelle" à coté de laquelle le titulaire appose sa signature. **Sur la partie invisible**, figurent éventuellement le nom patronymique, le mode d'exercice pour la ou les spécialités, la structure juridique d'activité, la nature du conventionnement avec les caisses d'Assurance Maladie et les **algorithmes de chiffrements** destinés à sécuriser les fonctions.

Concernant la sécurisation de la CPS, la carte CPS est conforme aux normes **ISO 7816**. Elle est dotée d'une mémoire de stockage réinscriptible en technologie EEPROM de **4 Ko** (Kilooctets). L'arrêté du 9 avril 1998 a apporté des précisions déterminantes sur le rôle des cartes CPS. Aux termes de ce texte, **les cartes de la famille dite "CPx" participent au chiffrement des messages échangés" et portent 3 algorithmes:**

- le protocole S/MIME de sécurisation du courrier électronique utilise RSA afin de signer et de chiffrer les données envoyées. **RSA** utilise des clés (privée et publique) propres à la carte, pour la **signature électronique** et **l'authentification de la carte par un tiers**.
- l'algorithme symétrique **A3S** est utilisé par les mécanismes de gestion interne de la CPS, pour la mise àjour de la carte par téléchargement.
- l'algorithme **DH** "**Diffie-Hellman**"[35] est utilisé pour la mise en œuvre du "service de confidentialité" (cryptage) avec clés gérées par une "**tierce partie de confiance"**. Selon Hervé Cassagne[36], ce serait une clé de 188 bits[37]. Pour utiliser la carte, il faut, après introduction dans le lecteur bifente, taper un **code personnel.**

Cette carte, payante, n'est pas obligatoire mais est indispensable pour créer des FSE et accéder au RSS (en pratique, il existe cependant des solutions qui permettent de s'en dispenser)**.** La CPS est déclinée dans les 14 professions médicales et paramédicales avec différentes situation d'exercice. Une carte peut contenir 8 modes d'exercice différents de la médecine. La **CPS médecin** (bandeau rouge) par décrit ses activités (médecin libéral, hospitalier, travaillant dans l'industrie pharmaceutique…). Une seule carte CPS suffit pour un médecin ayant une activité libérale et exerçant àl'hôpital.

Le **Groupement d'Intérêt Public "Carte de Professionnel de Santé"** (**GIP CPS**), chargé d'émettre, de gérer et de promouvoir la CPS, est né le 5 février 1993 par un arrêté ministériel. Cette création s'inscrit dans l'esprit de la loi de juillet 1982 qui a institué les GIP aux fins d'allier, sur des objectifs d'intérêt général, les secteurs publics et privés. L'**Organisation Professionnelle pour l'Harmonisation en l'Informatique de Santé** (**OPHIS**) créée en 1985 par le CSMF, puis élargie àl'ensemble des syndicats membres du CNPS (le syndicat des cliniques FIEHP, le syndicat des radiologues FNERQ, le syndicat des médecins de groupe SNMG) est membre du GIP CPS. La carte CPS est émise, gérée et promue par ce seul organisme. En cas de perte, vol ou dysfonctionnement, c'est **le GIP CPS qui tient la liste des oppositions** afin d'éviter les utilisations frauduleuses. Le GIP CPS délivre la carte (cf. Journal Officiel du 12 avril 1998) aux différents professionnels de santé, aux directeurs d'hôpitaux, aux étudiants effectuant des remplacement, aux employés des cabinets médicaux et des caisses de sécurité sociale. Chaque catégorie disposera d'un degré d'habilitation d'utilisation. On distingue 4 catégories de professionnels habilités en fonction de leur profil autorisant le niveau de lecture du Volet d'Information Médical (VIM) de la carte Vitale 2 :

- **Carte CPS** pour les professionnel de santé, directeurs d'organisme

[35] Cf. la partie technique de ce mémoire notamment la page 18
[36] Dans *Le Généraliste* du 15 septembre 1998
[37] Cf. arrêté du 9 avril 1998 relatif aux spécifications physiques et logiques de la carte de professionnels de santé

- **Carte CPF (Carte de Professionnel de Formation)** pour les étudiants à partir de la 6éme année validée

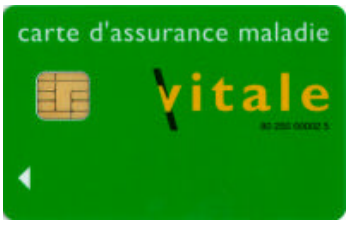
- **Carte CPE (Carte de Personnel d'Etablissement)** pour les personnels habilités par l'employeur (secrétaire médicale)

**- Carte CPA** pour les personnels autorisés. Les fournisseurs de service qui veulent s'authentifier auprès des professionnels de santé peuvent utiliser la carte CPA, émise par le GIP-CPS et qui identifie les fournisseurs d'applications (et leurs ordinateurs).: Les documents signés deviendront opposables au propriétaire de la carte, leur identité et leur qualité étant inscrite dans la mémoire de la carte[38].

La CPS dite de troisième génération (ou CPS 2 bis) devrait permettre des solutions communes de sécurisation des messageries et d'interopérabilité des échanges. Son utilisation future sera abordée dans la partie consacrée aux réseaux de santé.

*b) Le système* SESAM-VITALE*:*

Le début du projet **SESAM-VITALE** est plus ancien. Il date de 1978. Les intervenants du projet sont nombreux : **CNAMTS** (Comité de déploiement, Comité des sages, Maîtrise d'ouvrage, Centre National de Dépôt et d'Agrément, GIE Sesam-Vitale), **Ministère de la Santé** (Direction de la Sécurité Sociale, GIP Carte de Professionnel de Santé), **collectifs d'industriels** (Groupement des labellisées de l'Assurance Maladie, SNIIS) sans oublier le Conseil Supérieur des Systèmes d'Information de Santé...


La carte Vitale 1 est utilisée pour sécuriser la constitution des feuilles de soins électroniques (FSE) et pour leur envoi grâce au **Système Electronique de Saisie de l'Assurance Maladie (SESAM).** Cette procédure permet de saisir, de façon informatique, une FSE et de la transférer aux caisses d'assurance maladie en vue de remboursement des prestations (à l'assuré ou au Professionnel de santé en cas de tiers payant). Il faut toutefois noter que la seule transmission des feuilles de soins électroniques ne nécessitait pas en soi une carte à puce, (par exemple la télétransmission réalisée actuellement par les laboratoires de biologie ou certaines pharmacies se fait sans carte Vitale). Elle est pour le moment "familiale" (valable pour les ayants-droit) mais est appelée à évoluer vers une version 2 individuelle. Dotée d'un microprocesseur, la carte Vitale 1 contient le dossier administratif de l'assuré social (existant sur la carte d'assuré social) permettant de l'identifier. Un décret indique que la carte électronique est appelée "**carte d'assurance maladie**" et précise les

[38]Cf. annexe 1 pour connaître l'état du déploiement des cartes de la famille CPx au 4 septembre 2000

conditions de délivrance, de renouvellement, de mise à jour et d'opposition en cas de perte ou de vol. La Carte d'Assurance Maladie (Vitale 1) contient les **données administratives de l'assuré et de ses ayants droits**. Elle n'a pas de fonction de paiement et ne contient aucune donnée médicale pour le moment. Sa capacité est limitée à 8 Ko dont la moitié (soient 4 Ko) est utilisée. Lors de la délivrance de la carte, l'assuré reçoit une "copie sur papier" des informations administratives y figurant. L'assuré a le droit de la faire rectifier. Ce n'est que sous réserves de consentement écrit du porteur que figurent les droits ouverts en couverture complémentaire. La durée de validité des droits obligatoires est inscrite automatiquement. La carte Vitale peut être mise à jour au moyen de bornes télématiques. L'assuré devra "signaler tout dysfonctionnement, perte ou vol" de sa carte et une **liste d'opposition sera créée par les organismes d'assurance maladie** comme c'est le cas pour les cartes bancaires. Il était prévu d'en distribuer à chaque famille, soit **15 millions d'exemplaires** et probablement à chaque assuré soit 26 millions de cartes VITALE 1.

Lors d'une consultation, l'assuré présente sa carte au médecin qui l'introduit dans un lecteur après y avoir glissé sa propre carte de professionnel de santé. Le médecin coche la catégorie de l'acte médical effectué, signale son tarif et atteste du paiement. En cas d'échec de la transmission, le patient peut obtenir le remboursement en produisant une copie électronique ou un duplicata sur papier, dans une période de 15 à 90 jours suivant la consultation. Dès lors que le praticien se résout à la télétransmission des FSE, il doit obligatoirement disposer des équipements suivants : la Carte du Professionnel Santé, la Carte Vitale de l'assuré, un lecteur de carte SESAM-Vitale et une connexion vers un réseau de télétransmission et le logiciel requis à cette tâche. En pratique, le choix du moyen de télécommunication dépend directement du lecteur de carte choisi par le praticien. En effet, certains lecteurs constituent de véritables "solutions intégrées" parfaitement autonomes et donc capables de télétransmettre les FSE sans ordinateur associé. En revanche, les lecteurs destinés à être connectés à un ordinateur ne disposent d'aucune capacité de télécommunication. Dans ce cas, c'est l'ordinateur qui réalise la télétransmission par l'intermédiaire de son modem. Le médecin a alors le choix entre les différents acteurs du marché listés précédemment. Quelle que soit la solution envisagée, les différents organismes officiels ainsi que les revues médicales spécialisées conseillent au professionnel de santé de s'équiper de l'ensemble de ces éléments auprès du même fournisseur, afin de faciliter la maintenance et d'éviter que les différents prestataires ne se renvoient le problème en cas de dysfonctionnement.

Ainsi, le lecteur SESAM-Vitale est le seul équipement nécessaire à la réalisation d'une FSE. C'est un appareil identique à ceux utilisés pour lire les cartes bancaires. Certains de ces lecteurs acceptent d'ailleurs une carte bancaire. Il a cependant la capacité de lire

deux cartes simultanément : celle du professionnel de santé (CPS) et celle du patient (Vitale). Schématiquement, il est possible de différencier deux grands types de lecteurs SESAM-Vitale. D'un côté, on trouve les lecteurs aptes à télétransmettre les FSE indépendamment de tout ordinateur (avec les lecteurs totalement autonomes (Intellio) et les lecteurs réclamant un dispositif supplémentaire de télétransmission comme le Minitel pour le lecteur Méditrans). De l'autre, on a des lecteurs nécessitant un ordinateur équipé d'un modem afin de profiter de ses capacités de télécommunications. Dans tous les cas, le logiciel utilisé pour la télétransmission doit être agréé par un organisme habilité, le **CNDA** (Centre National de Dépôt et d'Agrément). Chaque mois, de nouveaux modèles reçoivent cet agrément et peuvent dès lors être mis sur le marché.

*c) La carte VITALE 2 :*

La **carte VITALE 2,** (carte individuelle) est en cours de conception et de négociation. Cette carte sera nominative (une par bénéficiaire). Il y aura donc à terme 48 à 60 millions de cartes (on ne sait pas encore si les moins de 16 ans en auront une). Actuellement, le Numéro de Sécurité Sociale est créé à l'entrée de la vie active ou pour les étudiants. La tenue du fichier nommée **RNIAM** (Répertoire National Inter régimes de l'Assurance Maladie) est confiée à la CNAVTS (Caisse Nationale d'Assurance Vieillesse). Avec VITALE 2, il faudra apparemment créer un numéro de sécurité sociale dès la naissance. Cette carte est, avec son volet de santé, présentée comme nécessaire pour assurer la continuité et la coordination des soins. Il convient de s'interroger sur les bénéfices réels pour le patient, aux vues des risques d'utilisation détournée et des risques d'utilisation défectueuse liée à la qualité et à l'intégrité des informations (par exemple : effacement de données, informations erronées ou incomplètes, difficultés liées au codage, non identification de l'émetteur pour certaines informations, etc.).

En janvier 1998, la Mission sur l'Informatisation (en accord avec le Conseil de l'Ordre des Médecins et la CNIL) a été chargée par le gouvernement de définir ce contenu. On évoquait la mémorisation des 3 derniers mois de FSE, la photo du patient, **Volet d'informations Médicales** (**VIM**), etc. La CNIL encore aujourd'hui "*s'interroge sur l'utilité de cette carte de santé à l'heure du développement des réseaux et des standards de communication, qui permettent aujourd'hui de disposer en temps réel de l'information que l'on souhaite même stockée en des lieux différents*". De plus, le contenu de ce VIM n'est pas encore défini. Juridiquement il repose sur l'ordonnance du 24 avril 1996 "*Le carnet de santé peut être porté sur le volet médical de la carte mentionné à l'article L 161-31"*. La quantité de mémoire de la carte conditionnera le volume d'information possible. Il est prévu que les informations soient normalisées et codées. Dans la zone "suivi de soins", on y trouvera sans

doute les antécédents médicaux, les dates et motifs des dernières consultations et hospitalisations, les dates d'examen et de prescription ainsi que les résultats de certains dépistages. Comme la place semble très limitée (8 Ko), des "pointeurs" vers d'autres sources médicales plus détaillées pourraient y prendre place. Avec la carte CPS, le médecin traitant aura accès à ce VIM, ainsi que d'autres professionnels de santé, mais seulement pour certaines catégories d'information. Le patient pourra refuser que certaines informations soient inscrites sur ce VIM. Comme pour le carnet de santé, il n'y aura aucune obligation pour le patient comme pour le médecin de remplir ce VIM.

