MASTER EN SCIENCES INFORMATIQUES

Contribution à la transmission téléinformatique des résultats d'analyses biomédicales

Frisque, Pascal

Award date:
1990

Awarding institution:
Universite de Namur

Contribution à la transmission téléinformatique des résultats d'analyses biomédicales

Promoteur

Professeur Jean Ramaekers

Année académique 1989-1990

Mémoire présenté pour
l'obtention du grade de
Licencié et Maître en Informatique
par

Pascal Frisque

Facultés Universitaires Notre-Dame de la Paix
Institut d'Informatique
Rue Grandgagnage, 21 B-5000 Namur
Tél. 081/229065, Télex 59222 facnam-b

Contribution à la transmission téléinformatique des résultats d'analyses biomédicales

Pascal Frisque

Résumé

Les progrès en informatique médicale et micro-informatique personnelle sont tels que les médecins commencent à s'informatiser. Cette informatisation est déjà très avancée dans les laboratoires d'analyses médicales.

Se pose dès lors la question de relier les équipements informatiques du médecin et du laboratoire, dans le but d'améliorer la circulation et le traitement des informations.

Ce mémoire tente d'apporter une réponse aux problèmes de la transmission téléinformatique de résultats confidentiels d'analyses biomédicales entre le laboratoire et le médecin prescripteur. Divers impératifs que devrait respecter toute solution sont définis et un système est proposé pour répondre à l'ensemble des exigences.

Abstract

The improvements in medical computer and in micro-computer sciences are such that doctors are getting computerized. This computerization is already very spread in laboratories for biomedical analyses.

The question is to link the doctor's equipments with the laboratory in order to improve the information flow and the data processing.

This study tends to bring an answer to the problems of communication of confidential results of biomedical analyses between the laboratory and the doctor. Different imperatives to be respected by any solution are determined and a system is proposed in order to answer to all requirements.

Mémoire de Licence et Maîtrise en Informatique
Année académique 1989-1990

Promoteur : Prof. Jean Ramaekers

J'exprime toute ma gratitude à Monsieur Jean Ramaekers, promoteur de ce mémoire, et à son assistant Monsieur Paul-Georges Crismer, pour l'attention qu'ils ont portée à la réalisation de ce mémoire et pour les excellents conseils qu'ils m'ont donnés.

J'exprime ma profonde reconnaissance au docteur Michel Beauloye qui m'a particulièrement stimulé par son intérêt soutenu et sa critique constructive.

Je remercie toutes les personnes qui m'ont fourni des indications essentielles avec une grande disponibilité, spécialement le docteur A. Bosly du Conseil provincial de l'Ordre des médecins de la province de Namur, le docteur T. Defour du CNIM, le docteur D. Gillet de la FAMGB, le docteur R. Huvelle de l'hôpital Vésale et Monsieur J. Stroëff de la RTT.

Enfin, je n'oublie pas toutes les personnes qui m'ont aidé dans mon travail, d'une façon ou d'une autre : qu'elles trouvent ici l'expression de mes plus vifs remerciements. Ce mémoire est aussi un peu le leur.

Table des matières

Cadre du mémoire

Eléments de théorie de sécurité informatique

Eléments de théorie de téléinformatique

Table des matières

Services publics de télécommunications

Analyse des besoins

Table des matières

Conception globale du système

Implémentation

Conclusions

Table des matières

Annexes

Bibliographie

1. Introduction

Parmi les nombreux domaines dans lesquels l'informatique a trouvé un champ d'application, il en est un en pleine évolution où elle doit encore répondre à de nombreux défis : c'est celui de l'informatique médicale. En effet, la variété et la complexité des activités liées à la médecine posent sans cesse de nouveaux problèmes techniques, scientifiques, économiques et juridiques.

Depuis quelques années, l'informatique a envahi certaines branches du monde médical, alors qu'elle est restée à peu près absente d'autres. Parmi les secteurs les plus informatisés, on trouve les laboratoires d'analyses. Une enquête récente de la Société belge d'informatique médicale (MIM) montrait que près de 100 % des laboratoires le sont, à des degrés divers, mais la tendance est à une informatisation toujours plus poussée, tant de la gestion que de l'activité même du laboratoire. Par contre, le taux d'informatisation des médecins est particulièrement bas. Ainsi, selon la même enquête, à peine 2 % d'entre eux l'étaient en 1988. Cependant, il est probable que, les progrès de la micro-informatique aidant, cette proportion s'accroisse rapidement.

Quelle est l'influence de l'informatique ? Si elle permet de résoudre certains problèmes, elle peut aussi en poser de nouveaux, en provoquant l'apparition de nouvelles pratiques. Ce qui soulève alors la question de leur adéquation avec les contraintes propres à la profession médicale. Tout ce qui a trait à la santé nous touche tous directement : c'est ce qui fait le caractère particulier des activités liées à la médecine et impose des obligations aux membres de la profession.

Comme illustration de cet aspect des choses, reprenons le cas de l'informatisation des laboratoires d'analyses et des médecins. Tant que le processus d'informatisation ne concerne que les activités propres du médecin ou du laboratoire, aucun problème particulier ne se pose. Cependant, dès lors que les deux parties souhaitent étendre ce processus à leurs échanges, des problèmes d'ordre déontologique interviennent, et, par là, des problèmes techniques.

L'objet de ce mémoire est de faire l'inventaire de ces problèmes pour la transmission téléinformatique des résultats d'analyses et de voir comment l'informatique peut y répondre.

Définition du cadre du mémoire

Pour définir le cadre de ce mémoire, nous commencerons par voir quels types de problèmes pose la transmission des résultats d'analyses entre le laboratoire et le médecin. Nous verrons quels sont les acteurs impliqués dans la recherche d'une solution et quels sont leurs rôles respectifs. Suivront quelques commentaires, la définition des objectifs poursuivis dans le cadre de cette étude et la démarche adoptée pour y parvenir.

2. Problèmes d'ordre déontologique

L'exercice de la profession médicale est régi par un ensemble de règles définies dans un code de déontologie[1] édicté par l'Ordre des médecins[2] qui a pouvoir de sanction. De plus, les médecins et les laboratoires d'analyses sont soumis par la loi à diverses obligations. Parmi ces contraintes, les deux plus importantes qui nous concernent directement sont : le respect du secret médical et la notion de libre choix du médecin.

Protection du secret médical

Les résultats des analyses sont des données nominatives et confidentielles, protégées par le secret médical. La règle du secret médical fait obligation au médecin de s'assurer que toutes les précautions sont prises pour en garantir le respect. Cette obligation s'étend à toutes les personnes impliquées dans la constitution du dossier médical du patient. Ainsi, les membres du laboratoire qui effectuent des analyses pour le compte d'un médecin sont tenus aux mêmes impératifs.

Libre choix du médecin

Le code de déontologie indique en ses articles 10 et 12 que "l'art médical ne peut en aucun cas être pratiqué comme un commerce" et que "la publicité directe ou indirecte est interdite". Le médecin et le patient doivent rester libres du choix du laboratoire auquel ils souhaitent s'adresser pour lui demander d'effectuer des analyses. En conséquence, le laboratoire ne peut exercer à l'égard des médecins aucune forme d'incitation visant à les lier de façon permanente. Cela pourrait conduire à l'apparition d'un monopole du laboratoire vis-à-vis des médecins qui serait la négation du principe de libre choix.

---

[1] Voir annexe 1

[2] Voir annexe 2

Au vu de l'actualité récente et des démêlés de la firme Biorim avec la justice, on comprend qu'il s'agit d'un problème brûlant. Toutes les précautions doivent donc être prises pour éviter l'apparition d'une nouvelle forme de monopole que le laboratoire pourrait être tenté d'exercer à l'égard des médecins, consentants ou non, via la mise en place d'un nouveau système de transmission des résultats des analyses.

Dispositions juridiques

Des dispositions juridiques sont prévues à l'égard des contrevenants. Pour le médecin, cela peut aller de la condamnation à une amende jusqu'à l'emprisonnement par un tribunal et d'un blâme à la suspension du droit d'exercer par l'Ordre des médecins.

On le voit, les peines encourues en cas d'infraction aux règles de la déontologie sont importantes. Dès lors, que ce soit le laboratoire ou le médecin, chacun voudra obtenir des garanties quant au respect de la déontologie avant d'adopter une nouvelle technique de transmission des résultats des analyses.

3. Problèmes d'ordre technique

Les problèmes techniques revêtent différents aspects qui découlent principalement des contraintes imposées par la déontologie de la profession et de la diversité des systèmes informatiques des laboratoires et des médecins. Nous distinguerons les problèmes relatifs à la codification des résultats des analyses et les problèmes relatifs à leur transmission proprement dite.

Codification des résultats

Avant de pouvoir être exploitée, toute information doit d'abord être comprise. Lorsque cette information est échangée, son émetteur et son destinataire doivent se mettre d'accord sur un ensemble de règles et de conventions qui leur permettront de se comprendre. Ainsi, lorsqu'un laboratoire transmet des résultats d'analyses à un médecin, il doit les rendre compréhensibles par le médecin. Ce qui pose le problème de la codification des résultats.

De nombreux groupes de travail se penchent actuellement sur la question, et un certain nombre de propositions ont déjà été faites. Il s'agit d'un point crucial, car l'absence actuelle d'un standard en la matière hypothèque, à coup sûr, toute tentative de développement d'un système de transmission téléinformatique des résultats des analyses. En effet, la variété des systèmes de codification est telle qu'il est impossible de les prendre tous en compte pour en assurer la conversion de l'un d'entre eux vers un autre. Pour cette raison, le laboratoire ne propose souvent qu'un système particulier de codification. Ce qui oblige le médecin à s'adapter à un système différent chaque fois qu'il s'adresse à un autre laboratoire, et peut apparaître comme un moyen de fidélisation des médecins vis-à-vis d'un laboratoire.

Nous n'entrerons pas plus en détail dans ces considérations, car nous estimons qu'il s'agit d'un problème purement médical, pour lequel nous ne pensons pas être en mesure de donner un avis qualifié. D'autre part, nous avons déjà signalé que des groupes de travail ont été constitués pour examiner la question. Nous nous concentrerons donc sur l'étude des problèmes liés à la transmission proprement dite des résultats des analyses, en faisant abstraction des problèmes de codification de ces résultats.

Transmission des résultats

La transmission des résultats des analyses concernent l'ensemble des moyens et méthodes à mettre en oeuvre pour en assurer le transfert entre un laboratoire et un médecin, dans le respect des contraintes propres à la profession médicale. C'est l'objet de ce mémoire.