La sécurisation des données de la carte Vitale 2 pose problème avec la banalisation dans les entreprises de lecteurs de carte à puce. Le patient devra-t-il taper un code pour autoriser la lecture du VIM ? La CNIL s'interroge sur la "*nécessité de prévoir la frappe par le patient, d'un code secret, pour permettre l'accès par le médecin habilité, au volet médical de la carte, pour ce qui concerne la zone suivi de soins.".* Une partie de la carte constituée "à la demande expresse du titulaire" serait accessible aux professionnels de santé européens lors des voyages à l'étranger, sans carte professionnelle type CPS. Sur ce volet dit d'urgence, pourraient être indiquées les affections chroniques. En France, en revanche, il faudra une CPS et l'accord du patient. La CNIL en particulier souhaite une sécurisation de ce volet, en effet il existe des lecteurs de carte à puce très peu onéreux avec lesquels, un employeur mal intentionné ou une compagnie d'assurance pourrait le lire. Certaines mutuelles désirent inscrire aussi sur la carte des informations.

Il a été aussi envisagé que Vitale 2 soit le "carnet de santé électronique". Dans cette hypothèse sa capacité aurait dû être de plusieurs Mo. Dans ce cas, la technologie différente de la carte VITALE 1 aurait interdit la lecture et l'écriture par les lecteurs bifentes VITALE 1 . Depuis, la technologie a évolué en particulier avec l'avènement des réseaux comme Internet. Le carnet médical électronique du futur pourrait être virtuel, la carte ne contenant que les adresses électroniques (e-mails des médecins, adresses URL des sites sur lesquels sont stockés les éléments du dossier médical). Finalement, sa capacité serait seulement le double de la carte VITALE 1. Dans ce cas, une simple mise à jour du logiciel du lecteur bi-fente devrait permettre de l'écrire. Afin de pallier les défaillances de la télétransmission, l'assuré disposera en mémoire d'un duplicata des feuilles de soins électroniques sur 3 mois (décret du 30 décembre 1997), fonction qui permettra dans des cas exceptionnels à l'assuré de se faire rembourser des soins aux guichets des CPAM.

Force est de constater que cette évolution de la carte VITALE soulève de nombreux débats aujourd'hui dans lesquels les problèmes d'utilisation et les questions de sécurité sont omniprésents.

**3) Les débats sur la sécurité et l'utilisation de ces outils perdurent :**

*a) Le respect de la vie privée :*

En marge de la loi portant création de la couverture maladie universelle, le Parlement a adopté des dispositions relatives au volet santé de la carte de sécurité sociale, la future carte Vitale 2. Cette carte à puce aura donc une double fonction, carte de sécurité sociale et carnet de santé. Le volet santé est destiné à recevoir des informations relatives d'une part aux interventions urgentes, d'autre part à la continuité des soins. Pour protéger le droit au respect de la vie privée, le projet prévoit que la mention des données de santé sur la carte du patient est subordonnée à son accord, et que la faculté lui est offerte de "verrouiller" l'accès à une partie des données enregistrées au moyen d'un code secret défini par lui-même. En outre le praticien de santé devra s'identifier au moyen de sa carte de professionnel de santé (CPS) pour accéder à certaines informations médicales figurant sur la carte du patient. Aussi importantes que soient ces garanties, elles ne doivent pas être surestimées. Le patient sera nécessairement perplexe quand il devra verrouiller l'accès aux diverses catégories d'informations médicales. Par exemple, comment une femme s'assurera-t-elle que l'information est cloisonnée de telle sorte que son ophtalmologiste n'apprenne pas qu'elle a subi une IVG ? De plus, les éventuels désaccords entre le patient et son médecin sur l'intérêt de mentionner une information seront potentiellement une source de conflit, le médecin pourra alors estimer que sa responsabilité professionnelle est mise en cause par l'absence de cette information sur la carte. Ainsi sera perturbée la relation entre patient et praticien de santé, jusqu'alors fondée sur la confiance et la garantie du secret médical. Cet aspect est actuellement gravement sous-estimé.

Dès lors que les patients exprimeront diversement leur accord pour inscrire leurs données de santé, le contenu de la carte ne sera pas le reflet des éléments du dossier médical utiles à la continuité des soins (par exemple pour les pathologies lourdes ou les situations d'urgence). Selon le choix effectué par le patient, le médecin tirera éventuellement profit de la lecture d'une information sur la carte, mais inversement l'absence de cette information ne saurait éliminer telle ou telle orientation diagnostique. Hors situation d'urgence vitale, le dialogue et la relation du praticien avec le patient et avec les autres professionnels de santé que celui-ci a consultés demeurent primordiaux pour assurer la qualité de l'information nécessaire à la prise de décision médicale. Ainsi l'utilité médicale du volet santé doit être considérée comme relative. La décision, pour le patient, de faire enregistrer ses données de santé sur sa carte exigera de lui un arbitrage permanent entre des enjeux contradictoires. Les patients n'auront pas la certitude que seuls des professionnels de santé seront à même de consulter le volet santé de leur carte : les données relatives aux

interventions urgentes pourraient demeurer libres d'accès, sans nécessiter l'usage de la CPS. Ainsi, quiconque possédant un lecteur de carte (assureur, employeur...) pourrait visualiser des informations susceptibles de figurer sur la partie urgences, telle la prise de médicaments psychotropes. Les utilisateurs de Vitale 2 adopteront-ils un système qui ne leur garantit pas la confidentialité de l'ensemble des données du volet santé ?

*b) Une informatisation massive, facteur de dérives potentielles :*

Les citoyens assistent au développement du projet SESAM-Vitale dans un contexte marqué par la récente décision d'interconnexion des fichiers fiscaux et sociaux au moyen du numéro de sécurité sociale. Vu les questions soulevées par le volet santé de la carte, les patients s'interrogeront légitimement sur les moyens d'assurer la sécurité et l'intégrité, la confidentialité et le non détournement de leurs données de santé, dans un système gérant 60 millions de personnes et 300 000 praticiens de santé. Et ce, d'autant plus que les multiples réseaux destinés à acheminer les informations médicales nominatives ne présentent pas à ce jour des garanties de sécurité optimales ; sans oublier que certains de ces réseaux sont aux mains d'entreprises ayant des intérêts dans le secteur de la santé (sociétés d'assurances, banques, industries pharmaceutiques...).

La situation actuelle de l'informatisation du système de santé est notamment marquée par le choix des responsables politiques en faveur d'une informatisation massive et ambitieuse. D'où un dispositif qui comprend le codage des actes, des prescriptions et des pathologies, la télétransmission de ces informations aux caisses d'assurance maladie via le RSS, la constitution d'un fichier unique des assurés sociaux et de leurs ayant droits identifiés par le NIR, l'attribution à chaque citoyen de la carte Vitale, administrative dans sa version 1 depuis 1998 puis médico administrative dans sa version 2 repoussée vers fin 2000. Les divers acteurs de la santé restent encore perplexes excepté quelques prises de position notables comme celles de la CNIL. Certains acteurs des administrations concernées et du domaine de la santé publique craignent pour les libertés. De même ils doutent du caractère indispensable du dispositif Sesam-Vitale pour la télétransmission des feuilles de soins électroniques (FSE).

Mais la question essentielle, préalable à toute constitution de n'importe quel réseau (national ou de télémédecine régionale) est de savoir si **le stockage des informations médico-sociales sur chaque personne apporte avantage pour le suivi médical du patient ou comporte plutôt un risque majeur d'atteinte à la vie privée du citoyen**. Dans le cas de l'architecture nationale combinant RSS, CPS et carte VITALE que cette partie du mémoire étudie, le fait que le codage des actes, des prestations et des pathologies, soit

transmis aux caisses d'assurance maladie sous forme électronique et en étant identifié avec le NIR, ou avec tout autre identifiant de portée générale, représente pour les citoyens un des risques majeurs de ce dispositif. Avec le chaînage des pathologies codées, on pourrait assister à la mise en place d'un authentique casier sanitaire. Tout ou partie de ces informations est appelé à figurer sur la carte Vitale 2 qui constituerait alors un extrait de casier sanitaire. Une banalisation du caractère confidentiel des informations nominatives est à craindre, dès lors qu'elles figureront sur un support qui appartiendra aux objets de la vie quotidienne (carte Vitale 2).

Placé en situation de demandeur, par exemple, certains, se sachant indemnes de toute pathologie, pourraient même être tentés d'aller au devant de toute demande, en présentant spontanément à l'employeur certaines données du volet médical de leur carte attestant de leur bon état de santé, d'autant plus qu'une copie papier de certaines de ces données pourrait être légalement délivrée. L'intérêt des employeurs, des banquiers, des assureurs pour les bases de données relatives à la santé des personnes est également évident. Les risques de détournement de finalité le sont tout autant, puisque justifiés au nom de la concurrence économique. Le casier sanitaire pourrait aussi servir à cibler les malades par profils et à mettre en regard une offre de soins restreinte prédéfinie, ceci dans une logique de mise en concurrence des caisses de sécurité sociale avec les assurances privées. Qu'en serait-il des fichiers sanitaires des personnes constitués par ces caisses puis confiés au privé ? Alors les informations ne seraient-elles pas utilisées dans une logique assurantielle de sélection préalable des risques ou croisées avec les fichiers d'assurance vie, de prêts...? Par ailleurs, les pouvoirs publics locaux et nationaux comme les organismes de protection sociale pourraient eux aussi être tentés d'utiliser ces données dans une perspective de gestion ou de contrôle des populations dites à risque.

L'exhaustivité et le regroupement des informations médico-sociales nominatives dans un fichier unique, identifiées avec le NIR ou avec tout autre identifiant permanent de portée générale, créent de fait les conditions objectives de toutes ces dérives potentielles, d'autant plus que ces informations seront aisément accessibles.

Toutes ces interrogations et ces craintes évoquées ici dans un cadre national (car liées à la carte Vitale 2 et à son utilisation) se retrouvent à l'échelon local. La problématique reste identique dans un réseau de télémédecine. Ces mêmes débats s'appliquent à tous les professionnels de santé et c'est dans ce domaine que la cryptographie associée à un bon questionnement préalable et nécessaire sur l'utilité du réseau à mettre en place entre en jeu.

## III) FACE A LA LIBERALISATION DE LA CRYPTOGRAPHIE ET AU RENOUVELLEMENT DE CERTAINS OUTILS, PLUSIEURS SYSTEMES D'ORGANISATION DE RESEAUX SECURISES DE TELEMEDECINE PEUVENT ETRE IMITES COMME CELUI DU CHRA OU D'AUTRES A VOCATION LOCALE OU NATIONALE :

### 1) La libéralisation de la cryptographie permet de bâtir des solutions communes plus efficaces avec la facilité d'utiliser la future CPS :

*a) La libéralisation de la cryptographie : un nouveau souffle pour les réseaux de télémédecine :*

Obligation légale pour l'échange des données à caractère personnel, le cryptage, ou chiffrement, n'était jusqu'ici réservé qu'à quelques réseaux expérimentaux. Mais voilà que le développement des Intranet médicaux amènent les différents opérateurs à proposer des services de cryptage. A titre "provisoire" car la généralisation de la CPS troisième génération, porteuse de clés de chiffrement, se fait encore attendre. Cette attente est peut-être liée au fait qu'on a longtemps estimé que peu de personnes pouvaient être intéressées, par exemple, par la transmission des taux d'albumine ou de cholestérol d'un patient X et que l'activité de pirates informatiques n'allait pas se porter sur ce type d'échanges. La CNIL s'en est pourtant (et à juste titre) inquiétée dès 1993 dans une recommandation. Il s'agissait alors de la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques. L'internet médical était dans les limbes. Mais déjà la CNIL jugeait que la protection par mots de passe n'était pas suffisante et recommandait l'utilisation de la cryptographie. Ainsi, les promoteurs d'un réseau d'échanges médicaux devaient-ils à la fois souscrire une déclaration à la CNIL et demander, au-delà des clés de 40 bits, une autorisation de cryptage au SCSSI. Ainsi ont démarré les réseaux ville-hôpital de Montpellier, d'Armentières, d'Annecy ou l'Intranet Apicem.

Le réseau ville-hôpital d'Annecy[39] qui relie aujourd'hui 70 médecins libéraux à une dizaine de services du centre hospitalier a dû, par exemple, obtenir l'autorisation de crypter les messages avec une clé à 56 bits. "*Le réseau a démarré en 1997 en utilisant la messagerie Eudora et le logiciel de chiffrement S-Tool de la société Cesir* ", explique le Dr Xavier Courtois, médecin DIM au **Centre Hospitalier d'Annecy**, qui reconnaît que ce n'était pas très ergonomique. Dans le système original, c'est la pièce jointe qui est cryptée : il faut donc extraire le document du logiciel médical, le mettre au format RTF, effectuer trois ou quatre manœuvres pour le crypter. Malgré tout, 400 messages partent chaque mois de l'hôpital vers les médecins de ville. Le médecin peut envoyer à l'hôpital le dossier d'un

[39] Cet exemple sera étudié en détail dans ce mémoire à partir de la page 55

patient hospitalisé en urgence. "*Nous sommes en train d'évoluer vers un réseau Extranet, avec assistance à l'utilisateur*, poursuit le Dr Courtois, *à terme, nous souhaitons utiliser la CPS*".

Autre expérience, celle de l'association **Apicem**[40] et de son logiciel Apicrypt. Le système a été mis au point pour développer la transmission des données nominatives dans le cadre de l'Intranet de l'association dunkerquoise. "*La solution choisie repose sur la messagerie Eudora, mais on peut aussi utiliser Outlook*, explique le Dr Alain Caron, président d'Apicem, *il n'y a pas d'échange de clés car les messages passent par un Serveur qui gère toutes les clés privées*". Apicrypt a démarré en 1996 et une quarantaine de médecins s'en servent, payant un abonnement de 290 F TTC/mois. Fin novembre, ils seront 200 dans le cadre d'un projet soutenu par des fonds européens.

L'arrivée de plusieurs Intranet médicaux à vocation nationale au cours des dix-huit derniers mois a sensiblement changé la donne, en offrant aux médecins des facilités accrues de communication. La tentation est grande de faire voyager quelques messages médicaux, avec l'illusion que la protection de l'accès par login/mot de passe est suffisante. N'a-t-on pas surpris un médecin qui transférait par email, en toute innocence, semble-t-il, ses dossiers médicaux, de l'ordinateur du cabinet à celui de la clinique ou de l'hôpital... Pour éviter ce genre de situation qui ne manquerait pas de se transformer en "affaire" médiatique, il devient urgent de proposer des messageries sécurisées par chiffrement.

La libéralisation du cryptage jusqu à 128 bits annoncée par Lionel Jospin le 19 janvier 1999 et l'autorisation d'exportation des produits de cryptage récemment accordée aux industriels américains sont autant de facteurs qui poussent à développer des moyens de chiffrements forts. Moyennant quoi, le RSS a été le premier, à proposer, dès la fin de 1998, à ses abonnés le chiffrement de leur message à 40 bits sur un réseau sécurisé, mesure de sécurité d'ailleurs prévue dans son cahier des charges. Les médecins sont un millier à avoir demandé leur certificat. La liste des certificats est gérée par le RSS qui est autorité de certification. C'est sur cette liste que l'on vient chercher le certificat qui contient la clé publique de son correspondant. La clé privée est en revanche conservée sur le poste du professionnel de santé. Cegetel.rss a intégré le logiciel de cryptage de Netscape (voir encadré) qui utilise les standards S/MIME et SSL (qui permet de chiffrer des flux web). Le choix de ce standard permettra de correspondre aussi avec des médecins abonnés à d'autres réseaux, sous réserve de connaître leur clé publique et pour peu qu'on ait pris la peine de joindre son certificat au message. Le passage à 56 bits est en cours et le 128 bits devrait être opérationnel à la fin de l'année dès que les logiciels seront agréés par le SCSSI.

[40] Cet exemple sera étudié également en détail dans ce mémoire à partir de la page 66

Ce qui n'empêche pas, bien sûr, Cegetel.rss de travailler avec le GIP CPS pour utiliser la CPS de 3éme génération dès sa sortie (voir plus loin).

C'est également dans un contexte "provisoire" que France Telecom propose, dès l'ouverture de Libéralis, intégré dans la messagerie Lotus Note, un logiciel à 56 bits (et bientôt 128 bits), conforme lui aussi au protocole S/MIME. La clé privée est stockée sur le poste de travail et la CPS contrôle le déblocage des clés. Un certificat Certplus correspondant àla CPS habilitée sera délivré au médecin en même temps que l'abonnement à l'Intranet des Unions. France Télécom reconnaît avoir choisi là un palliatif d'utilisation simple et sûr, l'avenir restant la CPS de 3éme génération. " *Nous fondons sur elle beaucoup d'espoir, à condition qu'elle soit conforme aux standards internationaux* ", prévient Jean-Marc Deshayes, responsable de l'offre Intranet santé, chez France Telecom. Chez Cegedim, la question du cryptage des échanges sur l'Intranet Santénet commence juste àse poser.

*b) La modernisation des réseaux et la recherche de solutions communes :*

"*La libéralisation permet de sortir de la vision française avec tiers de confiance et d'envisager des constructions standards*, note Robert Grandi de Cegedim*, si la CPS est au rendez-vous, nous l'utiliserons, sinon il n'y aura aucune difficulté pour faire monter le niveau de cryptage du réseau. Mais il faudra que l'enjeu soit important et que cela ne pose pas de problème d'ergonomie*". Club Medical Expand travaille "pour la fin de l'année" sur un système de cryptage asymétrique respectant le protocole S/MIME. Medsyn, le réseau développé par MG-France utilise déjà du *"brouillage*" (sic) de type S/MIME. Mais tous attendent surtout la nouvelle CPS pour démarrer un réel cryptage des échanges sur le réseau. "*Compte tenu du flux des échanges à l'heure actuelle, il n'y a pas d'urgence*, estime le Dr Roussy, l'un des responsables de Medsyn, *il ne faut en aucun cas créer une tour de Babel artificielle, ce serait dramatique et inacceptable"*, tout en rappelant que la sécurité par login/mot de passe est largement supérieure àla confidentialité d'un courrier, d'un téléphone ou d'un fax. Le Conseil supérieur des systèmes d'information de santé n'a pas dit autre chose dans son rapport d'activité 1998, s'inquiétant de l'interopérabilité des réseaux et de l'obligation pour les professionnels de santé de disposer d'outils de chiffrement identiques pour réaliser des échanges dans un environnement sécurisé. Et de souligner le caractère "provisoire" des systèmes de chiffrement proposés, dans l'attente de la CPS.

Le grand mérite de la CPS nouvelle génération, dite CPS 2 bis, sera de concentrer toutes les fonctions de la sécurité. La fonction d'authentification est déjà réalisée (l'accès n'est autorisé qu'aux personnes reconnues), la fonction de signature électronique est opérationnelle : elle garantit l'intégrité, du message et l'identité de son auteur; la fonction

chiffrement est en cours de réalisation. "*Les conditions étaient d'utiliser des outils de cryptologie compatibles avec les standards du marché*", rappelle Gilles Taib, directeur du GIP CPS.

Le principe du système CPS est le suivant : le logiciel de chiffrement (non encore connu) utilise l'algorithme triple DES et le chiffrement des clés de session se fait sur la base d'un algorithme RSA. La CPS porte l'ensemble des conventions secrètes (biclé publique et privée à 1 024 bits) qui se trouvent, dans les autres systèmes, dans le poste de travail Le GIP CPS assure la gestion clés certificats. Le professionnel de santé dispose d'un annuaire local de ses correspondants afin de les retrouver facilement. Il s'en sert pour constituer son propre annuaire."*Les aspects ergonomiques sont essentiels*, souligne Gilles Taib, *avec cette nouvelle CPS, il n'y aura plus besoin de demander un certificat c'est un nouveau service pour le professionnel de santé, qui sera intégré à la messagerie par les opérateurs dans le kit de connexion*." Les éditeurs auront également les outils nécessaires pour les intégrer dans leurs logiciels. Actuellement, les deux opérateurs Cegetel.rss et France Telecom ont signé un contrat avec le GIP pour utiliser la CPS. Medsyn a fait une demande en tant que fournisseur de services. Ces derniers figureront sur l'annuaire et auront une CSA (carte serveur applicatif) leur permettant de déchiffrer les messages qui leur sont transmis.

"*La CPS 2 bis remplacera peu à peu la CPS 2 qui ne possède pas la fonction de chiffrement. Une migration douce qui prendra deux ans. Une procédure de renouvellement anticipée est prévue pour ceux qui en feront la demande*" indique Gilles Taib. Mais il faut aussi compter avec la lourdeur de la gestion du parc informatique installé qui met en oeuvre de nombreux acteurs : opérateurs (plus nombreux qu'il n'était prévu !), éditeurs, revendeurs… Pour éviter que le "provisoire" ne dure, non seulement la CPS doit être à l'heure au rendez-vous, mais la logistique doit suivre.

c) *Les spécifications du GIP CPS nécessaires au développement d'outils de chiffrement de forte sécurisation à 128 bits des messages pour le secteur de la santé :*

Le GIP CPS a récemment diffusé les spécifications nécessaires au développement d'outils de chiffrement des messages de forte sécurisation à 128 bits[41]. Partant du constat que plus de 230 000 cartes ont été distribuées à ce jour aux différents acteurs du monde la santé et que plus de 300 000 cartes le seront avant la fin de l'année 2000, le GIP CPS cherche à renforcer la position centrale du système CPS pour la sécurité informatique dans

[41] Ces dispositions sont disponibles in extenso sur http://www.gip-cps.fr/fr/Gip-Cps/messagerie.htm

le secteur de la santé. L'objectif est de garantir la confiance des échanges électroniques dans le cadre d'une prise en charge cohérente des patients. En plus des fonctions actuellement utilisées par les professionnels de la santé évoquées dans ce mémoire (le contrôle d'accès sécurisé par authentification d'une carte validant l'identification et la qualité du porteur et la certitude de l'origine du message et de son intégrité par le biais de la signature électronique), de nouveaux outils de sécurisation de messageries seront mis en place avec la volonté d'assurer une totale confidentialité des échanges quels que soient les réseaux et les produits logiciels de messageries choisis.

La protection des données personnelles et le respect des règles déontologiques obligent à mettre en œuvre des solutions communes de sécurisation de haut niveau. La croissance du volume des échanges, et la liberté pour chacun de choisir son opérateur et ses outils nécessitent aujourd'hui une évolution rapide vers des solutions globales. On a vu que les grands réseaux médicaux nationaux sécurisaient déjà leur accès par le système CPS et que la confidentialité des messages était également proposée grâce à des solutions de sécurisation dépendantes des choix de l'opérateur. Les nouvelles solutions doivent être adaptées aux besoins des professionnels de santé et visent à améliorer la qualité et la continuité des soins qu'ils délivrent à leurs patients. Elles doivent éviter aux utilisateurs toute rupture technologique (compatibilité ascendante et transparence des usages). C'est pourquoi, les membres du Groupement d'Intérêt Public ont donné pour mission au GIP CPS de définir les spécifications d'une solution de sécurisation des messageries s'appuyant sur le système CPS et assurant l'interopérabilité des échanges.

Ces principaux éléments constitutifs des spécifications sont :

- la signature et l'authentification par la Carte du Professionnel de Santé.
- un appui sur les standards permettant de s'ouvrir vers d'autres milieux que la santé.
- des mécanismes cryptographiques robustes évolutifs "aptes à suivre l'état de l'art"
- des solutions utilisables avec les produits du marché actuels (Microsoft Outlook, Netscape, etc.) pouvant s'ouvrir sur de nouveaux produits émergeants et compatible avec les diverses applications du secteur, en particulier Sesam Vitale
- une carte indispensable pour déchiffrer un message reçu
- la prise en compte des listes d'oppositions mises à jour par le GIP CPS dans son annuaire.
- une utilisation simple et transparente pour l'utilisateur
- une solution pouvant être disponible rapidement et utilisant les cartes existantes.

Cela a conduit le GIP à proposer une solution de sécurisation s'articulant avec les messageries du marché et s'appuyant sur :

- des bi-clés de confidentialité générées et stockées de manière sûre dans le poste
- une certification des clés publiques par le GIP avec un lien fort avec la carte et intégration du certificat dans l'annuaire GIP
- un rôle central de l'annuaire du GIP pour gérer, et diffuser dans la communauté de la santé, les informations nécessaires à la sécurité (clés publiques, certificats, listes d'opposition) et à l'interopérabilité.