4. La position de l'Ordre des médecins

Le 19 avril 1986, l'Ordre des médecins émet un premier avis sur le problème de la transmission téléinformatique des résultats d'analyses entre le laboratoire et le médecin, qui est une condamnation nette de ce procédé. En septembre 1989, la position de l'Ordre s'assouplit et apparaît l'idée d'un règlement que le laboratoire et le médecin devraient préalablement soumettre à l'approbation du conseil provincial de l'Ordre.

Dans cet avis, le Conseil de l'Ordre stipule notamment que :

- "Il doit résulter de ce document que les précautions nécessaires ont été prises en vue d'éviter des infractions à la déontologie."

- "Pour que le libre choix du patient soit respecté, il doit ressortir du règlement que l'usage de ce service n'entraînera pas la création d'un lien illicite entre le médecin et le laboratoire et que le médecin conserve la liberté de travailler avec d'autres laboratoires. Ce service doit être mis à la disposition de tous les médecins qui souhaitent y recourir, sans aucune obligation pour eux d'y envoyer des patients."

- "L'usage de ce mode de transmission de données médicales ne peut procurer au médecin traitant d'autre avantage que celui d'une communication meilleure et plus rapide des résultats. Tout autre avantage doit être considéré comme une dichotomie camouflée et est par conséquent interdit."

L'Ordre des médecins rappelle par là les droits et devoirs du médecin et des membres du laboratoire, tels qu'ils sont définis dans le code de déontologie. Les notions de respect du secret médical et de libre choix du médecin et du patient vis-à-vis du laboratoire sont confirmées.

5. Commentaires

La transmission des résultats d'analyses entre le laboratoire et le médecin présente donc des aspects juridiques et techniques. Les aspects juridiques sont concrétisés par l'obligation faite au laboratoire et au médecin d'établir un règlement pour la transmission des résultats. Ce règlement doit rester en accord avec les principes de déontologie de la profession et soumis à l'approbation de l'Ordre des médecins. Les aspects techniques concernent la mise en oeuvre de ce règlement.

La première chose à faire est donc de définir ce règlement. Cela devrait être réalisé conjointement par le responsable du laboratoire, le médecin traitant, l'informaticien et le patient. Le concours d'un juriste peut s'avérer utile. Cependant, les difficultés de communication existant entre les différents partenaires rendent cette tâche particulièrement difficile, chacun n'étant souvent spécialiste que dans son domaine. Aussi, nous n'estimons pas être en mesure de répondre à tous ces problèmes dans le cadre de ce mémoire, que nous limiterons volontairement aux aspects techniques de la transmission téléinformatique des résultats des analyses.

Par ailleurs, ne pouvant prendre en considération tous les cas particuliers pouvant se poser, nous restreignons notre étude à celle de la transmission des résultats d'analyses biomédicales en milieu extra-hospitalier. Il s'agit d'un choix délibéré, dicté par la nécessité de limiter l'étendue des problèmes afin de les rendre plus maîtrisables. Des indications seront fournies pour montrer des pistes possibles menant à la généralisation des enseignements que nous pourrons tirer de notre étude.

6. Buts

En conséquence de ce qui précède, les buts que nous poursuivrons dorénavant sont :

- faire l'inventaire des besoins à satisfaire sur le plan technique, pour la transmission téléinformatique des résultats des analyses ;

- chercher des solutions pratiques et montrer qu'elles sont compatibles avec les contraintes propres à la profession médicale.

7. Démarche

Nous débuterons par quelques notions théoriques de sécurité informatique et de téléinformatique. Nous poursuivrons par l'examen des services de télécommunications disponibles. Viendra ensuite la partie étude proprement dite du problème, sous ses aspects techniques, qui comprendra : l'analyse des besoins, la conception du système et son implémentation. La conclusion qui clôturera ce travail permettra de tirer un certain nombre d'enseignements. Diverses informations seront fournies en annexe pour les lecteurs désireux d'en savoir un peu plus sur quelques aspects particuliers du problème.

L'une des difficultés de ce mémoire tient à la diversité de ses lecteurs potentiels, principalement des médecins, des biologistes et des informaticiens. Rester accessible à tous, en fournissant l'information que chacun attend est un exercice ardu. Nous espérons avoir trouvé un compromis conciliant les intérêts de chacun. Cependant, des parties sont plus spécifiquement destinées aux lecteurs informaticiens. Elles seront signalées en temps opportun.

1. La protection des systèmes téléinformatiques

Les réseaux accroissent considérablement les possibilités des systèmes de traitement de l'information, mais introduisent aussi de nouveaux risques vis-à-vis de la protection de l'information : risques d'accès à distance aux systèmes de traitement, risques d'accès aux données en cours de transmission.

Les principaux objectifs des dispositifs et des techniques de protection sont les suivants :

- Identifier et authentifier les utilisateurs.
- Ne permettre l'accès à un objet ou ressource qu'aux utilisateurs autorisés.
- Tenir un journal d'utilisation du système pour vérifier quels utilisateurs accèdent à quels objets.
- Protéger les données transmises afin d'empêcher leur modification ou leur divulgation par des actions volontaires ou involontaires.

2. Identification et authentification

Un élément primordial dans le contrôle d'accès est l'établissement d'une identité formelle et unique pour chaque utilisateur. Ceci est généralement réalisé en deux étapes :

- la présentation d'une identité prétendue : un identifiant ;
- la présentation d'une information pour vérifier l'identité prétendue : un authentifiant.

La première étape constitue l'identification et la seconde l'authentification. Chaque utilisateur doit avoir un couple identifiant-authentifiant unique qui lui permet d'être reconnu par le système. A ce couple sont associés les droits et privilèges de l'utilisateur.

L'identification ne pose pas de problèmes particuliers. Par contre, l'authentification nécessite l'emploi de méthodes et de techniques capables de fournir des résultats fiables, puisque ceux-ci conditionnent l'accès au système. C'est donc sur la méthode d'authenfication que doit se porter toute l'attention des gérants du système.

3. Méthodes d'authentification

Il existe trois méthodes de base permettant de vérifier l'identité prétendue d'un individu. Elles reposent sur la reconnaissance par le système :

- d'une information détenue par l'individu ;
- d'un objet physique possédé par l'individu ;
- d'une caratéristique propre à cet individu.

Une information détenue par l'individu peut être un mot de passe ou un ensemble de faits appartenant à son passé. Un objet physique possédé par l'individu peut être une clé, une carte d'accès ou un badge. Une caractéristique propre à cet individu peut être sa signature, sa voix, ses empreintes digitales ou d'autres caractéristiques personnelles. En fait, l'authentification est toujours réalisée sur base de la détention d'une information. Tout le problème consiste à relier cette information de la façon la plus sûre à un individu.

31. Le mot de passe

Le mot de passe est le moyen le plus utilisé pour contrôler l'accès aux systèmes. Le nombre total de mots de passe pouvant être attribués doit être suffisamment grand pour réduire à un niveau acceptable le risque de découverte d'un mot de passe validé soit par inadvertance, soit au travers d'une recherche systématique.

Trois méthodes sont utilisées pour produire des mots de passe :

- mot de passe obtenu par dérivation ;
- mot de passe obtenu aléatoirement ;
- mot de passe choisi par l'utilisateur.

La méthode par dérivation consiste à définir le mot de passe à partir d'une ou plusieurs informations connues du système et de l'utilisateur, selon un algorithme défini. Cette méthode permet de changer de mot de passe lors de chaque accès au système. Il suffit pour cela de modifier l'une ou l'autre des informations à la base de la dérivation. Ce peut être, par exemple, la date, ou l'heure, ou encore une information préalablement échangée par le système et l'utilisateur.

La génération aléatoire du mot de passe fait appel à des techniques de choix aléatoire dans un ensemble fini de caractères.

Quant à la troisième méthode, son nom indique le procédé utilisé : c'est l'utilisateur qui choisit lui-même son mot de passe.

Chaque méthode a ses avantages et ses désavantages. Voyons-en les principaux, selon une comparaison inspirée de Longley D. & Shain M., Data & Computer Security.

Comparaison des différentes techniques de génération des mots de passe

"+" = favorable à la sécurité et "-" = défavorable à la sécurité

	Assigné par dérivation	Assigné aléatoirement	Choisi par l'utilisateur
Mémorisation	+ inutile	- valeur arbitraire difficile à se rappeler	+ facile à se rappeler
Distribution des mots de passe	+ distribution plate	+ distribution plate	- distribution agrégée
Remise des mots de passe	+ inutile	- nécessite une remise	+ inutile
Vulnérabilité lors de la remise	+ pas de risques	- vulnérable	+ pas de risques
Stockage	+ inutile (recalculé à chaque fois)	- sous forme chiffrée	- sous forme chiffrée
En cas de divulgation	- méthode de dérivation menacée	- nécessite un remplacement	+ peut être changé par l'utilisateur

Les mots de passe ou les informations qui servent à les générer sont habituellement stockés sous forme de tables ou listes. Ces informations doivent être soigneusement protégées, car elles sont dangereuses pour le système de sécurité. Une méthode pour réaliser cette sécurité est de les chiffrer.

Le mot de passe est vulnérable à plusieurs menaces pendant son entrée : observation de l'utilisateur pendant l'entrée, recherche heuristique, écoute passive ou active, dérivation du flux de données.

Afin d'éviter la première menace, des précautions doivent être prises pour empêcher la vue du mot de passe durant l'entrée. Par exemple, celui-ci ne doit pas apparaître à l'écran. Pour se protéger d'une attaque du type recherche heuristique, il devra être prévu un délai entre chaque essai d'accès infructueux et une limite sur le nombre de ces essais. La défense contre les systèmes d'écoute est de chiffrer le mot de passe différemment chaque fois qu'il est envoyé au système central.

L'inconvénient le plus important de l'utilisation des mots de passe est la possibilité que cette information puisse être connue par un imposteur qui pourrait alors l'utiliser comme son utilisateur légitime.

32. La possession d'un objet

La possession d'un objet, tel qu'une clé ou un badge codé, est un autre moyen d'authentifier un utilisateur. Les clés peuvent être utilisées seulement s'il s'agit d'un terminal personnel. Pour cette raison, elles sont peu utilisées dans l'informatique répartie.

Les badges codés peuvent utiliser différentes techniques de codage. Tous les types de badges peuvent être dupliqués si suffisamment de temps et d'argent sont consacrés à cette tâche.