Lors de l'assemblée générale du 15 juin 2000, le GIP CPS a arrêté les orientations pour la mise en œuvre de la sécurisation des messageries. Elle comporte deux parties :
- le **service d'inscription** permet à un porteur de carte de la famille CPS de faire certifier sa clé publique de chiffrement et d'inscrire ce certificat dans l'annuaire du GIP CPS. Son développement est à l'initiative et sous la responsabilité du GIP. Ce service sera accessible à tous les porteurs de carte de la famille CPS, ceci indépendamment du réseau auquel ils sont affiliés. L'annuaire est la référence dans laquelle seront enregistrés pour les porteurs de cartes de la famille CPS, leurs certificats de confidentialité et les adresses des messageries associés. Sur la base de ces développements, le GIP lancera un appel d'offres pour le choix de l'exploitant du serveur d'inscription. Parallèlement, le GIP élaborera l'annexe de sa politique de certification relative aux certificats de confidentialité (document disponible en octobre 2000).
- le **logiciel de sécurisation des messageries** sera distribué à l'utilisateur final pour intégration dans son environnement informatique. Afin de dynamiser le marché des industriels de la sécurité informatique, le GIP a décidé que la réalisation des logiciels serait soumise à une publication et à une procédure d'homologation sur la base de spécifications fonctionnelles et techniques émises par le GIP CPS. Depuis la fin du mois de juillet 2000, les industriels peuvent retirer auprès du GIP CPS, après signature d'une convention d'homologation, le référentiel des spécifications fonctionnelles et techniques. Cette convention décrit les modalités de vérification et de conformité au référentiel. Les conditions d'obtention de l'homologation favorisent la collaboration entre les différents industriels et le GIP pour anticiper les évolutions techniques futures et les nouvelles réglementations. En janvier 2001, devraient ainsi être diffusés par les industriels auprès des professionnels de santé les premiers produits.

En attendant de développer des réseaux utilisant la solution de la CPS comme procédé d'authentification, il serait plus prudent peut-être de développer des solutions sans l'utilisation de l'actuelle carte qui va être amenée à évoluer. C'est ce que la prudence impose. Toutefois, il est important dans le projet d'intégrer la possibilité de recourir à cet outil performant dans des choix qui doivent être marqués par une évolutivité dans le matériel, les

connexions et les logiciels retenus. C'est un peu ce qui a très tôt animé la démarche du Centre Hospitalier de la Région Annecienne dans la constitution de son réseau de télémédecine.

## 2) Le Centre Hospitalier de la Région Annecienne et ATM 74 :

*a) Contexte et utilité du projet :*

Ce projet a été élaboré en janvier 1995 pour deux raisons. D'une part, a été décidée et autorisée la construction d'un nouvel hôpital à Annecy, sur le site de Metz-Thessy, à l'échéance de 2002-2003 et ce nouvel établissement se veut communiquant. D'autre part, ce projet concerne l'appel à candidatures sur les autoroutes de l'information. Le district et l'hôpital d'Annecy ont réfléchi à la possibilité d'utiliser les nouvelles technologies de l'information dans le cadre d'un projet commun. De plus, est intervenue au printemps 1995 l'ouverture de la fenêtre télémédecine du Conseil de l'Informatique Hospitalière et de Santé, qui visait, justement, à promouvoir certains projets utilisant ces technologies.

Le CHRA disposait d'un contexte assez favorable au développement de cette expérimentation[42]. Tout d'abord, l'ensemble des secrétariats médicaux du Centre Hospitalier était informatisé depuis plusieurs années. En conséquence, les dossiers médicaux de court séjour étaient déjà disponibles sur support informatique. Deuxièmement, l'hôpital possédait un serveur de dossier médical commun. En tout point de l'établissement, il est possible d'accéder à l'ensemble des données médicales relatives aux patients suivis à l'hôpital. Un réseau câblé couvre tout l'établissement, et à l'époque, un travail en réseau s'amorçait avec les médecins libéraux.

Le projet a été constitué à partir d'une réflexion sur les relations entre les médecins de ville et les médecins hospitaliers. Aujourd'hui, s'agissant de communication entre la ville et l'hôpital, les médecins de ville se plaignent de ne pas obtenir d'informations concernant un patient envoyé à l'hôpital. Ils ont l'impression de perdre le patient de vue dès qu'il franchit la porte de l'établissement hospitalier. Pour leur part, les médecins hospitaliers ont un peu le même sentiment de ne pas connaître le devenir d'un patient à l'issue de son séjour hospitalier. Ainsi, il est impossible d'assurer un suivi au long cours d'un patient. Les médecins libéraux ont donc été appelés à exprimer leurs souhaits de communication avec l'hôpital. Concernant le patient hospitalisé lui-même, ils souhaitaient disposer rapidement du résumé de séjour hospitalier. Or, la réglementation prévoit qu'à la sortie d'un patient de

[42] Cette présentation du contexte annecien s'inspire d'une intervention d'Anne-Marie FABRETTI le 21 novembre 1997 au cours d'un séminaire à Castres sur les NTIC avec le Club national des Réseaux de Villes

l'hôpital, le médecin hospitalier doit envoyer une lettre de sortie à son médecin traitant. Les médecins libéraux souhaitaient donc recevoir ce support dans des délais plus brefs. En effet, la seule utilisation du courrier entraîne systématiquement un retard dans la transmission de l'information de l'ordre de trois à quatre jours. Deuxièmement, les médecins libéraux ont besoin de connaître les résultats d'examens effectués à l'hôpital, ainsi que le devenir du patient. Cette communication concerne les dossiers médicaux individuels.

Ensuite, dans les relations ville/hôpital, on peut noter différentes communications téléphoniques pour obtenir des avis spécialisés. Les spécialistes sont sollicités régulièrement pour connaître des conduites à tenir dans des cas particuliers, comme par exemple une pathologie donnée intervenant en période de grossesse, certaines situations peu fréquentes pour les médecins généralistes, mais sur lesquelles les spécialistes peuvent apporter une aide appréciable. Les médecins libéraux peuvent également requérir des conseils en terme d'épidémiologie et de stratégie diagnostique et thérapeutique.

Qui dit réseau de communication dit un émetteur et un récepteur. Un réseau fonctionne si chacun trouve un intérêt à cette communication. Le médecin hospitalier est lui aussi intéressé par une communication avec les médecins de ville. Tout d'abord, pour connaître les antécédents du patient. Il est inutile de recommencer l'ensemble des examens lorsqu'un patient arrive à l'hôpital. Cette démarche est génératrice de surcoûts, bien souvent de souffrance également, et surtout n'est pas très rationnelle, ni très rassurante pour le patient. Le médecin hospitalier souhaite également disposer de données cliniques. Le médecin traitant, qui suit régulièrement le patient, peut disposer de données qui éclairent très sensiblement le diagnostic au moment d'une hospitalisation. De même, le médecin hospitalier est intéressé par les résultats d'examens (radios, examens biologiques) réalisés en ville. Ensuite, le médecin hospitalier souhaite connaître, à l'issue d'une hospitalisation, le devenir du patient. Un médecin aimerait savoir, notamment pour évaluer son intervention, si le devenir du patient correspond bien à ce qu'il avait imaginé.

*b) L'analyse des avantages d'un réseau sécurisé de télémédecine:*

Il est intéressant de reprendre la réflexion qui a été entreprise à l'époque sur les moyens de communication mis en œuvre aujourd'hui dans le cadre d'un réseau ville-hôpital. Jusqu'à aujourd'hui, on utilisait couramment trois supports : le téléphone, la télécopie (même si cet outil n'est pas conforme à la réglementation en matière de confidentialité) et le courrier. Le quatrième support est constitué par l'outil développé par le CHRA : la télémédecine. Le téléphone présente l'avantage considérable d'être simple. Grâce à la communication verbale, on obtient directement les informations. Ce mode de communication est rassurant,

peu coûteux et immédiat. En revanche, il présente un certain nombre d'inconvénients. Tout d'abord, il n'offre pas de véritable sécurité : rien n'empêche une personne de se présenter sous le nom d'un docteur qui aimerait des informations concernant M. X. Rien ne garantit qu'il s'agit effectivement d'un docteur. Il peut très bien s'agir d'un expert d'assurances qui recherche des données sur ce patient. Ce support présente donc effectivement des risques. De plus, il est désorganisant et perturbe l'activité. Il présente également l'inconvénient d'une nécessité de simultanéité de présence au bout du fil des deux interlocuteurs.

Le deuxième support est la télécopie. Aujourd'hui, l'intérêt du fax est la simplicité et l'authentification de l'émetteur. II y a possibilité, par le fax, de transmettre des documents de tous types, aussi bien du texte manuscrit que des images. Il s'agit d'un support très simple à utiliser. En revanche, un fax ne présente aucune garantie de confidentialité et dans le domaine médial, cet écueil est rédhibitoire. Cette solution n'est donc pas très satisfaisante au niveau du respect de la confidentialité. La télécopie ne comporte pas non plus d'avis de remise, ni d'historique.

Le troisième support est constitué par le courrier. Son intérêt repose sur sa simplicité et son authenticité. Il est signé et lorsque le médecin a envoyé un courrier signé, il est effectivement l'émetteur de cet envoi. En revanche, son inconvénient majeur est sa lenteur et la dépendance à l'égard des délais de poste. Et surtout, l'efficacité du courrier est liée à l'organisation. Le médecin dicte son courrier, la secrétaire le dactylographie, puis l'envoie. En fonction de la longueur de ce circuit, il n'est pas rare qu'une lettre de sortie parvienne au médecin traitant 6 à 8 jours après le départ du patient de l'hôpital. On réalise donc que si le contenu du courrier lui-même est intéressant, le délai de transmission lui fait perdre beaucoup de pertinence.

Quels sont donc les avantages du projet de communication ville-hôpital par la télémédecine ? D'abord la simplicité : l'apprentissage du système proposé est relativement aisé. L'intérêt porte également sur l'automatisation des tâches, la sécurisation puisque le système proposé par le CHRA dispose d'un avis d'envoi, d'un cryptage des données, garantissant la confidentialité. La solution initiale de cryptage développée par la société Cesir avec son logiciel S-Tool reposait sur une clé de 56 bits, donc plus forte que le RSS à l'époque[43]. L'hôpital d'Annecy a dû obtenir un agrément de la CNIL (avis favorable à titre expérimental du 24 juin 1997 n°453828) pour pouvoir utiliser cette solution pour l'échange de données nominatives. Cette communication repose aussi sur une certaine organisation qui

[43] Cf. *La santé demain. Vers un système de soins sans murs*, coordonné par J-P CLAVERANE et C. LARDY, Centre Jacques Cartier, Economica, 1999

intègre l'utilisation de la télémédecine dans le fonctionnement quotidien des services hospitaliers, aussi bien que des cabinets libéraux. Ce système est également de disponibilité permanente. Les inconvénients concernent l'investissement en ordinateurs. Il ne faut pas négliger non plus l'aspect formation. Même si l'outil est simple à utiliser, il faut assurer la formation des utilisateurs pour qu'ils l'utilisent effectivement sans appréhension. Le troisième inconvénient concerne l'utilisation du clavier qui demeure, aujourd'hui, incontournable.

*c) Objectifs et méthodes :*

À partir de cette volonté de communiquer de médecins libéraux et de médecins hospitaliers, un projet a été constitué qui poursuivait plusieurs objectifs.
Les objectifs techniques étaient de constituer un réseau de communication interactif et convivial, se greffant sur les systèmes informatiques existants, donc hétérogènes. Il s'agissait bien d'ajouter alors une simple couche de communication aux systèmes existants. Il était hors de question de contraindre les médecins à s'équiper d'un système précis. Cette solution constitue une messagerie professionnelle améliorée.

Les objectifs médicaux essentiels étaient donc l'échange de données médicales nominatives sécurisées au sujet de patients suivis en commun, l'enrichissement itératif du dossier médical afin de faire en sorte que le dossier médical ne soit pas des successions de vues, mais bien un dossier suivi dans le temps. Il s'agissait aussi d'apporter une continuité à la prise en charge du patient, c'est-à-dire éviter tous les examens redondants si fréquents dans le système de soins français, facteurs de surcoût, recommencés lorsqu'un nouvel intervenant prend en charge le patient. Cette continuité de prise en charge apporte également une sécurité supplémentaire au patient.

Deux espaces ont été constitués : un espace médical et un espace de communication. Ils répondent aux besoins d'échange des données médicales nominatives, de demandes d'avis de spécialistes et d'envoi de ces avis. Ceci permet l'obtention et la mise à disposition d'informations. Par exemple : il apparaît, à partir des analyses bactériologiques, qu'un germe est en cause dans une épidémie quelconque. Très facilement, par un système de forum, il est possible de diffuser des informations concernant la stratégie thérapeutique à adopter. Cette démarche permet d'éviter la prescription de traitements trop lourds, lorsqu'un traitement moins agressif et mieux ciblé sur le germe à combattre peut être conseillé. Cette diffusion d'informations peut éviter quinze à vingt communications téléphoniques par jour pour le spécialiste des maladies infectieuses par exemple.

A l'hôpital d'Annecy existe un réseau filaire de type Ethernet. La plupart des services hospitaliers sont actuellement connectés sur ce réseau protégé par un firewall des intrusions des accès extérieurs. Le CHRA dispose aussi de son propre serveur de mails protégé par le firewall. Les médecins libéraux sont également en relation avec le réseau par l'intermédiaire d'un provider internet. "*L'originalité est que ce réseau n'est pas centré sur l'hôpital*" indique Anne-Marie Fabretti, directrice adjointe, responsable des systèmes d'information et des coopérations sanitaires au CHRA, initiatrice de ce réseau de télémédecine, qui insiste beaucoup sur ce point. "*Cette notion est très importante sur le plan stratégique comme psychologique. il ne s'agit pas du projet de l'hôpital d'Annecy, mais bien d'un projet ville/hôpital, conçu sur le modèle d'un anneau. C'est-à-dire que par le biais du réseau, les médecins hospitaliers peuvent très bien communiquer entre eux sans sortir de l'établissement, les médecins libéraux peuvent échanger entre eux également, sans transiter par l'hôpital. Le choix technologique effectué, l'architecture retenue permettent à l'ensemble des acteurs du réseau de communiquer entre eux sans passage obligé par l'un des acteurs.*"[44]

Avec l'utilisation d'Internet, il est nécessaire d'intégrer sa contrepartie, la sécurité. Il faut indiquer qu'aujourd'hui, l'expérimentation réseau ville/hôpital d'Annecy a obtenu le premier et le seul accord de la CNIL concernant la transmission de données médicales nominatives sur Internet. Pour obtenir un avis favorable le projet a été passé au crible d'un certain nombre de filtres afin de garantir la sécurité de ces informations. La CNIL a finalement donné son aval en juin 1997. Par ailleurs, le Conseil national de l'Ordre des médecins, a reçu pour avis, le contrat d'interchange, c'est-à-dire les règles de fonctionnement du réseau. Il était nécessaire de disposer de cet avis, aussi bien sur le plan déontologique que sur le plan juridique. Les contrats d'interchange sont déjà bien développés au niveau commercial, dans le domaine de la télécommunication, mais peu dans le secteur médical. La presse médicale et généraliste a consacré de nombreux articles à l'époque sur ce réseau assez exceptionnel puisqu'il s'est retrouvé, après le lancement du RSS, beaucoup plus sécurisé que ce dernier, plus ouvert (car reposant complètement sur Internet et non pas sur un réseau propriétaire), plus efficace aussi sur la quantité des données échangées et indépendant de la carte CPS.

Concernant la sécurité logique, le SCSSI a du analyser le logiciel de cryptage. Pour satisfaire cette condition, a été retenu un logiciel de cryptage qui était déjà agréé par ce service, qui apportait donc déjà les garanties de sécurité demandées par le service du

[44] Anne-Marie FABRETTI, citée dans les Actes du séminaire international de Castres du 21 novembre 1997 sur les NTIC

Premier Ministre. Aujourd'hui, un médecin libéral qui souhaite envoyer un message à un médecin hospitalier constitue son fichier, qui prend la forme d'une lettre par exemple. Au lieu d'adresser ce courrier sur une imprimante, le médecin va l'envoyer à une adresse Internet. En sélectionnant l'adresse de son correspondant, automatiquement, après le chiffrage du contenu de ce dossier, ce document est envoyé crypté chez le *provider.* Il n'y a donc aucune communication sur réseau public de données nominatives en clair. Ensuite, le destinataire du message va rechercher, dans la boîte aux lettres, le message. Et à partir de son code d'accès, il rapatrie le document, le déchiffre, et le consulte. Cette communication fonctionne évidemment dans les deux sens.

Aujourd'hui, l'hôpital d'Annecy gère les clés publiques, qui représentent l'annuaire des utilisateurs de ce réseau. Il agit un peu comme une IGC. Il n'y a en aucun cas intrusion sur le réseau de l'hôpital d'Annecy, mais il y a simplement transmission de message. Ainsi, les acteurs gardent la maîtrise de leur système d'information. Par ailleurs, les médecins libéraux, par le biais de leur *provider,* disposent d'une adresse Internet, envoient des messages et récupèrent les leurs.

*d) Organisation :*

La maîtrise d'ouvrage a été confiée à l'hôpital d'Annecy[45]. Deux directeurs de projet ont été désignés par le Conseil d'Administration de l'établissement : le docteur Jacques Gaillat, responsable du Département d'Information Médicale, et Anne-Marie Fabretti chargée des systèmes d'information. Ensuite, un chef de projet, Monsieur François Meusnier-Delaye, s'est vu confier la conduite de cette expérimentation. Un comité de pilotage a été constitué, auquel participent trois médecins hospitaliers et trois médecins libéraux. Mme Fabretti insiste beaucoup sur la méthodologie qui doit inspirer tout autre directeur souhaitant développer un réseau, même sur un autre modèle que celui du CHRA : "*Pour mettre en place une telle expérimentation, il est absolument essentiel de garder la maîtrise de ce projet, de bien fixer des objectifs précis, et de mettre en place une démarche d'évaluation extrêmement rigoureuse tout au long de cette expérimentation, afin d'éviter toute dérive du système*". A ce comité de pilotage, contribuent également, avec voie consultative le Conseil de l'ordre des médecins, le Conseil de l'informatique hospitalière et de santé (qui a apporté un financement à la réalisation et à l'évaluation de ce projet), ainsi que l'organisme d'évaluation qui a été retenu pour mener l'évaluation de tout ce processus.

Le comité de pilotage est assisté, dans ces travaux, par deux types de comités : le comité technique, qui valide les solutions techniques et les fait évoluer, et le comité

[45] Cf. rapports d'étape interne au CHRA du projet de télémédecine, novembre 1998 et mars 2000

fonctionnel, composé de médecins référents, libéraux et hospitaliers, permettant de faire évoluer la règle du jeu en fonction de la pratique. C'est ce comité qui était notamment chargé d'élaborer le contrat d'interchange. La démarche d'évaluation constitue un volet extrêmement important de l'expérimentation. Un laboratoire du CNRS a été retenu à cette fin. Il est important d'effectuer un diagnostic de la communication avant l'expérimentation pour apprécier l'impact de cette expérimentation dans les pratiques, et évaluer la valeur ajoutée apportée aux intervenants. Le laboratoire a tout d'abord effectué des visites auprès des différents acteurs, afin de caractériser les grandes étapes de la prise en charge du patient, aussi bien au niveau hospitalier que libéral. Ensuite, il a procédé à l'étude des relations hôpital d'Annecy/médecins de ville : quels étaient les supports utilisés, la pertinence des informations échangées, la qualité des informations utilisées, assurer une description des processus de traitement de l'information… Il a ensuite réalisé une analyse des dysfonctionnements actuels : problèmes de secrétariat, délais de frappe du courrier, etc. Il s'agit en fait des dysfonctionnements classiques que tout directeur connaît dans la communication entre la ville et l'hôpital.

Le CHRA procède ainsi à l'analyse des incidences de la mise en place de ce réseau sur les prises en charge à l'hôpital. Par exemple, si un médecin libéral souhaite faire admettre un patient dans un service hospitalier, l'expérimentation confirme, que l'on va éviter un passage inutile au service d'accueil des urgences. Il y aura une communication plus précise, d'une part quant à la demande du médecin libéral, et d'autre part quant à l'acceptation par le médecin hospitalier, donc quant à cette collaboration. Des analyses des incidences sur la prise en charge au niveau des médecins de ville sont également réalisées. En mettant en place ce type de réseau, on apporte au patient la sécurité de se sentir suivi par une chaîne d'intervenants qui communiquent entre eux. Le patient sera peut-être incité à fidéliser sa clientèle auprès du médecin libéral. La notion de médecin traitant qui tend à disparaître aujourd'hui au fil du temps, pour des raisons sociologiques, pourrait reprendre de l'importance, et ce dans l'intérêt du patient. Cette évolution éviterait le phénomène bien connu de nomadisme médical.

*e) Bilan et perspectives :*

A ce jour, plus de 35 médecins libéraux sont équipés ainsi que les services de l'hôpital d'Annecy, et 3 établissements de soins de suite et réadaptation (le Château Bon Attrait et La Marteraye notamment). Parmi les médecins libéraux, figurent également des cliniques (notamment à Annecy, la clinique du Lac). Dans ce panel, le réseau dispose donc des principaux intervenants médicaux du bassin annecien. Il avait été prévue une montée en charge progressive, après validation de la première vague, courant 1998. Tous les services hospitaliers ont été équipés et une centaine de médecins se sont engagés par écrit à participer à ce projet (la plupart s'étaient déjà engagés depuis 1995, mais n'étaient pas tous encore informatisés). Par ailleurs, d'autres médecins ont manifesté leur volonté d'entrer dans ce réseau en ce début d'année. On arrive donc à Annecy à la situation paradoxale où les médecins qui ne souhaitent pas participer à ce réseau ont l'impression de se marginaliser alors qu'il s'agit de l'inverse sur le plan national !!!

Après la phase d'expérimentation de 1997-1998 (qui a pu réunir jusqu'à 70 participants, ce qui est énorme pour un réseau de télémédecine français à l'heure actuelle), le CHRA a conservé le système S-Tools, qui à l'origine, n'était effectivement pas ergonomique. Malgré ses défauts, plus de 200 à 300 courriers circulaient par voie électronique chaque mois. Aujourd'hui, la moyenne est de 400 à 500. En 1999, l'**Association Télé Médecine 74** (**ATM 74**) a vu le jour dans le but de créer un réseau de professionnels de santé. Cette association a pour but de permettre à ces professionnels d'échanger des données relatives aux patients dans le but d'optimiser leur prise en charge, dans le cadre d'un réseau de communication (voix, données, images) dans le respect des règles de la déontologie et de confidentialité (inscrites dans une charte de communication), contribuant à la constitution du système d'information de santé. ATM 74 a aussi pour but de promouvoir un forum de professionnels (via le Web et la messagerie), d'assurer une veille technologique pour en faire bénéficier ses adhérents et de mettre en œuvre ce réseau par des formations, un accompagnement… L'un des principes majeurs est que l'association s'engage à travailler de manière ouverte tant en terme de matériels que d'applications et de modes de transmission et à ne pas imposer de solution technique à ses adhérents. Ceux-ci restent libres de leurs choix dans ces domaines[46]. Au cours de cette période, une étude a été menée afin de changer la solution de cryptage. La libéralisation de l'usage de la cryptographie permettait d'utiliser des clés plus fortes (notamment à 128 bits).

La société Cesir, en se rapprochant de la Compagnie des Signaux, avait développé un nouvel outil de cryptographie appelé CS Cipher. Mais la société MSI avec son logiciel

[46] cf. article 2 des statuts d'ATM 74

Security Box Mail a finalement été retenu[47]. Reconnu par la CNIL, ce logiciel est conforme aux réglementations internationales et utilise les standards de cryptographie évoqués en première partie : système de cryptographie asymétrique de type RSA configurable à 512, 1024 voire 2048 bits, système de cryptographie symétrique de type DES 40 et 64 bits et triple DES 128 bits avec fonction de hachage MD5 et SHA. Cette solution présente l'avantage d'être peu coûteuse, efficace et très conviviale puisqu'elle devient invisible pour l'utilisateur. D'autre part, elle est intéropérable avec tous les produits utilisant le protocole S/MIME version 3 dont on a déjà parlé des avantages. Ce qui suppose dans la pratique une interopérabilité avec les acteurs utilisant un réseau ou une solution propriétaire (comme le RSS ou pour certains logiciels de gestion médicale équipée d'une interface pour la transmission de données). Finalement, cette messagerie sécurisée qui gère les différents types de certificats permet l'authentification par carte, ce qui suppose que le CHRA pourra très bien à l'avenir intégrer l'utilisation de la CPS dernière génération sans avoir à modifier l'architecture de son réseau. Depuis avril 2000, les adhérents sont tous passés à ce nouveau logiciel. Désormais, lorsqu'un patient arrive aux urgences du CHRA et que son médecin traitant appartient à ATM 74, celui-ci est informé par mail sécurisé. Toute l'information est dorénavant cryptée (en-tête, corps et pièce jointe). Grâce à la cryptographie, l'interfaçage entre le poste du médecin libéral et le logiciel Epimed/SAU des urgences d'Annecy est sécurisé.

La solution technique est relativement simple et peu coûteuse pour chacun des acteurs puisqu'il s'agit dans les faits d'une messagerie Internet un peu plus élaborée. Le coût du projet initial pour le CHRA avait été de 1,5 millions avec une subvention du CIHS. Les accès Internet avaient été financés dans le cadre du CIHS par le CHRA (qui avait un partenariat avec France Télécom). Aujourd'hui, le praticien libéral d'ATM 74 en choisissant l'une des solutions France Télécom (Wanadoo classique; Wanadoo Santé, Libéralis ou Oléane Santé) par l'intermédiaire de l'association peut recevoir gratuitement le logiciel Security Box Mail (d'une valeur commerciale de 800 F) mais il peut rester libre de son fournisseur d'accès et dans ce cas il doit payer le logiciel. C'est l'un des écueils peut-être du système car tout internaute a plutôt l'habitude d'utiliser des produits gratuits (freeware) mais cette solution reste sans commune mesure la moins chère de tous les autres réseaux existant en France. L'autre inconvénient du système d'Annecy est de totalement utiliser l'Internet, réseau non sécurisé par défaut. Le choix du CHRA a clairement été celui de sécuriser au maximum le contenu et de gérer dans un espace protégé le système de gestion de clés. La seule faille théorique repose sur la capture sur l'Internet d'un flux d'informations contenant ces informations cryptées et sur leur décryptage (et non le déchiffrement) avec

[47] Cf. guide d'utilisation de Security Box Mail de MSI

des moyens informatiques lourds. On rejoint alors tout le débat sur le choix technique d'un logiciel. Mais à partir du moment où la CNIL et le SCSSI ont agréé ce logiciel, la responsabilité du directeur d'hôpital est dégagée.