Les lecteurs de badge doivent avoir des détecteurs d'effraction. De plus, les lignes de communication entre le lecteur de badge et tout système central doivent être protégées par un contrôle permanent ou le chiffrement des messages.

La carte à microprocesseur

La carte à microprocesseur est née d'une invention française : en 1974, Roland Moreno dépose son premier brevet. Bull décide en 1977 de développer cette technique et intègre sur la carte un microprocesseur, ce qui justifie l'appellation de carte à microprocesseur de préférence à carte à mémoire.

Sous l'apparence d'une carte de crédit classique, la carte contient dans l'angle supérieur gauche le microprocesseur, inséré dans l'épaisseur du plastique. Le verso de la carte peut être équipé d'une piste magnétique.

Une carte intègre par exemple :

- un microprocesseur 8 bits ;
- une mémoire programmable ROM de 1600 octets, dans laquelle est enregistré le programme de gestion de la carte ;
- une mémoire EPROM de 8 Kbits pouvant contenir des données, des paramètres, mais également des instructions exécutables. Cette mémoire est ineffaçable, protégée contre les rayons UV, résiste aux rayons X et aux champs magnétiques. Elle est également inviolable et incopiable, car les accès sont filtrés par le microprocesseur ;
- une mémoire de travail RAM de 36 octets, destinée aux entrées-sorties et au stockage des résultats intermédiaires.

L'identification est réalisée en comparant le code du porteur de la carte avec celui stocké dans la zone secrète de la carte.

L'authentification est réalisée de la façon suivante : le système auquel veut se connecter le porteur de la carte demande à la carte d'exécuter un calcul qu'elle est seule, avec le système, à savoir exécuter. Le résultat obtenu par la carte est comparé avec le résultat obtenu par le système : l'authentification nécessite une égalité des deux résultats. Le calcul peut être différent lors de chaque session.

La carte peut aussi avoir des fonctions de chiffrement-déchiffrement qui la rendent ainsi apte à la protection des données transmises.

33. Les méthodes biométriques

L'inconvénient des clés et badges tient au fait que l'objet d'identification peut tomber dans les mains d'un imposteur et être alors utilisé comme par son propriétaire légitime. En raison des limites des méthodes précédentes, on a placé beaucoup d'intérêt dans le développement de techniques utilisant les caractéristiques personnelles d'un individu pour effectuer la vérification d'identité.

Un des problèmes principaux dans l'utilisation des caractéristiques personnelles telles que la géométrie de la main, les empreintes digitales, la signature, la voix, la surface de la rétine, est la difficulté de réaliser des mesures précises et répétitives de ces caractéristiques.

Les équipements utilisant des caractéristiques personnelles opèrent généralement de la manière suivante :

- l'utilisateur entre sa prétendue identité,
- l'appareil réalise la mesure et obtient un profil mesuré,
- le profil mesuré est comparé avec le profil de référence correspondant à l'identité prétendue,
- la valeur résultante est comparée avec un seuil prédéterminé. De cette comparaison résulte la décision d'accepter ou de rejeter l'individu.

Deux types d'erreurs peuvent intervenir :

- type 1 : rejet de personnes accréditées,
- type 2 : acceptation d'imposteurs.

Très peu de ces équipements sont actuellement commercialisés et leurs coûts sont tels qu'ils ne sont pas rentables dans un grand nombre d'applications.

4. Le contrôle d'accès

Une nouvelle menace est commune à toutes les méthodes d'auhentification : un fraudeur potentiel réussit à obtenir l'accès à un réseau en forçant un utilisateur autorisé à se connecter et à réaliser la procédure d'authentification, après quoi le fraudeur peut alors utiliser le terminal ou donner des ordres à cet utilisateur.

Afin de se protéger contre cette menace, on doit prévoir une possibilité d'alarme "prise d'otage" dans le système. Ceci doit être réalisé par une action insoupçonnable signalant que l'opérateur agit sous la contrainte.

Autorisation

Une fois que l'identité d'un utilisateur a été établie et authentifiée, il peut demander l'utilisation de ressources (objets). L'accès à un objet demandé peut être restreint. Par exemple, une base de données sur le contrôle des stocks peut être consultée par le département "Etude des marchés", mais ne peut être mise à jour par ce même département.

Deux types de politiques peuvent être définies :

- Politique du privilège minimal : l'utilisateur peut accéder uniquement aux objets nécessaires à sa fonction.

- Politique du privilège maximal : l'utilisateur peut accéder à tous les objets si ceux-ci ne sont pas spécialement protégés.

Différents types de contrôles répondant à des objectifs distincts de sécurité sont utilisables.

A. Contrôle d'accès indépendant du contenu.

Selon ses droits et privilèges, une personne peut accéder à une certaine catégorie d'objets, indépendamment du contenu. La décision d'accès peut être prise sans accéder à la valeur de la donnée. Par exemple, dans une base de données médicales, un médecin peut accéder aux noms, résultats d'examens, etc... tandis que le personnel administratif ne peut accéder aux résultats des examens.

B. Contrôle d'accès dépendant du contenu.

L'accès peut être dépendant du contenu de l'objet. Par exemple, un directeur des ventes peut avoir accès aux salaires de ses vendeurs, mais pas aux salaires des membres des autres départements. Avec ce type de contrôle, la décision d'accès peut être prise seulement après la recherche de la valeur de la donnée.

C. Contrôle par type d'accès.

Il existe un ensemble de possibilités associées à un objet. L'emploi de l'ensemble de ces possibilités n'est peut-être pas autorisé pour tous les utilisateurs. Par exemple, toute personne intéressée dans une banque, peut lire le cours des changes, mais une seule personne, dûment autorisée, peut mettre à jour ce fichier.

D. Contrôle d'accès dépendant du contexte.

Ce contrôle détermine les objets auxquels on peut accéder dans une même requête ou dans un ensemble spécifique de requêtes. Le corollaire de cette politique est l'obligation que certains objets apparaissent ensemble. Par exemple : afin d'éviter la découverte du salaire d'un employé, on peut interdire que le nom et le salaire soient demandés simultanément. Comme exemple complémentaire : l'information au sujet d'une personne arrêtée ne peut être fournie que si l'arrêt du tribunal est aussi demandé.

E. Contrôle d'accès dépendant de l'historique.

Ce contrôle considère la requête actuelle dans le contexte de requêtes précédentes. Un objet est compromis si un utilisateur peut déduire des valeurs confidentielles à partir des informations reçues lors de ses précédentes demandes. Par exemple, un utilisateur peut d'abord demander les noms et les fonctions des membres d'un département et, quelques temps après, la liste des salaires des membres de ce département. Avec ces informations, il pourrait trouver certaines corrélations entre les noms et les salaires.

F. Contrôle de flux.

Un flux existe entre un objet X et un objet Y dès lors qu'il existe un échange d'informations entre X et Y. Copier un fichier X dans un fichier Y est un exemple de flux simple. Un contrôle de flux est nécessaire afin d'éviter la fuite d'informations d'un utilisateur autorisé vers un utilisateur non autorisé. Ce contrôle est réalisé en affectant à chaque objet une classe de sécurité. Les flux sont autorisés ou interdits en fonction de cette classification.

Journal d'utilisation du système

Un tel journal est nécessaire pour les raisons suivantes :

- aucun système de sécurité n'est sûr à 100 %, une supervision du système pour en déceler les failles est donc indispensable ;
- détecter les violations et tentatives de violations de la sécurité ;
- décourager les utilisateurs de tenter des activités frauduleuses.

La création de journaux peut produire un grand volume de données qui doivent être analysées afin d'être utiles. Le but de l'analyse est de permettre aux responsables de la sécurité de détecter et de réagir à des atteintes aux règles et politiques établies.

5. Cryptologie

51. Introduction

Le transport et le traitement de l'information ayant trouvé des solutions techniques efficaces avec les réseaux de transmission de données et les systèmes informatiques, de nouvelles préoccupations deviennent maintenant primordiales pour assurer un développement harmonieux des systèmes télématiques. Elles portent le nom de discrétion, identification, certification, authentification, confirmation, validation, signature, ...

Par exemple, le développement du courrier électronique ne peut se faire sans apporter un équivalent électronique à ce qui fait la spécificité du service postal. Or, le service postal est caractérisé par une enveloppe portant le cachet de la poste qui fait foi. Cette enveloppe préserve la confidentialité et l'intégrité du message. Le pli est délivré au légitime destinataire, éventuellement contre un accusé de réception. La lettre, une feuille de papier où sont réunis texte et signature, peut être soumise à expertise et produite devant les tribunaux. Il faut trouver un équivalent à toutes ces garanties.

Lorsque le message est transmis par des moyens de télécommunications, il est illusoire de songer à en interdire l'accès aux indiscrets, si on n'a pas le contrôle total du (des) support(s) de transmission. Mais on peut rendre le message indéchiffrable par d'autres que son (ses) destinataire(s). C'est l'objet de la cryptologie.

52. Quelques définitions

Cryptologie : science du chiffre dans ses deux aspects : cryptographie et cryptanalyse.

Cryptographie : science du chiffrement et du déchiffrement.

Cryptanalyse : science du décryptement.

Cryptogramme : message chiffré.

Chiffrer : transformer un texte clair en cryptogramme à l'aide d'un algorithme de chiffrement.

Déchiffrer : rétablir en clair un cryptogramme, en connaissance de l'algorithme de déchiffrement.

Décrypter : rétablir en clair un cryptogramme, sans connaissance de l'algorithme de déchiffrement.

Clés de chiffrement et de déchiffrement : informations secrètes ou publiques, partagées ou non, utilisées conjointement avec un algorithme de chiffrement ou de déchiffrement.

53. La sécurité des systèmes de chiffrement

Shannon a montré que pour qu'un système de chiffrement soit inconditionnellement sûr, il faut que l'entropie (mesure du désordre) de la source de la clé de chiffrement soit supérieure à l'entropie de la source du message, de manière à masquer totalement la redondance naturelle du langage après chiffrement. Dans ce cas, sans idée particulière sur la clé mise en oeuvre, le décrypteur ne peut rétablir en clair un cryptogramme.

Un système inconditionnellement sûr serait effectivement utilisé pour protéger la liaison rouge entre Washington et Moscou. Les clés sont des suites binaires produites au hasard et utilisées une seule fois. Elles sont échangées sous forme de bandes magnétiques transitant par les valises diplomatiques. Le signal numérique représentant l'information est combiné bit à bit par "OU exclusif" avec la suite binaire figurant la clé, qui doit donc avoir une taille supérieure ou égale à celle du message. L'opération inverse permet au récepteur de retrouver l'information claire.

Il n'en va pas de même pour les systèmes mis en oeuvre sur les réseaux. D'abord, les clés de chiffrement, de tailles limitées, sont bien plus petites que les quantités d'informations échangées, d'où une entropie inférieure pour la clé. Ensuite, en l'absence de valise diplomatique généralisée, la transmission des clés est beaucoup moins sûre.

Pour décrypter un cryptogramme, le décrypteur peut toujours essayer des clés au hasard et déclarer qu'une clé est probable à condition que le "déchiffrement" du cryptogramme intercepté fournisse un résultat intelligible. Le but de la cryptanalyse consiste à définir des stratégies sur les clés pour atteindre la bonne solution avec un minimum d'efforts.

Le but de la cryptographie consiste donc à spécifier des algorithmes de chiffrement tels que la seule solution pour trouver des clés probables à partir de couples "clair-chiffré" soit d'essayer des clés les unes après les autres. La sécurité du système dépend alors de la complexité et de la durée des calculs à effectuer pour le déchiffrement et du nombre de clés potentielles, qui doit être le plus grand possible pour diminuer les chances de réussite par recherche exhaustive.

Remarquons enfin qu'il est impossible de démontrer qu'un système est sûr au sens de la complexité de calcul : seul le fait de casser un système montre qu'il est mauvais.

54. L'apparition de la cryptologie publique

Jusqu'à ces 20 dernières années, la connaissance en cryptologie est restée confinée à quelques organismes gouvernementaux spécialisés. Son usage était limité à des applications diplomatiques et militaires.

Les années 75 à 80 furent particulièrement fertiles, notamment avec la publication des spécifications de l'algorithme DES (**D**ata **E**ncryption **S**tandard).

55. Les opérations élémentaires du chiffrement

Les opérations élémentaires sont la substitution et la transposition.

La substitution consiste à remplacer chaque caractère du texte clair par un autre caractère pris dans un alphabet de susbtitution.

Une transposition consiste à permuter les caractères du texte clair suivant une règle de transposition.

56. Les algorithmes à clés secrètes et publiques

Différents systèmes de chiffrement-déchiffrement sont utilisés suivant les menaces à conjurer. Les menaces élémentaires concernent la confidentialité et l'intégrité des données.

- Une information sensible peut atteindre quelqu'un d'autre que le légitime destinataire : c'est le problème de la confidentialité.

L'émetteur remplace le clair par le chiffré grâce à un algorithme de chiffrement. Le récepteur rétablit le clair à partir du chiffré par une opération de déchiffrement. Quand la confidentialité est menacée, au moins le récepteur doit maintenir secret son algorithme.

- Une information fausse peut être injectée dans le système. Un message transmis peut être intercepté, modifié, retardé. Un faux message peut être produit, en simulant l'émetteur légitime. C'est le problème de l'intégrité.

L'émetteur utilise un algorithme de signature et émet un message signé. Le récepteur teste le message signé grâce à un algorithme de vérification. Quand l'intégrité est menacée, au moins l'émetteur doit maintenir secret son algorithme.

Dans les systèmes à clés secrètes, on déduit en général facilement l'algorithme de chiffrement à partir de l'algorithme de déchiffrement, et réciproquement. La sécurité repose donc sur les clés utilisées. Les clés correspondantes doivent être secrètes et il est impossible de dissocier les deux types de menaces.

Dans les systèmes à clés publiques, il est "impossible" (voir remarque) de déduire facilement l'algorithme de chiffrement à partir de l'algorithme de déchiffrement, et vice-versa. L'émetteur maintient secret son algorithme pour protéger l'intégrité et le récepteur maintient secret son algorithme pour protéger la confidentialité.

Remarque.

Le mot "impossible" doit être précisé. Le concept s'éclaire quand on considère l'efficacité des algorithmes. Un algorithme est efficace tant qu'il peut être exécuté avec des ressources raisonnables en temps, mémoire et énergie. Nous considérons donc qu'il n'existe aucun algorithme efficace permettant de déduire l'algorithme de chiffrement à partir de l'algorithme de déchiffrement, et vice-versa.

57. Le DES

L'algorithme DES (**D**ata **E**ncryption **S**tandard) fut publié le 15 janvier 1977 par le NBS (**N**ational **B**ureau of **S**tandards) afin de protéger les informations nominatives non classifiées détenues par les Agences Fédérales des Etats-Unis. En mars 1978, le même algorithme fut publié par l'ANSI (**A**merican **N**ational **S**tandard **I**nstitute) sous le nom de DEA (**D**ata **E**ncryption **A**lgorithm), pour servir de norme commerciale de chiffrement. Depuis, l'ISO envisage la normalisation de cet algorithme sous le nom de DEA1 (**D**ata **E**ncipherment **A**lgorithm number one).

Le DES est du type algorithme à clés secrètes. La description de l'algorithme est publique. La clé de chiffrement est la même que la clé de déchiffrement. Cette clé a une longueur de 56 bits, ce qui offre 2 exposant 56 clés différentes.

On estime le temps nécessaire pour casser le DES, par recherche exhaustive de la clé, entre 11000 ans et 228 millions d'années, selon la puissance de calcul disponible. Bien sûr, il faut tenir compte de l'évolution rapide des puissances de calculs, mais le DES a encore de beaux jours devant lui. Pour augmenter encore l'efficacité du DES, On peut procéder à deux, ou plus, opérations de chiffrement successives.

6. Le facteur humain

On peut comparer la sécurité d'un système à une chaîne. Le niveau de sécurité dépend de la résistance du maillon le plus faible.

En sécurité informatique, comme dans d'autres domaines, le maillon le plus faible est souvent l'utilisateur du système, c'est à dire l'homme.

Tout le problème est de renforcer ce maillon. En fait, il s'agit de diminuer l'influence du facteur humain par l'utilisation de techniques d'autant plus sophistiquées que l'on désire atteindre un niveau de sécurité élevé.

Or le coût de ces techniques peut devenir prohibitif.

Il faut donc trouver un compromis entre les souhaits et ce qui est matériellement et financièrement réalisable, en n'oubliant pas que la confiance que l'on peut avoir dans un système repose en définitive sur la confiance que l'on a dans ses utilisateurs.

Eléments de théorie de téléinformatique

1. Définitions

La téléinformatique est l'association de techniques de télécommunications et de l'informatique pour la transmission d'informations.

La télématique est l'ensemble des services de nature ou d'origine informatique pouvant être fournis à travers un réseau de télécommunications (Macchi & Guilbert, Téléinformatique).

2. Codage de l'information

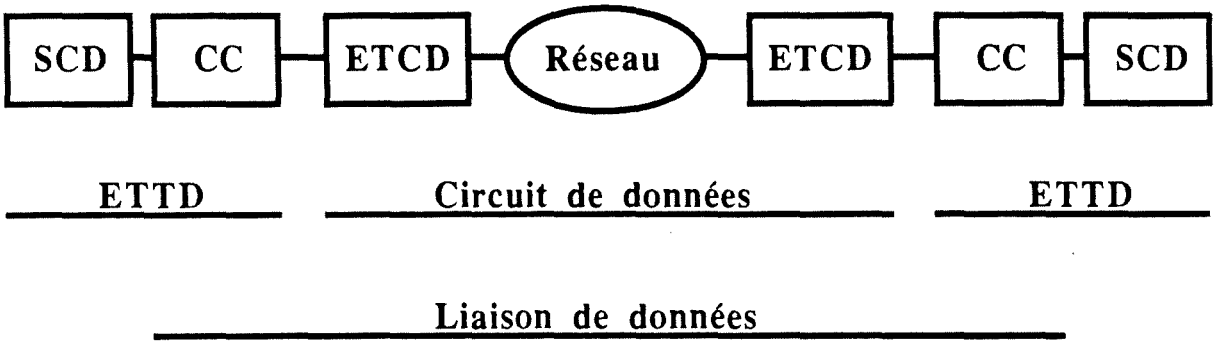
Afin de pouvoir être manipulée et échangée, toute information doit être mise sous forme de symboles. La signification précise de ces symboles est fondamentale pour permettre leur interprétation. Il s'agit d'une convention entre l'émetteur et le destinataire de l'information.

En informatique, le symbole élémentaire pour représenter l'information est le **bit** (**bi**nary digi**t**). Un bit peut représenter deux informations différentes. On peut grouper plusieurs bits en un mot. Si **n** est le nombre de bits dans un mot, cela permet de représenter 2 exposant **n** informations différentes. De nombreux ordinateurs reconnaissent des mots de 8 bits appelés octets ou bytes, ce qui permet de coder 256 symboles différents. Ces symboles sont agencés pour représenter l'information.

Différents codes ont été proposés, permettant d'établir une correspondance entre les informations et les symboles utilisés. L'un des plus usités est le code ASCII (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange), ou CCITT n° 5 (Comité **C**onsultatif **I**nternational **T**élégraphique et **T**éléphonique), qui permet de coder tous les caractères couramment utilisés, lettres minuscules ou capitales, chiffres, signes de ponctuation et autres symboles.

3. Structure générale d'un système de télécommunication

De manière générale, la structure d'un système de télécommunication comprend des équipements terminaux (ETTD), des équipements d'adaptation (ETCD) et un réseau assurant le transfert des informations entre les utilisateurs (Macchi & Guilbert, Téléinformatique).



SCD : Source et/ou Collecteur de Données

CC : Contrôleur de Communications

ETCD : Equipement de Terminaison du Circuit de Données

ETTD : Equipement Terminal de Traitement de Données

31. ETTD

L'information est émise ou reçue par un Equipement Terminal de Traitement de Données (ETTD). Dans un ETTD, on peut distinguer deux parties qui réalisent des fonctions différentes : la machine de traitement qui peut être source ou collecteur de données et le contrôleur de communication qui regroupe les fonctions de communication.

Un ETTD peut être un terminal, un gros ordinateur, un ordinateur personnel, un téléfax, etc.

32. ETCD

L'Equipement de Terminaison du Circuit de Données (ETCD) est chargé d'adapter les signaux émis par l'ETTD au support de transmission, et vice-versa. L'ETCD assure de plus les fonctions d'établissement et de libération du circuit de données.

L'ETCD le plus commun est un modem qui permet d'utiliser divers supports de transmissions, tel le réseau téléphonique commuté. L'ETCD peut être inclus physiquement dans l'ETTD.