Sur le plan organisationnel, les atouts du réseau ATM 74 sont fondamentaux et la méthode entreprise peut servir d'exemple. La télémédecine a progressivement changé le mode de fonctionnement entre la ville et l'hôpital et a fait tomber deux des principaux reproches faits à juste titre à l'hôpital : l'absence de suivi sur le long cours du patient ainsi que le défaut de communication. Un autre avantage est la contractualisation de la communication. Pour une fois, les relations entre les partenaires ont été formalisées par le biais d'un contrat d'interchange qui répartit donc très précisément les responsabilités. Tous les acteurs sont bénéficiaires car tous gagnent du temps. Mais il est évident que l'objectif majeur est bien la qualité de prise en charge du patient, aussi rationalisée que possible, en évitant les coûts inutiles tout en assurant une bonne qualité des soins.

Le type de solution technologique utilisé au niveau du réseau de la région annecienne est également utilisé dans d'autres régions, par exemple à Montpellier ou Lille sur orientation de la CNIL ainsi que du Ministère de la Santé. L'association OREIP à Senlis a développé également un réseau comme celui d'Annecy (avec la solution Security Box Mail) en partenariat avec le RSS comme fournisseur d'accès. Le CHRA a également reproduit cette démarche et ce schéma dans le cadre d'un réseau de cardiologie réunissant cardiologues du privé et du public, clinique et hôpitaux. Dans le cadre du réseau nord-alpin des urgences, ce modèle sera prochainement reproduit : ce réseau aura pour but de renforcer la communication entre hôpitaux et de faciliter l'échange de protocoles et d'avis spécialisés sur des problèmes pathologiques urgents.

Le projet du CHRA pour l'année 2000 est de réussir avec autant de succès le projet Périn@t, une vaste coopération régionale avec le regroupement du Centre Hospitalier de Grenoble et tous les centres hospitaliers et cliniques de Savoie et de Haute-Savoie[48].

[48] Cf. projet élaboré en réponse à l'appel à candidature Périn@t intitulé *Périn@t, la toile des neiges*, 1999

**3) Autres exemples facilement reproductibles de réseaux sécurisés de télémédecine :**

*a) Perin@t à Annecy :*

Les centres hospitaliers de Savoie et de Haute-Savoie ont déjà à leur actif plusieurs réalisations ou expérimentations en matière de nouvelles technologies, Annecy en étant un peu le fer de lance. Mais ces hôpitaux ont aussi, et c'est ce qui est le plus essentiel, une longue pratique du travail en réseau de soins. Conscients de l'importance de la communication dans le secteur de la santé, ils ont décidé ensemble de réaliser le Système d'Information et de Communication de la médecine périnatale des Pays de Savoie et de l'avant-pays savoyard. Tous les hôpitaux de la Savoie et de la Haute-Savoie participent à ce projet ainsi que l'hôpital de Belley dans l'Ain et l'hôpital de Beauvoisin en Isère qui font partie de la zone d'attraction du centre hospitalier de Chambéry. Certaines cliniques privées ont également participé au projet. Les deux CHR de Lyon et Grenoble se sont associés à ce réseau pour le volet de la télémédecine et pour des recours fréquents en diagnostic et en formation.

Ce projet part d'un constat géographique : les départements 73 et 74 sont des pays de montagnes et les axes de circulation sont régulièrement très encombrés notamment lors des flux touristiques. Les conditions climatiques (surtout hivernales) perturbant fréquemment les communications. Aux franges Est du secteur 11 par exemple avec les massifs du Mont Blanc, des Aravis, des Bornes et de Chablais, les problèmes d'accessibilité se posent. Les hôpitaux de Chambéry et d'Annecy sont respectivement désignés comme têtes des secteurs 11 et 12.

Ces départements ont déjà une grande pratique des réseaux de soins traditionnels et de télémédecine. Des équipements de visioconférence existent déjà dans les CHR et dans des hôpitaux de plus petite taille. Les transferts d'images échographiques in-utero pour diagnostic cardiopédiatrique anténatal entre la maternité de Moutiers et le CHU de Grenoble sont fréquents. On recense aussi un grand nombre de boîtes aux lettres électroniques non sécurisées au CHRA, au CH de Chambéry, aux hôpitaux du Léman… Partant de cet existant et conformément au SROS, l'objectif du réseau Périn@t est d'améliorer la qualité de la prise en charge de la grossesse en optimisant l'accès aux informations utiles en tout lieu et à tout moment sur le réseau afin de faciliter et d'optimiser les transferts in-utero pour réduire les délais de prise en charge pour la mère et son enfant. La connaissance en tout lieu du réseau de la disponibilité de l'accueil dans chaque structure de référence en temps réel est un gain de temps pour quiconque, surtout en urgence, pour l'établissement à la recherche d'une autre structure pouvant recevoir une grossesse à risque. L'échange de données médicalisées permettra aussi de suivre le suivi d'une grossesse entre un réseau de

médecins libéraux (généralistes ou obstétriciens), les médecins concernés issus de divers établissements et les centres périnataux de proximité. Grâce aux moyens de communication mis en oeuvre, reposant sur le modèle d'ATM 74 en matière de sécurité, le télédiagnostic sera plus efficace et les mères pourront être orientées vers des centres plus adaptés à la pathologie présumée de l'enfant. Conjointement, on peut supposer, avec cette plus grande rapidité dans les échanges, une réduction des transferts en urgence. Grâce à la télémédecine, la formation professionnelle se trouve raffermie. Les concertations hebdomadaires pluridisciplinaires permettent de meilleurs diagnostics et suivis de la parturiente. Pour des dossiers complexes, la télémédecine est une véritable solution qui permet de gagner du temps et de l'efficacité de par la consultation conjointe avec des confrères de ces dossiers.

Grâce à la télétransmission sécurisée d'éléments du dossier médical (données cliniques et biologiques standardisées, images échographiques et radiologiques…), il est tout à fait possible d'envisager une concertation entre un personnel médical distant et un collège de praticiens plus expérimentés sans aucun déplacement du médecin et du patient. Mais pour être totalement sécurisée, la télé-expertise doit pouvoir être sollicitée à tout moment sur le réseau avec une véritable garde d'experts disponibles pour répondre instantanément en urgence à des médecins isolés confrontés à des problèmes obstétricaux ou post-nataux. Beaucoup de pratiques peuvent donc être mises à la disposition des médecins avec le réseau Périn@t. C'est en ce sens qu'il va plus loin qu'ATM 74. La vocation n'est pas la même car il s'agira avec Périn@t de faire du télé-diagnostic, de la télésurveillance, de la téléformation, des échanges de données sécurisées… Les médecins ont besoin d'échanger des données du dossier médical, des tracés de rythmes cardiaques foetaux, des graphiques de surveillance de grossesses, des examens biologiques..
La messagerie sécurisée développée à Annecy est un modèle facilitant ce type de transferts. Chambéry a mis en place une équipe hebdomadaire pluridisciplinaire composée d'un cytogénéticien, un biochimiste, des pédiatres, des réanimateurs néonatologistes et des obstétriciens en relation avec d'autres centres hospitaliers, des cliniques et des praticiens de ville. Les données d'un dossier (textes et images) pourront être préalablement transmises à l'ensemble des participants pour formuler les hypothèses de diagnostics les plus pertinentes. Les comptes rendus de cette équipe seront envoyés au médecin référent tandis que les tests diagnostics réalisés à Chambéry (notamment en cytogénétique) pourront être envoyés par voie sécurisée aux différents médecins prenant en charge la patiente.

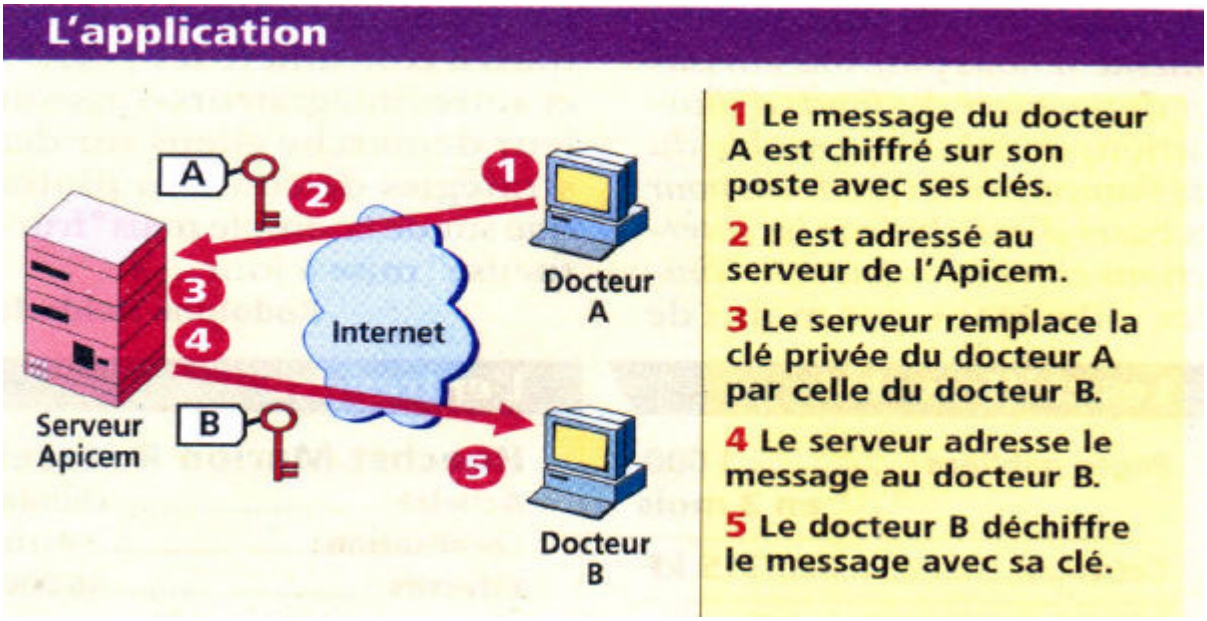
Encore une fois, l'usage de la cryptographie est devenu complètement invisible, le seul souci étant d'avoir des logiciels compatibles entre eux, ce que le protocole S/MIME

permet assez facilement. Compte-tenu de l'hétérogénéité des réseaux déjà existant, c'est une solution d'interopérabilité qui devra être mise en place et le système d'Annecy à base d'une solution tout Internet semble la plus simple à mettre en place. Il reste encore à la comparer aux autres solutions (notamment le RSS ou Oléane Santé). Textes et images fixes (généralement au format DICOM) pourront être envoyée sous forme cryptée avec tous les procédés liés à la cryptographie évoqués dans ce mémoire. L'idée est de créer un extranet afin de faire communiquer les différents intranets hospitaliers et assurer un accès Internet.

Ce qui est intéressant de constater dans le projet Périn@t, c'est que la difficulté technique majeure ne se rencontre pas dans le volet relatif aux échanges sécurisés des données mais à l'organisation du système de visioconférence, autre élément du réseau. On trouve en effet aujourd'hui suffisamment de solutions sur le marché qu'il est désormais beaucoup plus facile de créer et de se raccorder à un réseau de type extranet intéropérable. Encore ne faut-il pas oublier les règles essentielles de sécurité et bien choisir son produit.

*b) Apicrypt :*

Evoquer les produits de cryptographie dans le milieu médical sans évoquer Apicrypt serait mettre de côté une autre solution séduisante présente sur le marché Apicrypt utilise lui aussi les techniques de l'Internet mais avec une autre philosophie. C'est un système de cryptage et de transfert permettant d'échanger des données médicales dans la plus parfaite confidentialité et dans la plus grande simplicité mais avec un passage obligé vers le serveur de l'**APICEM** (**Association pour la Promotion de l'Informatique et de la Communication en Médecine**), aujourd'hui subventionnée par un fonds européen et par le **CERIM** de Lille (**Centre d'Etudes et de Recherche en Informatique Médicale**).



Le principal logiciel de chiffrement des courriers électroniques, Pretty Good Privacy, de Zimmermann, a pour inconvénient majeur sa faible diffusion chez les médecins. Il est vrai que ce dernier n'était pas légalement utilisable en France jusqu'en 1999 de par son système de cryptographie forte. II nécessite de plus la création (automatique et très facile) de deux clés, l'une, privée, à conserver, et l'autre, publique, à diffuser a ses correspondants. A côté des autres logiciels comme PGP, Security Box Mail ou Scramdisk, ApiCrypt (commercialisé par Keyserve) est un concurrent français conçu par Alain Caron et des médecins du Nord de la France à Dunkerque[49]. II présente pour principal intérêt de dispenser de l'échange de clés si le corps médical adopte ce système, le site faisant office de serveur de clés et surtout d'intermédiaire de mail (le serveur procède lui-même à l'échange). Chaque message crypté est envoyé à un serveur qui fait office de tierce partie de confiance Le serveur procède aux changements de clés nécessaires pour que le destinataire puisse déchiffrer le message qui lui est adressé sans difficulté. ApiCrypt s'utilise de façon simple en s'interfaçant dans un gestionnaire de mail courant. Le cryptage/décryptage d'un message s'effectue par un simple clic de souris. ApiCrypt a reçu une autorisation du SCSSI pour son utilisation par les médecins en France.