Modem

Le modem est un ETCD permettant la transmission des données par une technique de modulation-démodulation, d'où son nom. D'une façon schématique, on peut considérer qu'un modem se caractérise par deux paramètres : la vitesse d'émission de l'information et le support utilisable.

La vitesse de transmission est mesurée par le nombre de bits transmis par seconde (bps). Les avis du CCITT, qui ont valeur de normes internationales, couvrent des vitesses allant de 300 à 144000 bps. Tandis que les supports de transmissions considérés sont le réseau téléphonique commuté, la ligne téléphonique spécialisée définie par l'avis M1020 et le canal groupe primaire défini par l'avis H14.

33. Réseau

En principe, la nature du réseau, les équipements et techniques mis en oeuvre ne concernent pas l'utilisateur. Seules les caractéristiques de l'interface et les fonctionnalités du réseau sont indispensables pour permettre la connexion au réseau et son utilisation.

Ainsi, un réseau peut faire appel à des techniques aussi diverses que la transmission par ondes hertziennes, par voie analogique ou numérique, ou encore par satellites.

4. Notion de protocole : le modèle de référence OSI

Un protocole définit un ensemble de conventions nécessaires pour faire coopérer des entités généralement distantes, en particulier pour établir et entretenir des échanges d'informations entre ces entités.

Le modèle de référence pour l'**I**nterconnexion de **S**ystèmes **O**uverts (**O**pen **S**ystems **I**nterconnection) définit l'architecture en couches normalisée, adoptée conjointement par l'ISO et le CCITT pour les réseaux téléinformatiques et télématiques.

41. Technique de modélisation

L'objectif de la normalisation OSI est de permettre la constitution de réseaux téléinformatiques normalisés, au sein desquels peuvent venir s'intégrer des systèmes téléinformatiques hétérogènes alors appelés systèmes ouverts. Pour permettre cette hétérogénéité, les normes OSI se limitent à spécifier les fonctions à remplir par chaque système ouvert et les protocoles à mettre en oeuvre entre ces systèmes, en évitant soigneusement d'imposer un mode de réalisation particulier des dites fonctions. Les normes OSI spécifient donc globalement le comportement des systèmes ouverts dans leurs échanges avec d'autres systèmes ouverts, et non leur fonctionnement interne.

42. Concepts de base

L'architecture définie par le modèle OSI est constituée par l'empilement de sept couches d'activités, chaque couche utilisant les services de la couche inférieure et offrant les siens à la couche supérieure. Chaque couche possède un rôle bien défini, ce qui permet l'indépendance de réalisation des services entre couches, celles-ci communiquant par des primitives de services constituant les interfaces entre couches.

43. Les 7 couches du modèle OSI

1- Couche physique : la couche physique est chargée de l'interface entre le système et le support physique.

2- Couche liaison de données : la fonction de base de la couche liaison de données est d'effectuer, le cas échéant, la détection et la reprise des erreurs.

3- Couche réseau : la fonction essentielle de la couche réseau consiste à effectuer le relais ainsi que le routage des messages à travers le réseau. De plus, la couche réseau peut effectuer un contrôle de flux lorsque cela permet d'optimiser l'utilisation des ressources de transmission.

4- Couche transport : les fonctions essentielles de la couche transport sont d'effectuer le contrôle global du transport de données entre systèmes extrémités.

5- Couche session : la couche session réalise les fonctions qui sont nécessaires au support du dialogue entre systèmes extrémités, telles l'initialisation, la synchronisation et la terminaison du dialogue.

6- Couche présentation : la couche présentation prend en charge les problèmes associés à la représentation des informations que les applications désirent échanger ou manipuler. En d'autres termes, elle s'occupe de la syntaxe des données échangées, permettant ainsi aux entités d'applications de ne se préoccuper que des aspects sémantiques des informations.

7- Couche application : la couche application réalise les fonctions nécessaires aux applications tournant sur les machines et désireuses de se connecter avec d'autres applications via le réseau.

5. Protocole de transfert de fichiers

51. Définition

Un fichier est une collection d'informations. Un fichier est caractérisé par une structure et un format. La structure définit l'organisation des données dans le fichier, c'est-à-dire le contenu, tandis que le format décrit le fichier lui-même et tous ses attributs, c'est-à-dire le contenant.

L'objet d'un protocole de transfert de fichiers est de permettre la transmission de tout ou partie d'un fichier, d'un système à un autre. Selon l'étendue de ses responsabilités, il peut être une application au sens du modèle OSI, mais il peut aussi remplir des fonctions normalement du ressort des couches inférieures du modèle OSI.

Les transferts peuvent être de trois types : soit un utilisateur A peut demander à un utilisateur B de lui transmettre un fichier, soit A peut vouloir transmettre un fichier à B, soit A peut demander à B de transmettre un fichier à un troisième utilisateur C.

Un protocole de transfert de fichiers interagit avec trois entités : l'utilisateur local, le système de gestion de fichier local et le protocole de transfert de fichiers tournant sur le système distant.

Un transfert de fichier peut concerner : soit les données contenues dans le fichier, soit les données et la structure du fichier, soit les données, la structure et tous les attributs du fichier.

Caractéristiques

Un protocole de transfert de fichier peut être caractérisé par les services qu'il offre et les règles qui régissent ses échanges avec d'autres systèmes.

52. Quelques grands noms

Parmi les principaux protocoles de transfert de fichiers, citons :

FTP

Au début des années 70, l'interconnexion de réseaux basés sur différentes techniques a nécessité la mise en place de protocoles permettant cette interconnexion. Ainsi est apparu TCP-IP (**T**ransmission **C**ontrol **P**rotocol - **I**nternet **P**rotocol) qui, bien qu'encore répandu sur un grand nombre de systèmes, est remplacé progressivement par le modèle OSI. IP se situe au niveau 3 du modèle OSI et assure l'interconnexion des réseaux. TCP correspond aux niveaux 4 et, en partie, 5 du modèle OSI. Ces protocoles ont permis la mise en oeuvre de services divers, tel FTP (**F**ile **T**ransfert **P**rotocol). FTP permet le transfert de fichiers quelconques d'un système vers un autre.

FTAM

FTAM, pour **F**ile **T**ransfert, **A**ccess and **M**anagement, est le protocole de transfert et de manipulation de fichiers normalisé par le CCITT sous la référence DP 8571 et par l'ECMA sous la référence ECMA-85. FTAM est un protocole du niveau application du modèle OSI.

Comme FTP, FTAM permet le transfert de fichiers d'un système vers un autre, en y ajoutant des fonctions d'accès et de gestion. FTAM introduit la notion de fichier virtuel qui définit une structure unique pour les fichiers. Ce qui assure l'indépendance du fichier vis-à-vis d'un système particulier. Chaque système extrémité est alors responsable de la conversion fichier réel-fichier virtuel et vice-versa.

XModem et dérivés

Apparu vers la fin des années 70, XModem est surtout utilisé pour les communications entre micro-ordinateurs. Assez pauvre dans ses possibilités, XModem souffre de limitations qui rendent souvent indispensable l'adjonction de fonctions supplémentaires. Néanmoins, de par la simplicité des concepts mis en oeuvre, XModem reste accessible à tout programmeur quelque peu averti. C'est ce qui en a fait son succès et la grande variété de ses descendants, chacun lui ajoutant l'une ou l'autre caractéristique qu'il juge indispensable. Il a donné ainsi naissance à une kyrielle de protocoles de transfert de fichiers "XModem like", de telle sorte qu'il est aujourd'hui bien difficile de trouver deux protocoles se réclamant de XModem capables de coopérer pour mener à terme le transfert d'un fichier.

Kermit et dérivés

Kermit est aux communications entre micro-ordinateurs et gros ordinateurs ce que XModem est aux communications entre micro-ordinateurs. Beaucoup plus complet que XModem, Kermit présente de nombreuses caractéristiques qui en font un produit polyvalent. Comme XModem, Kermit a subi diverses évolutions qui ont généré une descendance variée de protocoles "Kermit like".

Nous commencerons par faire un panorama d'ensemble des services de télécommunications et de leurs fournisseurs. Nous passerons ensuite en revue les services susceptibles d'être utilisés pour la transmission des résultats d'analyses biomédicales, sans préjuger du système que nous proposerons.

1. Panorama d'ensemble

11. Les fournisseurs de services de télécommunications

Tandis qu'en Europe, à quelques exceptions près, les télécommunications sont encore un monopole confié à des organismes publics ou parapublics, le continent nord-américain a été le théâtre d'une prolifération d'entreprises privées de télécommunications nationales ou régionales.

Le début des annnées 80 a été marqué par une évolution importante aux USA : la dérégulation ou déréglementation, qui introduit la concurrence dans le domaine des services de télécommunications. Ce terme de dérégulation a également été utilisé à propos des mouvements d'ouverture du monopole ou de privatisation des organismes publics de télécommunications amorcés dans les pays membres de la Communauté Européenne.

12. Evolution des services de transmission de données

La téléinformatique s'est tout d'abord appuyée, pour la connexion de terminaux distants à des ordinateurs, sur des moyens classiques de télécommunications plus ou moins bien adaptés, comme les réseaux télégraphiques et téléphoniques. Le début des années 70 a vu un développement systématique de services de transmission de données spécifiques aux besoins du télétraitement.

Les efforts ont principalement porté sur les points suivants :

- Amélioration de la qualité et des performances, par la réalisation de supports améliorés télégraphiques, téléphoniques ou de circuits spécialisés.

- Diminution des coûts de transmission à grande distance, doublée d'une amélioration de la qualité.

- Constitution de réseaux de commutation spécifiques pour les données, tout d'abord analogiques, puis numériques. Deux filières ont été développées en concurrence : la commutation de circuits de données, dérivée de la commutation téléphonique temporelle, et la commutation par paquets, dérivée des techniques de commutation de messages et des techniques informatiques utilisées dans les réseaux d'ordinateurs. La commutation par paquets a pris vers 1973-1975 un net avantage sur la commutation de circuits.

- Utilisation de satellites pour faciliter les communications à longues distances et à haut débit.

- Généralisation des techniques de transmission numérique, moins chères et plus fiables.

Enfin, l'intégration des différents services de télécommunications et des infrastructures est menée progressivement, au fur et à mesure de la numérisation du réseau téléphonique, à travers les étapes de mise en place des **R**éseaux **N**umériques à **I**ntégration de **S**ervices (RNIS).

13. Classification des services

Indépendamment des techniques utilisées, c'est en fonction de la richesse du service offert que l'utilisateur va déterminer les équipements qu'il devra acquérir pour mettre en oeuvre des applications téléinformatiques. On a souvent regroupé les services selon ce critère en cinq catégories allant des services traditionnels de télécommunications à des services spécifiquement informatiques :

- La fourniture de moyens classiques de transmission, le plus souvent analogiques, et sans interface spécifiquement informatique. L'utilisateur doit alors ajouter des dispositifs de conversion du signal et de protection contre les erreurs. Mais le support est transparent à toute forme de signal respectant certaines limites.

- Les circuits de transmission de données à débit binaire spécifié, présentant des interfaces normalisées et reconnues par les constructeurs de matériel informatique. Cette catégorie comprend notamment les liaisons spécialisées équipées de modems.

- Les réseaux publics de commutation de données, avec interfaces, signalisations et protocoles d'accès normalisés. De tels réseaux permettent de diminuer encore plus les coûts de transmission par un partage plus dynamique des supports et d'éviter la prolifération de réseaux privés coûteux et incompatibles. Ils facilitent les interconnexions de systèmes, l'évolution vers l'informatique répartie et peuvent jouer un rôle important dans la progression de la normalisation informatique.

- La location de terminaux compatibles avec les services de transmission précédents et, si possible, avec une variété de systèmes de traitement. Un exemple : le minitel.

- Enfin, la cinquième catégorie empiète encore plus nettement sur le domaine informatique, avec la fourniture de services publics de télétraitement ou de bases de données, ou encore de systèmes téléinformatiques complets.

2. Transmission de textes

Un texte est un ensemble sans structure prédéfinie de caractères divers.

21. Télex

Le télex permet la transmission d'informations écrites. Le réseau télex assure la connexion temporaire entre deux terminaux télex, qui sont des téléimprimeurs à réception automatique.

Un abonné du télex a ainsi la possibilité :

- de converser par écrit avec un autre abonné, si celui-ci est présent au moment de l'appel ;

- de transmettre, ou de recevoir, des messages à toute heure, même si son correspondant, ou lui-même, est absent.

Le réseau télex est étendu au monde entier. La transmission se fait à la vitesse faible de 50 bps (7 caractères par seconde). Un ordinateur peut être connecté au réseau.

L'évolution est marquée par l'introduction de terminaux plus intelligents et par la mise en oeuvre de nouveaux services tels que la remise différée, le circuit de conférence et l'adressage multiple.

22. Télétex

Le télétex est un service international normalisé pour la communication de textes. Il utilise le réseau public de transmission de données par paquets DCS (Data Communication Service). Le terminal est relié au réseau DCS au moyen d'un raccordement direct respectant le protocole X25.

Fonctions de base

1. Fonction de transmission.

L'appareil reçoit et envoie des messages de et vers d'autres abonnés, aussi bien en service national qu'international avec une vitesse minimum de 2400 bps (environ 20 secondes pour un document de format A4).

2. Fonction de traitement de textes.

L'appareil offre en général les mêmes facilités qu'une machine classique de traitement de textes, à savoir : composer, modifier, stocker et imprimer des lettres ou des documents. Les textes sont toujours élaborés localement et mémorisés avant d'être expédiés. Les caractères utilisés correspondent au jeu de caractères d'une machine à écrire électronique ordinaire (309 symboles différents peuvent être imprimés).

3. Interfonctionnement avec le service télex.

Par ailleurs, le terminal télétex offre la possibilité de recevoir et d'envoyer des messages de et vers n'importe quel abonné télex dans le monde.

Cela est possible grâce à une unité de conversion installée et exploitée par la RTT. Cette unité a pour tâche de transposer les protocoles télex en protocoles télétex et vice-versa, de convertir le codage des caractères et d'adapter les vitesses de transmission.

Grâce aux possibilités de traitement de textes, l'abonné télétex a de plus la faculté de préparer ses messages télex de façon souple avant de les envoyer.

Nouvelles fonctions

Un certain nombre de nouvelles fonctions ont été normalisées par le CCITT dans le cadre des protocoles télétex. Ainsi, on peut noter :

- La possibilité de transmettre des documents comportant à la fois des textes et des images.

- L'intégration du service télétex dans le service plus général de messagerie électronique. Ce dernier regroupera toutes les fonctions en rapport avec l'échange de documents.

Rôle de la RTT

La RTT gère l'unité de conversion télex/télétex, publie la liste des abonnés télétex tant nationaux qu'internationaux et agrée les terminaux destinés à être raccordés au service télétex.

23. DCS.MAIL

Le service DCS.MAIL est offert sur le réseau DCS. Il permet à l'abonné d'accéder à une boîte aux lettres qui lui est réservée et qui est destinée à l'échange de messages entre utilisateurs du service. Les messages peuvent être envoyés et reçus à l'aide d'un terminal avec clavier et écran ou imprimante, ou encore d'un appareil télex.

L'interconnexion entre DCS.MAIL et le réseau télex est assurée. Cette facilité offre la possibilité d'échanger des messages avec les abonnés télex tant au niveau national qu'international.

De plus, dans un proche avenir, l'interconnexion de DCS.MAIL avec d'autres systèmes de messagerie belges et étrangers sera également possible. Cette interconnexion conduit à la création d'un service de transfert de messages DCS.400 répondant à la norme X400.

3. Transmission de documents

Un document peut être constitué de textes, de graphiques, de dessins, sans structure prédéfinie.

31. Téléfax

Le téléfax offre la possibilité de transmettre à un correspondant des lettres, des dessins, etc ..., dans leur forme originale à l'aide d'une ligne téléphonique, sans avoir à traiter d'abord le document. Le correspondant reçoit sans délai la copie sur son télécopieur.

Le téléfax est un service international normalisé pour la transmission de télécopies via le réseau téléphonique public. Les appareils téléfax doivent être conformes à des normes internationales, ils sont classés en trois catégories appelées "groupes" qui diffèrent par la durée de transmission, pour un document de format A4 :

- groupe 1 : 6 minutes,
- groupe 2 : 3 minutes,
- groupe 3 : 1 minute.

La RTT met des appareils des groupes 2 et 3 à la disposition des abonnés.

32. DCS.FAX

La RTT offre un service public pour fac-similé à hautes performances, DSC.FAX, qui assure la transmission d'un document A4 en 10 secondes avec une résolution de 200 points par pouces.

Le courrier électronique

Le courrier électronique est un terme générique pour désigner la transmission de textes et/ou de documents.

4. Transmission de données

La transmission de données est l'acheminement de données sous forme codée.

41. Datel

Datel est le service de transmission de données sur le réseau téléphonique public. Ce service requiert l'utilisation d'un modem sur lequel est raccordé un équipement terminal de traitement de données.

La vitesse de transmission autorisée est limitée à 9600 bps. Les installations des correspondants doivent être équipées avec des modems compatibles. Toutefois, la RTT ne peut en aucun cas garantir la qualité des transmissions. Les modems avec un débit binaire inférieur ou égal à 2400 bps sont fournis par la RTT. Cependant, dans certains cas, l'utilisation d'un modem agréé par la RTT est autorisée.

Les terminaux qui sont raccordés sur un modem fourni par la RTT doivent être agréés au préalable par la RTT.

42. Circuits d'abonnement

Ces circuits, appelés aussi lignes louées ou spécialisées, sont mis à la disposition du client pour ses besoins personnels et relient entre eux, de manière permanente, deux ou plusieurs points terminaux. Ils sont disponibles tant sur le plan national qu'international.

Les circuits de transmission de données permettent des vitesses variant entre 200 bps et 2 Mbps ; des vitesses de 8, 34 et 140 Mbps seront possibles dans un proche avenir.

Les avantages de tels circuits sont : permanence, disponibilité, coûts fixes, qualités normalisées, transparence, fiabilité, hauts débits, souplesse d'utilisation et d'application, support personnalisé, gestion du réseau et modems au choix.

43. DCS : Data Communication Service

DCS est le nom du réseau public belge de transmission de données avec commutation par paquets. Il est constitué d'un certain nombre de liaisons numériques à grande vitesse reliant des noeuds de commutation. Il est accessible par des lignes analogiques équipées de modem exclusivement fournis par la RTT. Le principe appliqué est la commutation de paquets : les messages à transmettre sont divisés en paquets qui sont acheminés indépendamment les uns des autres par le réseau.

Accès au réseau

Les abonnés peuvent accéder au réseau de 4 manières :

- par une liaison permanente respectant l'avis X25, à des vitesses diverses : 2400, 4800, 9600, 48000, 56000 et 64000 bps ;

- par une liaison permanente vers un équipement public d'assemblage et de désassemblage de paquets (PAD), selon l'avis X28 et à des vitesses de 300 et 1200 bps ;

- par le réseau téléphonique commuté vers un PAD, à des vitesses de 300, 1200 et 1200/75 bps ;

- par le réseau télex vers un PAD.

Avantages

Les principaux avantages du réseau DCS sont :

- l'interconnectabilité d'appareils différents avec adaptation des vitesses ;
- la bonne protection contre les erreurs de transmission ;
- la possibilité de créer plusieurs connexions simultanées sur une liaison d'accès ;
- la possibilité de créer des circuits permanents ;
- la disponibilité ;
- la tarification indépendante de la distance, en service national ;
- la connexion à de nombreux réseaux étrangers.

Secret des communications

Tout usager est identifié sur le réseau par :

- son NUA (**N**umber **U**ser **A**dress), s'il est relié directement,

- son NUI (**N**umber **U**ser **I**dentifier), s'il accède au réseau DCS par le réseau téléphonique. Ce NUI est transformé par le réseau en un NUA que reçoit l'abonné appelé dans le paquet d'appel entrant.

L'abonné qui reçoit un appel peut, lui aussi, vérifier sa provenance, car il reçoit toujours le NUA de l'abonné appelant.

La RTT propose des services complémentaires qui permettent de s'assurer que les correspondants ont bien l'autorisation d'accès : ce sont les **G**roupes **F**ermés d'**U**sagers (GFU).

Des mesures supplémentaires peuvent toujours être prises par les abonnés :

- test du NUA de l'abonné appelant ;

- utilisation de mots de passe supplémentaires ;

- chiffrement des données avant de les introduire dans les paquets.

5. Le vidéotex

Le service vidéotex de la RTT est décrit plus en détail, en raison de l'importance future qu'il sera amené à prendre dans le cadre d'une télématique grand public et professionnelle.