Aujourd'hui, un nombre important de médecins réunis dans la région du Nord de la France échangent des données hautement confidentielles telles que des documents médicaux nominatifs (résultats d'analyse, courriers…). Ce système a également reçu l'approbation de la CNIL et le nombre d'adhérents à la communauté continue de s'agrandir depuis sa commercialisation à l'ensemble de la France en mars 1999. Pour Alain Caron, "*le système ne pouvait rester cantonné à la région de Dunkerque, il fallait donc en assurer la diffusion la plus large possible*". Le MEDEC a été l'occasion en 1999 de lancer l'Opération ApiCrypt. C'était un moment adéquat car les solutions de chiffrement du RSS n'assuraient pas encore un niveau de sécurité élevé et celles de la CPS n'étaient pas opérationnelles. ApiCrypt est donc un système à double clé de cryptage et chaque message crypté est envoyé à un serveur qui fait office de tiers de confiance. Le serveur n'est pas lié au fournisseur d'accès Internet : il procède aux changements de clés pour que le destinataire puisse décrypter le message qui lui est adressé sans difficulté.

Alain Caron a été le premier à lancer en France la Formation Médicale Continue interactive, l'information pour les patients… Il a développé pour les médecins, Intermédic, un extranet hautement sécurisé pour leur permettre de dialoguer et de se tenir informés. "Au *départ, il s'agissait* de *savoir comment les nouveaux outils pouvaient nous aider à faire une médecine différente, de qualité et intégrant l'informatique. D'où l'idée de développer un*

[49] Cf. revue de presse du Dr Alain CARON sur le logiciel Apicrypt, CD ROM, mise à jour septembre 2000

*réseau local",* explique le docteur Caron. Plusieurs axes sont prévus : la formation médicale continue dans laquelle peuvent s'intégrer des mails et des news groups locales avec mot de passe, des sites FTP pour transfert de fichiers orienté vers le transfert d'images pour la télémédecine (des expériences ont eu lieu en ophtalmologie avec l'hôpital de Dunkerque), et enfin la messagerie qui permet d'échanger des courriers de PC à PC. Autour de cette zone Intranet, tout un site médical s'est constitué avec les home pages de l'hôpital et des cliniques. Un module entièrement écrit en Java script permet une évaluation de la formation continue du médecin qui se rend sur cette zone. Concernant la sécurité sur Intermédic, le dernier module de l'outil permet l'utilisation d'ApiCrypt et les médecins peuvent donc envoyer des informations confidentielles sur leurs patients par courrier électronique en toute sécurité. L'une des forces du produit est d'avoir pu obtenir un agrément du SCSSI avec un système de chiffrement avec une clé publique et une privée supérieures à 128 bits, ce qui rend effectivement cette solution séduisante. Plus de 500 médecins avaient adhéré à l'APICEM en 1999.

L'APICEM apparaît donc comme un nouveau concurrent du RSS, à la fois pour constituer un extranet et pour proposer une solution de cryptage via ApiCrypt. Toutefois, malgré les avantages indéniables que présentent les solutions du Docteur Caron, il s'agit dans tous les cas d'un produit extrêmement centralisateur puisque l'infrastructure repose sur un seul serveur. On peut d'une part s'interroger sur la viabilité de l'association et de son infrastructure et sur le danger éventuel d'avoir comme passage obligé le serveur d'APICEM. Si cette solution est effectivement valable, il faut accepter une dépendance vis-à-vis de la solution proposée. Si un quelconque problème se pose au niveau du serveur, c'est l'ensemble des acteurs du réseau qui se trouvent paralysé. Ce n'est pas le cas à Annecy avec ATM 74 puisque l'infrastructure passe entièrement par l'Internet. Seule la gestion des clés sera temporairement suspendue au CHRA en cas de problème grave, ce qui empêchera certes l'entrée de nouveaux acteurs sur le réseau mais n'empêchera pas les autres de communiquer. De plus, choisir ApiCrypt et Intermédic, c'est se rendre très dépendant de l'APICEM. Les produits proposés sont prévus pour être évolutifs et s'interfacer avec les autres systèmes à condition de continuer à choisir les produits de cette association. Dans le cas d'Annecy, le changement de logiciels de cryptage (de S-Tools vers Security Box Mail) s'est fait rapidement en quelques mois sans révolutionner l'infrastructure du réseau. Il n'en aurait pas été de même avec ApiCrypt puisque toute une autre architecture aurait dû être redessinée. Dans le cas d'ApiCrypt, les solutions de cryptographie employées sont fortes mais l'infrastructure qui sous-tend le système apporte d'autres interrogations liées à son architecture centralisée et à ce passage obligé par un seul serveur.

L'essentiel est, après l'analyse de ces exemples, de bien voir que la problématique du sujet n'est plus d'ordre technique comme le laisse croire la simple évocation du mot cryptographie mais bien organisationnelle. C'est pourquoi un tel sujet doit être une préoccupation pour un DSIO. Plus qu'un choix technique, il s'agit d'un choix d'organisation. C'est ce que la cryptographie suppose avant tout. Si face à un réseau déjà existant et bien avancé, avec beaucoup d'adhérents communiquant réellement, un directeur d'hôpital souhaite en construire ou en susciter un nouveau en empruntant le modèle d'un autre hôpital par exemple, il y a une forte probabilité pour que ce réseau échoue, même si la sécurité est absolue (ce qui est théorique).

L'important est de bien saisir les enjeux, de fixer des objectifs clairs dans le projet et de contacter les acteurs sur le terrain à propos de leurs attentes. C'est ce qu'a bien compris le RSS aujourd'hui qui essaie de susciter l'émergence de réseaux de soins en France avec les hôpitaux (exemple de Macon, Armentières…) en se présentant comme un grand fédérateur. Mais cette ultime partie retraçant des exemples locaux appelés à se développer montre bien que le directeur d'hôpital a d'autres solutions tout autant sécurisées. Et grâce à la libéralisation de la cryptographie, une nouvelle liberté s'offre au directeur d'hôpital souhaitant faire communiquer son système d'informations. A lui de savoir s'adapter, de vouloir faire communiquer, d'écouter et de bien choisir les solutions en fonction du contexte médico-social et de ses ambitions.

## CONCLUSION

La cryptographie sera peut-être d'ici une dizaine d'années complètement généralisée et inscrite dans tous les logiciels de communication sous une forme plus ou moins standardisée, il faut l'espérer. Pour le moment, ce n'est pas encore le cas mais une certitude demeure : crypter des données médicales ou administratives concernant un individu est devenu une obligation et la prise de conscience des dérives est rapide chez les acteurs de la santé. Les réseaux de soins se multiplient et la cryptographie devient de plus en plus intégrée dans les réflexions et dans les solutions. L'ensemble des outils nationaux est appelé à se moderniser pour mieux respecter la confidentialité des informations relatives à un patient.

Il n'y a pas de solution générale unique de cryptographie qui pourrait s'appliquer à un réseau de soin. Même pour la télétransmission des FSE, on a vu la multiplicité des acteurs. Cette profonde hétérogénéité se retrouve dans les choix des praticiens, des directeurs d'hôpital et des autres partenaires dans leurs systèmes informatiques. Les protocoles de l'Internet permettent désormais l'unification de ces acteurs dans des solutions communes. A cause de problèmes d'interopérabilité entre plates-formes informatiques, systèmes d'exploitation ou logiciels, les échanges ont longtemps été limités. Mais avec l'explosion du marché et la volonté des différents gouvernements à entrer dans une société des nouvelles technologies de l'information, l'hôpital rentre dans une ère communicante. Pour réussir ce nouveau défi, il doit certes s'attarder sur les aspects techniques mais ne pas omettre celui qui est au cœur du système : le patient. La cryptographie sera la technologie qui le protégera et le sécurisera.

C'est pourquoi le directeur se doit d'avoir cerné les différentes utilités qu'il peut apprendre de cet outil et d'avoir saisi les principaux enjeux et objectifs du réseau qu'il veut construire ou dans lequel il veut s'immiscer. Avec la généralisation des NTIC, le droit du patient sera d'ici quelques années peut-être modifié afin que ce dernier voit d'une part la circulation et les informations de son dossier médical (qui sera à l'avenir de plus en plus dématérialisé) sécurisés par un cryptage fort et d'autre part que celui-ci soit informé de l'utilisation qui est faite de ces données. Avoir compris que le cryptographie était une réponse à insérer dans le cadre d'une réflexion sur l'organisation et les objectifs d'un réseau, c'est déjà anticiper cette évolution.

Ce que doit retenir absolument un directeur d'hôpital en matière de cryptographie, c'est qu'aujourd'hui, lors du lancement d'un projet de réseau, il peut rester maître de sa sécurité et doit d'emblée décider la part de liberté qu'il veut conserver. Et cette décision ne peut être prise qu'en fonction des objectifs du réseau à mettre en place et de l'évolutivité qu'on voudra bien lui donner. Pour comprendre et adapter la cryptographie au monde médical, le directeur n'a pas besoin d'être un technicien, il lui suffit d'être intéressé, curieux, bien organisé et s'il ne l'est pas déjà, un peu visionnaire.

# ANNEXES

**ANNEXE 1** : État du déploiement des cartes de la famille CPx au 4 septembre 2000

**ANNEXE 2** : Tableau de bord SESAM/VITALE RSS

# ANNEXE 1

**État du déploiement des cartes de la famille CPx au 4 septembre 2000**

**Source : http://www.gip-cps.fr/fr/Actualite/stats.htm**

| | Dossiers de demande de cartes envoyés | Demandes reçues | % des demandes reçues | Demandes en attente de réception des informations télétransmises par les autorités compétentes | Demande en cours de traitement | Cartes CPS émises | Cartes CPE émises | Total de cartes émises |
|---|---|---|---|---|---|---|---|---|
| | Un dossier comporte la demande d'une carte CPS et CPE | | | | | Ce nombre correspond à un dossier traité | CPA ou CSA pour les autres établissements | |
| **Secteur libéral** | **(A)** | **(B)** | **(B/A)** | **(C)** | **(D)** | **E=(B-C-D)** | **(F)** | **G=(E+F)** |
| Professions déployées en masse | | | | | | | | |
| Médecins | 113.566 | 76.739 | 67,57 % | 677 | 530 | 75.532 | 27.819 | 103.351 |
| Pharmaciens | 28.319 | 21.961 | 77,55 % | 958 | 33 | 20.970 | 67.574 | 88.544 |
| Masseurs-Kinésithérapeuthes | 38.179 | 19.640 | 51,44 % | 288 | 368 | 18.984 | 3.510 | 22.494 |
| Orthophonistes | 9.647 | 5.498 | 56,99 % | 138 | 557 | 4.803 | 969 | 5.772 |
| Infirmiers | 47.240 | 11.008 | 23,30 % | 233 | 288 | 10.487 | 2.125 | 12.612 |
| Professions en procédure individuelle | | | | | | | | |
| Chirurgiens-Dentistes | 3.108 | 1.468 | | 31 | 44 | 1.393 | 643 | 2036 |
| Pédicure-Podologue | 96 | 30 | | 3 | 2 | 25 | 7 | 32 |
| Orthoptiste | 116 | 36 | | 0 | 3 | 33 | 11 | 44 |
| **Total Secteur Libéral** | **240.271** | **136.380** | **56,76 %** | **2.328** | **1.825** | **132.227** | **102.658** | **234.885** |
| **Établissements de soins** | | | | | | | | |
| Nombre d'établissements et CDE | | | | | | | 580 | 580 |
| Nombre d'employés | | | | | | | 11 724 | 11 724 |
| Nb. de PS salariés ( sans activité libérale ). | | | | | | 2 826 | | 2 826 |
| **Total établissements** | | | | | | **2 826** | **12 304** | **15 130** |
| | | | | | | | | |
| **Autres Établissements** | | | | | | | | |
| Nombre d'établissements CPA maître | | | | | | | 21 | 21 |
| Nombre d'employés | | | | | | | 641 | 641 |
| **Nombre de cartes Serveurs - CSA** | | | | | | | **3** | **3** |
| | | | | | | | | |
| **Total cartes émises** | | Mise à jour du tableau le 04/09/2000 | | | | **135.053** | **114.965** | **250.018** |