Présentation

Né en France, le vidéotex est le produit conjugué des techniques de télécommunications, de l'informatique et de la télévision.

C'est dans les années 70, qu'est apparue l'idée de connecter à un ordinateur central des terminaux constitués d'un récepteur TV, d'un clavier, d'un modem et d'un système de décodage et de visualisation d'informations alphanumériques ou graphiques.

Cet équipement, connecté d'un côté au réseau téléphonique et de l'autre à la prise d'antenne ou de vidéo du récepteur TV, constitue un terminal et correspond au mode d'utilisation dit vidéotex interactif.

Une variante, appelée vidéotex diffusé ou télétext, consiste à utiliser le réseau de diffusion de la télévision : un démultiplexeur permet à l'usager de sélectionner une page d'informations parmi un ensemble de pages diffusées en permanence sur un canal de réception.

Le vidéotex offre deux types de services liés à ses deux modes d'utilisation, ce sont :

- les services de consultation qui permettent à l'usager d'interroger les banques de données les plus diverses : annuaire électronique, cours de bourse, météo, comptes bancaires, etc ;

- les services de transaction avec identification de l'appelant. Grâce à ces services, l'usager a la possibilité d'interroger divers prestataires de services et, son choix fait, de le concrétiser en passant une commande, en effectuant une réservation, etc.

La norme

La RTT a opté pour la norme PRESTEL (norme CEPT, profil 3). Afin de représenter correctement les caractères accentués, il existe des terminaux suivant une variante belge de cette norme.

Les services ouverts (sans restriction d'accès) peuvent être offerts sur le réseau uniquement dans le format de 40 caractères par ligne. Des services fermés peuvent, par ailleurs, utiliser le format 80 caractères par ligne.

Le terminal

Un terminal, de bureau ou portable, peut être un :

- ordinateur personnel adapté avec carte et/ou logiciel vidéotex ;
- téléviseur adapté avec décodeur ;
- terminal ASCII (TTY) ;
- terminal TELETEL pour l'accès international aux services en France.

Ces appareils doivent avoir été préalablement présentés à la RTT par leur constructeur ou distributeur pour agrément. Le service vidéotex en contrôle par après le bon fonctionnement sur le réseau.

L'émulation par micro-ordinateur

Mis à part le modem, les micro-ordinateurs standards disposent de tous les éléments pour être utilisés comme un terminal vidéotex : un clavier, un écran, de la mémoire, une capacité de traitement de l'information et de communications externes.

L'émulation peut se faire de deux façons :

- soit par un logiciel sur un ordinateur personnel doté d'un modem agréé,
- soit par une carte additionnelle d'émulation complète avec modem intégré sur la carte.

Les fonctions remplies peuvent être :

- visualisation d'écran en couleurs ou teintes de gris ;
- stockage et traitement des écrans : extraction des données utiles, modification ou composition graphique ;
- éditeur de textes en local ;
- appels automatiques préprogrammés ;
- réponse automatique ou fonction serveur ;
- téléchargement de logiciels divers à partir de serveurs étrangers ;
- communication de micro à micro.

Il faut encore ajouter à toutes ces fonctions les utilisations classiques des micro-ordinateurs grâce à des logiciels de traitement de textes, des gestionnaires de bases de données, des tableurs, etc.

Les périphériques disponibles

Si le terminal est un ordinateur de type PC, on peut lui connecter les périphériques classiques tels que : imprimante, unités de stockage (disques, disquettes, bandes magnétiques, etc) et autres.

On peut, en outre, lui adjoindre un lecteur de cartes. Voyons quels sont les services potentiels d'un lecteur de cartes à mémoire.

Selon la carte utilisée, il permet :

- la connexion automatique à un service ;
- le contrôle d'accès à un service par authentification de la carte présentée et, éventuellement, vérification du code confidentiel du porteur ;
- le calcul de signature électronique des messages émis, permettant au serveur de s'assurer de l'intégrité des messages reçus ;
- la mémorisation certifiée de transactions dans la carte et la lecture certifiée d'informations contenues dans la carte, garantissant la non répudiation des transactions effectuées ;
- la confidentialité des échanges par chiffrement et déchiffrement des données transmises sur le réseau.

On constate donc que l'utilisation d'une carte permet une protection accrue des informations et des transactions effectuées.

Le modem

Le modem doit être conforme à l'avis V23 du CCITT. Il se caractérise par une vitesse d'émission-réception de 75/1200 bps réversible. Cette propriété de réversibilité permet, par exemple, d'émettre des données vers un centre serveur à 1200 bps au lieu de 75 bps, ce qui procure un gain de temps appréciable lors d'un transfert important de données.

Les appareils vidéotex à modem incorporé et agréés peuvent être utilisés tels quels. Pour les autres appareils agréés, le modem externe peut être loué ou acheté à la RTT.

Le réseau et les centres serveurs

Les terminaux vidéotex sont reliés via le réseau téléphonique commuté à un PAV (**P**oint d'**A**ccès **V**idéotex) qui sert d'interface avec le réseau DCS sur lequel sont connectés directement les centres serveurs vidéotex. Les centres serveurs peuvent être publics ou privés.

Afin de pouvoir atteindre des services sur des ordinateurs externes, le système vidéotex RTT utilise, pour les couches supérieures au protocole X25, le protocole RTX entre PAV et ordinateurs externes. Le protocole RTX est basé sur le protocole PRESTEL-GATEWAY, pour les terminaux de type PRESTEL, et sur des variantes de X29 pour les autres types de terminaux.

Les services complémentaires

Le service vidéotex étant basé sur le réseau DCS, il en offre plusieurs possibilités. On notera principalement :

- la constitution de groupes fermés d'utilisateurs (GFU) ;
- la taxation à l'arrivée ;
- la vérification de l'identité de l'appelant ;
- la messagerie.

Les avantages

les principaux avantages avancés par la RTT sont :

- La bonne qualité de la communication via le réseau vidéotex ;
- Le droit d'accès, plusieurs langues et types de terminaux sont soutenus sur le réseau ;
- La RTT peut percevoir les coûts de la taxation et encaisser la rétribution des services payants. Le prestataire de services est alors déchargé du suivi des abonnements. L'utilisateur reçoit une facture globale ;
- Le prestataire de services choisit lui-même l'ordinateur sur lequel il désire mettre son service à disposition ;
- Chaque service est atteint d'une façon uniforme par l'utilisateur ;
- Tous les utilisateurs peuvent correspondre entre eux via un service public de messagerie vidéotex ;
- Pour le serveur, un raccordement X25, également utilisable pour d'autres applications, est suffisant.

1. Synthèse du problème

Un laboratoire d'analyses biomédicales souhaite utiliser ses moyens informatiques pour mettre à disposition des médecins les résultats des analyses demandées par ceux-ci. La transmission est envisagée par voie téléinformatique.

Le domaine spécifique de ce travail oblige à tenir compte d'éléments propres à la profession médicale. Celle-ci est régie par un code de déontologie édicté par l'Ordre des médecins qui veille à son respect et qui a pouvoir de sanction.

Les deux principaux problèmes sont la protection du secret médical et le libre choix du médecin et du patient.

Les résultats des analyses sont protégés par le secret médical. Celui-ci fait obligation que seules les personnes autorisées aient accès à ces données. Les mots clés sont identification et authentification des utilisateurs, confidentialité et intégrité des données transmises.

Le risque d'apparition d'un monopole du laboratoire vis-à-vis des médecins est dénoncé par l'Ordre des médecins. Ce monopole pourrait s'exercer sur les plans technique et financier. Les mots clés sont alors standardisation et faible coût du système à mettre en oeuvre.

Rappel

Nous nous intéressons à la transmission des résultats des analyses. Comment ces résultats sont produits et quelle utilisation en est faite ne nous concernent que dans la mesure où cela peut imposer certaines contraintes dans la recherche d'une solution au problème spécifique de la transmission.

2. Echanges laboratoire-médecin

A tout résultat d'analyse correspond une demande préalable. La demande ne nous intéresse pas directement, mais nous la considérerons aussi, afin de permettre une vue d'ensemble.

21. La demande d'analyses

La demande d'analyses est faite par le médecin prescripteur qui s'adresse au laboratoire de son choix. Cette demande est habituellement constituée de l'identification du patient, d'un sachet de tubes contenant les prélèvements et de la liste des examens à effectuer.

La transmission de cette demande peut se faire par divers moyens :

- Le patient se rend au laboratoire qui effectue les prélèvements.
- Le médecin effectue les prélèvements et porte la demande directement au laboratoire.
- Le médecin effectue les prélèvements et le laboratoire vient chercher la demande.
- Le médecin effectue les prélèvements et le laboratoire charge un transporteur privé de les prendre chez le médecin.

22. Les résultats des analyses

Une fois la demande reçue, le laboratoire commence les analyses et produit les résultats. Pour une même demande, certaines analyses peuvent être plus urgentes que d'autres. Selon l'urgence, l'analyse est effectuée plus ou moins rapidement. Ainsi, pour une même demande, les résultats des analyses peuvent être transmis en plusieurs comptes rendus partiels. La fréquence de transmission des comptes rendus résulte d'une convention entre le médecin et le laboratoire. Mais le laboratoire peut prendre l'iniative de transmettre un résultat plus rapidement que prévu, s'il l'estime nécessaire, par exemple pour la santé du patient.

Les modes de transmission les plus courants sont :

- Le laboratoire porte les résultats directement au médecin.
- Le laboratoire charge un transporteur privé de porter les résultats au médecin.
- Le médecin prend les résultats directement au laboratoire.
- Si l'urgence du résultat le justifie, le laboratoire peut le téléphoner au médecin.
- Le laboratoire envoie les résultats par la Poste.

Les supports de transmission les plus courants sont :

- Le papier, sous enveloppe s'il est transporté par un intermédiaire.
- Un support informatique (disquette, bande magnétique, etc...).
- Le téléphone, par voie orale.
- Le téléfax.

3. Ce que peut apporter la téléinformatique

Voyons quels sont les avantages et désavantages potentiels d'une transmission téléinformatique des résultats des analyses.

31. Le médecin prescripteur

Considérons la situation actuelle : pour une seule demande d'analyses, le médecin est susceptible de recevoir plusieurs comptes rendus partiels, sous diverses formes (papier, communication orale, support informatique). Le médecin est ensuite responsable de l'élaboration du dossier médical[1] du patient à partir des différentes informations récoltées. Cette disparité des moyens employés ne facilite pas sa tâche et peut être cause d'erreurs, d'oublis. Son intérêt réside donc dans la mise à disposition d'un système qui l'aiderait à gérer la multitude des informations qui lui sont nécessaires pour compléter le dossier médical du patient et établir son diagnostic d'une façon précise, rapide et fiable.