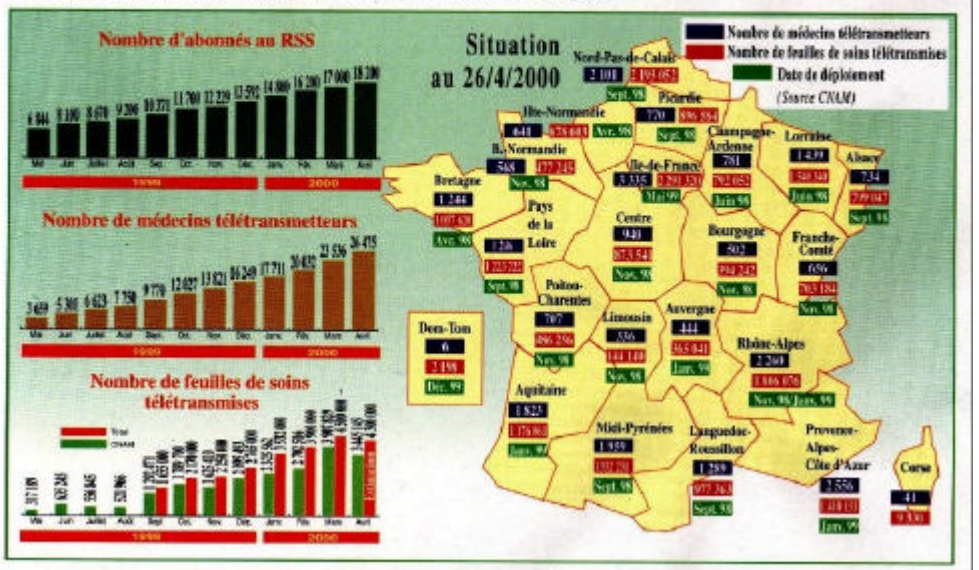
# ANNEXE 2

*Le Quotidien du Médecin*, 18 mai 2000, page 4

## TABLEAU DE BORD SESAM-VITALE/RSS

Encore près de 3 000 nouveaux médecins télétransmetteurs en avril. Les généralistes s'y mettent (36,4 %), tandis que les spécialistes font de la résistance : 11,36 %. Le 2 mai, 61,5 % des médecins avaient reçu leur CPS. Malgré cette croissance du parc de télétransmetteurs (TLT), le nombre de FSE « stagne » à un peu plus d'un million par semaine. Toujours optimiste, la CNAM y voit un effet « vacances de printemps », mais se prépare tout de même à lancer, en juin, une campagne de communication grand public.

Côté réseau, Wanadoo Santé a atteint 15 268 abonnés à la fin d'avril, dont la moitié télétransmettent. Club Medical en affiche 12 500 (dont 2 400 TLT), Medsyn, 1 600 (dont 650 TLT), Santesurf (Internet gratuit) 25 000, (dont 3 000 TLT). Liberalis a démarré et compte 450 médecins à la fin d'avril.




INFORMATIQUE LE QUOTIDIEN DU MEDECIN - PAGE 4
JEUDI 18 MAI 2000

# BIBLIOGRAPHIE

## Textes juridiques

Article 12 de la *Déclaration des Droits de l'Homme et du Citoyen*

Loi 90-1170 du 29 décembre 1990 (avec décret d'application en décembre1992).

Décret n° 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie·

Arrêté du 13 mars 1998 définissant le modèle de notification préalable parle fournisseur de l'identité des intermédiaires utilisés pour la fourniture de moyens ou prestations de cryptologie soumis àautorisation

Arrêté du 13 mars 1998 définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fourniture d'un moyen ou d'une prestation de cryptologie

Décret n° 98-11 du 24 février 1998 définissant les conditions pour lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie

Décret n° 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation

Décret n° 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable

Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisations relatives aux moyens et prestations de cryptologie

Décret n° 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation, J.O.Numéro 66 du 19 Mars 1999 page 4050

Décret n° 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable, J.O. Numéro 66 du 19 Mars 1999 page 4051

Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie, J.O. numéro 66 du 19 Mars1999 page 4052

Article 28 de la loi sur la réglementation des télécommunications 90-1170 du 29 12 90, modifiée par la loi 91-648 du 11 juillet 1991, modifiée par la loi 96-659 du 26 juillet 1996

Décret n° 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, J.O. du 25 Février 1998 page 2911

Décret n° 98-102 du 24 février 1998 définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, J.O. du 25 février 1998 page 2915

Arrêté du 13 mars 1998 définissant les dispositions particulières qui peuvent être prévues dans les autorisations de fourniture d'un moyen ou d'une prestation de cryptologie, J.O. du 15 mars 1998 p.3888

Arrêté du 13 mars 1998 fixant la forme et le contenu du dossier de demande d'agrément des organismes gérant pour le compte d'autrui des conventions secrètes, J.O. du 15 mars 1998 p.3888

Arrêté du 13 mars 1998 définissant le modèle de notification préalable parle fournisseur de l'identité des intermédiaires utilisés pour la fourniture de moyens ou prestations de cryptologie soumis àautorisation, J.O. du 15 Mars 1998 page 3888

Arrêté du 13 mars 1998 fixant la liste des organismes agréés pouvant recevoir dépôt des conventions secrètes, J.O. du 15 Mars1998 page 3891

Arrêté du 13 mars 1998 fixant le tarif forfaitaire pour la mise en œuvre des conventions secrètes au profit des autorités mentionnées au quatrième alinéa du II de l'article 28 de la loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, J.O. du 15 Mars1998 page 3891

Extrait de la loi sur la réglementation des télécommunications 90-1170 du 2912 90, modifiée par la loi 91-648 du 11 juillet 1991, modifiée par la loi 96-659 du 26 juillet 1996

Articles 226-13 à226-17 du Code Pénal

Article L 365-2 Code Santé Publique

## Rapports et articles juridiques

*Le publipostage électronique et la protection des données personnelles*. Commission Nationale de l'Informatique et des Libertés. Rapport présenté par Madame Cécile Alvergnat, adopté le 14 octobre 1999

*Santé, informatique et libertés . Professions libérales de santé* Rapport CNIL mars 1999

*Rapports d'activité du CSSIS 1997 et 1998*

*Rapports d'activité de la CNIL 1996, 1997, 1998 et 1999*

Géraud LAC et Cédric VIEAU *Les Aspects Légaux de la Cryptographie en France et dans le Monde*, rapport ENSIMAG, mars 1999

*Mission gouvernementale pour le commerce électronique.* Synthèse par Francis Lorentz du rapport : "*La nouvelle donne du commerce électronique*". Disponible àcette URL :

http://www.finances.gouv.fr/mission_commerce_electronique/travaux/synth_generale.html
http://www.juriscom.net/droit/espace2/crypto3.htm Juriscom.net, article de décembre 1998 *Cryptographie : l'exception française.* Interview de Maître Valérie Sédallian
http://www.juriscom.net/espace2/crypto2.htm , *Analyse comparée des politiques nord-américaines en matière de cryptographie*
*Cryptographie : un droit pour les citoyens ?* Débat du comité de rédaction de TERMINAL avec Meryem Marzouki et François Sauterey de l'association **IRIS** (Imaginons un Réseau Internet Solidaire), 1998 sur http://www.iris.sgdg.org/documents/entretien-terminal.html
*Carte vitale et vie privée*, Le mOnde du vendredi 21 mai 1999 page 16
*Informatique et libertés en 1997 : vers où allons-nous* par L.Cadoux in *La Gazette du palais*, 16 et 17 avril 1997

**La cryptographie, les NTIC et les réseaux de santé**

*La stratégie intranet à l'hôpital*, Christophe Menuet, mémoire ENSP 1998
*Le Quotidien du Médecin,* 24 janvier 2000, pages 8 et 10
*Le Quotidien du Médecin,* 18 juin 1997, page 11
*La réforme du système de santé, le dispositif Sesam Vitale : enjeux et perspectives*, rapport CNIL, avril 1998
*Les réseaux régionaux de télémédecine* Rapport d'activité CNIL, 1996
*La santé demain : vers un système de soins sans mur coordonné* par J-P Claveranne et C. Lardy, Economica, Centre Jacques Cartier, 1999
*Aide méthodologique à l'évaluation de la télémédecine*, CREDES, mars 2000
*Charte d'éthique et de qualité des services d'informatisation destinés aux professionnels de santé*, OPHIS, mai 1998
*DH magazine* juin-juillet 2000 sur les réseaux ville-hôpital
*Sécurité Informatique*, numéro 24, avril 99
Evaluation Graphos *Projet Télémédecine Région Annecienne*, mars 2000
*Actes du séminaire national de Castres du 21 novembre 1997* du Club National des Réseaux de Ville sur les NTIC
*La télémédecine : enjeux médicaux et industriels* par Dr Jean-Pierre Thierry, octobre 1993
*Rapport interne CHRA La toile des neiges*
*Les nouvelles techniques de transfert de données médicales*, Dossier du CNEH, 1998
*Le dossier du patient à l'hôpital*, document CNEH septembre 1999

**Aspects techniques, pratiques et historiques de la cryptographie**

*La science du secret*, Jacques STERN

*Cryptographie appliquée Seconde Edition*, Bruce Scheier, Ed.WILEY , 1997

*Cryptographie : théorie et pratique*, Douglas Stinton, Vuibert, 1996

*Initiation à la cryptographie*, G. Dubertret, Vuibert, 1998

*L'Internet sécurisé*, Eric Larcher, Editions Eyrolles, 2000

*Privacy on the Line,* Whitfield Diffie et Susane Landau*.*

*Decrypted Secrets,* F.L. Bauer*.*

*The codebreakers,* Davis Khan

*Handbook of applied cryptography*, A.Menezes, P Van Oorschot et S.Vanstone, CRC Press Incorporation 1997

*La cryptographie militaire*, Auguste Kerckhoffs *Journal des sciences militaires*, volume IX, pages 5 à38, janvier 1883 et pages 161 à191 février 1883

*Public Key Infrastructures* de J.Gottel, E.Larcher, G.Lebreton et R.Nguyen, rapport ENST mai 1999

**Ressources internet**

**Newsgroups :** news.talk.politics.crypto et news.fr.misc.cryptologie

**Site du Ministère de l'Emploi et de la Solidarité** : http://www.sante.gouv.fr/

**Site du SESI (Direction des Hôpitaux, sous-direction des systèmes d'information du Ministère des Affaires Sociales)** : http://www.sante.fr/htm/index.htm

**Site du Ministère de l'économie, des finances et de l'industrie.**

http://www.telecom.gouv.fr/francais/activ/techno/technweb1g.htm

**Site du Journal Officiel** : http://www.journal-officiel.gouv.fr/

**Site de la CNIL :** http://ww.cnil.fr

**Site du SCSSI *:*** http://www.scssi.gouv.fr/

**Site du GIP CPS :** http://www.gip-cps.fr/

**Site du GIP Sesam Vitale** : http://www.sesam-vitale.fr/

**Site de l'Association des Médecins Généralistes pour l'Information et la Transmission des données (AMGIT**) : http://www.amgitweb.com

**Site de la Fédération des Utilisateurs de Logiciels MEDIcaux COmmunicants (FULMEDICO)** : http://ww.fulmedico.org

**Site de l'UPIDF (Union Professionnelle des Médecins Libéraux d'Ile-de-France)** : http://www.upidf.org/accueil1.asp

**Site du RSS :** http://www.cegetel.rss.fr

**Site d'Oléane Santé** : http://www.oleane.tm.fr

**Site d' Egora** : http://www.egora.fr

**Site d'INTERMEDIC** : http://www.intermedic.org

**Site MG Web** : http://come.to/mgweb

**Site Keyserve :** http://WWW.keyserve.com

**Site d' Informéd** : http ://www.multimania.com/informed

**Site de l'IRIS (Imaginons un Réseau Internet Solidaire)** : http://www.iris.sgdg.org/

**Centre documentaire international de PGP *:*** http://www.pgpi.org/doc/

**La réglementation de la cryptographie** avec une bonne analyse de la loi de 1996, http://www.planete.net/~jbaagoe/loi_cryto.html/

**Bibliothèque de l'ordre des Avocats de Paris**. Minutes de la Table ronde sur la cryptologie du 24 juin 1998 par Maître HIBLOT. Une réflexion sur la législation française du point de vue des avocats. http://www.grolier.fr/cyberlexnet/COM/A980901.htm

**Page personnelle de Sven Knispel**. Discussion sur les lois concernant la cryptographie en France et dans le monde. http://www.planet-express.com/sven/links/lois_fr_links.htm

Site personnel de **G.Schutz** : http://cui.unige.ch/~schutz/crypto/

**Law Survey.** : Site très complet regroupant l'état actuel des législations sur la cryptologie de plus d'une soixantaine de pays. http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm

**European Cryptography Resources.** Liens sur la cryptographie en Europe. http://www.iki.fi/avs/eu-crypto.html

Pour en savoir plus sur l'actualité de la **cryptographie aux Etats Unis**. http://www.crypto.com/

L'univers des codes sources sur **Cryptosoft** : http://www.cryptosoft.com/html/download.htm

La référence technique **Counterpane** : http://www.counterpane.com/

**PGP International Homepage** : http://www.pgpi.org/

**Scramdisk** : http://www.scramdisk.clara.net/

**Security Box Mail de MSI** : http://www.msi-sa.fr

**Infowar** : http://www.infowar.com/

**Site de l'Internet sécurisé** : http://www.internet-securise.com