Un système téléinformatique pour la transmission des résultats d'analyses peut répondre à ces attentes pour ce qui concerne la rapidité et la fiabilité. De plus, les données ainsi transmises peuvent être récupérées par un système informatique de gestion de cabinet médical et intégrées dans le dossier médical du patient. La mise-à-jour du dossier médical est alors automatique et réduit ainsi le risque d'erreurs et d'oublis. Le médecin est ainsi libéré d'une

[1] Voir annexe 1

grande partie des opérations de gestion de ces informations et peut consacrer plus de temps et d'énergie à son rôle premier : soigner. Ajoutons encore la disponibilité potentielle d'un système automatique de remise des résultats qui serait opérationnel 24 heures sur 24 et 7 jours sur 7.

32. Le laboratoire d'analyses

Confronté à l'obligation de manipuler des volumes toujours plus importants d'informations, l'utilisation de la téléinformatique pour la transmission des résultats des analyses est une étape supplémentaire dans le processus d'automatisation de la gestion du laboratoire. Les avantages potentiels sont un nombre plus réduit de manipulations et une diminution des risques d'erreurs et d'oublis.

33. La protection du secret médical

Les résultats des analyses sont protégés par le secret médical. Ils ne peuvent donc être portés à la connaissance de tout un chacun. Or, les moyens employés pour protéger les résultats au cours de leur transmission sont souvent réduits et parfois même inexistants. Le plus sûr est la transmission directe entre le laboratoire et le médecin. Mais il est contraignant. Quant aux autres, passons les en revue :

La Poste

La protection des données est assurée par une simple enveloppe. Bien mince, mais voyons ce que prévoit le code pénal dans son article 460 :

"Quiconque sera convaincu d'avoir supprimé une lettre confiée à la Poste, ou de l'avoir ouverte pour en violer le secret, sera puni d'un emprisonnement de huit jours à un mois et d'une amende de 26 à 200 francs, ou d'une de ces peines seulement, sans préjudice des peines plus fortes, si le coupable est un fonctionnaire ou un agent du gouvernement ou de l'administration des postes."

Il faut encore prouver le délit. Or chacun sait combien il est facile d'ouvrir une enveloppe, d'en consulter le contenu, puis de la refermer sans que l'on s'aperçoive de rien.

Le transporteur privé

Les mêmes risques que par la Poste, peut-être moins importants s'il y a moins d'intermédiaires.

Le téléfax

Qu'est-ce que le téléfax, si ce n'est un système de photocopie à distance. Le chiffrement des données peut les protéger au cours de leur transmission. Mais à l'autre bout, elles devront apparaître en clair sur le papier. Reste à savoir qui récupère la photocopie de l'autre côté... Il n'existe aucun moyen de s'en assurer.

Le téléphone

Les problèmes inhérents à la communication vocale par le téléphone sont bien connus. Ce sont :

- L'identification et l'authentification des interlocuteurs. La RTT ne garantit pas que l'appel demandé aboutira bien à l'abonné identifié par le numéro formé. L'authentification repose alors sur la reconnaissance vocale mutuelle des interlocuteurs. Il suffit que l'un d'eux soit enrhumé pour mettre en faillite ce procédé.

- Les risques d'écoutes et d'interception des messages sont la plupart du temps incontrôlables.

- Les risques d'erreurs de lecture orale et de retranscription manuelle des résultats sont importants.

Le support informatique

Un support informatique, tel qu'une disquette, présente un avantage fondamental sur tous les autres moyens de transmission : l'information n'est pas présente en clair. Elle nécessite un dispositif de lecture adapté pour en permettre la consultation. De plus, on peut protéger cette information en la chiffrant, ce qui rend pratiquement impossible son utilisation par quelqu'un non autorisé. En outre, les résultats mis sous cette forme peuvent être récupérés par un système informatisé de gestion de cabinet médical.

En conclusion

Nous avons vu que, parmi les moyens de transmission les plus couramment utilisés, le plus sûr est le fichier sur support informatique. L'un des objets de la téléinformatique est la transmission de données, par exemple sous forme de fichiers. On remplace alors le support de stockage par un support de transmission et on pallie le risque de perte de la confidentialité et de l'intégrité par le chiffrement des données. De plus, la téléinformatique permet des méthodes d'identification et d'authentification des interlocuteurs beaucoup plus sûres que pour tous les autres moyens, excepté la transmission directe.

34. Les inconvénients

L'introduction de toute nouvelle technique implique non seulement des investissements pécuniaires, mais aussi en temps d'apprentissage et de formation. Si l'outil informatique est bien implanté dans les laboratoires, c'est loin d'être le cas chez les médecins, souvent réticents, car jaloux de leur liberté qu'ils craignent de voir se réduire s'ils sont astreints à de nouvelles obligations et pratiques.

Un autre problème est celui de l'absence de règles pour la transmission des résultats d'analyses par voie téléinformatique. En effet, il est plus que probable que, en raison du vide actuel, chaque laboratoire voudra proposer son propre système de transmission. Ce qui aura pour résultat la plus grande hétérogénéité matérielle et logicielle, et comme conséquence que le médecin, peu au courant de la chose informatique, s'en trouvera désorienté. Il est prévisible qu'alors son réflexe sera de faire confiance au laboratoire auquel il a l'habitude de s'adresser, laboratoire qui, gageons-le, s'empressera de lui fournir toute l'aide nécessaire pour lui permettre d'utiliser ses services. Et si plus tard, le médecin désire travailler avec un autre laboratoire, il devra s'adapter à un autre système de transmissions, remettant ainsi en cause les investissements précédemment réalisés.

On le voit, la liberté de choix du médecin et, par la même occasion, celle du patient, n'est pas garantie. Le risque d'apparition d'un monopole du laboratoire vis-à-vis du médecin est réel. Comment l'éviter ? Une seule solution : élaborer un système de transmission de faible coût pour garantir l'indépendance financière du médecin et définir les règles d'un protocole pour la transmission des résultats des analyses qui puisse être facilement implanté sur une grande variété de systèmes, pour garantir l'indépendance technique du médecin. C'est ce à quoi nous nous emploierons dans ce qui suit.

4. Définitions des objets

Les résultats des analyses

Les résultats des analyses sont constitués de séries de chiffres, de nombres, de textes standards et de commentaires libres. Ces résultats sont fournis sous forme de fichiers informatiques. Un fichier regroupe tous les comptes rendus, partiels ou complets, des analyses de tous les patients d'un seul médecin. On ne peut faire aucune hypothèse sur l'organisation des données. La taille moyenne d'un compte rendu est de 10000 octets, soit l'équivalent de 3 ou 4 feuilles dactylographiées de format A4. Le nombre de compte rendus par médecin est variable et dépend de la fréquence de transmission des résultats.

5. Spécifications des besoins fonctionnels

Une fonction correspond à un objectif et un comportement considérés comme élémentaires. Elle représente un échange indécomposable de messages entre l'utilisateur et le système, et effectue une action minimale et cohérente.

Le système comporte deux parties distinctes. Ce sont les fonctions à réaliser respectivement par le laboratoire et par le médecin. Cependant, comme chaque partie réalise les mêmes fonctions et que seule diffère leur implémentation, elles sont regroupées afin de ne pas compliquer inutilement leur description. Les fonctions à remplir concernent la gestion des informations relatives aux médecins et aux laboratoires, la protection des données confidentielles et la transmission des résultats d'analyses.

Nom	Objectif
Ajout-inter	Collecte et ajout des informations relatives à un interlocuteur.
Suppression-inter	Suppression des informations relatives à un interlocuteur.
Début-com	Etablir une communication avec un interlocuteur.
Fin-com	Couper une communication.
Identification	Identification des interlocuteurs mis en communication.
Authentification	Authentification des interlocuteurs mis en communication.
Protection-rés	Protection des résultats des analyses.
Transmission-rés	Transfert des résultats des analyses.

6. Spécifications des besoins non fonctionnels

Les besoins non fonctionnels représentent l'ensemble des contraintes que le système doit satisfaire. Sont reprises ici des contraintes déjà évoquées et de nouvelles, s'ajoutant aux précédentes.

Protection du secret médical

La règle du secret médical fait obligation que :

- Un médecin ne peut avoir accès aux résultats des analyses d'un patient d'un autre médecin.

- Un laboratoire ne peut avoir accès aux dossiers médicaux des patients d'un médecin.

- Les résultats des analyses doivent être protégés de toute violation au cours de leur transmission, qui menacerait leur intégrité et/ou leur confidentialité. Leur chiffrement est indispensable.

Une règle générale pour diminuer les menaces d'atteintes à la sécurité des données est que le nombre d'intermédiaires entre l'émetteur et le récepteur soit aussi réduit que possible. Un intermédiaire peut être une personne physique ou une organisation.

Le caractère standard

L'un des risques les plus importants dénoncés par l'Ordre des médecins est l'apparition d'un monopole du laboratoire qui pourrait être tenté de fidéliser sa clientèle en lui offrant, par exemple, un service original sur le plan technique.

Il est impérieux que le médecin prescripteur puisse s'adresser au laboratoire de son choix, sans que cela implique une remise en question des investissements qu'il a effectués. En d'autres termes, chaque laboratoire devrait fournir un service identiquement accessible par tous les utilisateurs potentiels. Cela implique l'obligation de définir des règles précises et communes de dialogue avec l'usager.

Le coût

Les coûts de mise en oeuvre et d'utilisation doivent être minimaux pour plusieurs raisons :

- Il s'agit d'éviter que seuls les laboratoires les mieux nantis puissent offrir ce service aux médecins prescripteurs. Cela leur permettrait d'ajouter un plus à leur image de marque et pourrait apparaître comme un moyen de fidélisation. On retombe sur le problème du monopole qui est fermement condamné par l'Ordre des médecins.

- D'autre part, le laboratoire, comme n'importe quelle entreprise, essaie de réduire ses coûts de fonctionnement. C'est d'ailleurs du laboratoire que vient la demande la plus pressante, car la mise en oeuvre d'un tel système lui permettrait d'automatiser encore plus sa gestion.

- Pour le médecin prescripteur, qu'il faut encore convaincre des avantages potentiels d'un tel changement de ses habitudes, le coût reste un élément déterminant pour l'adoption d'une solution qui nécessitera, non seulement un investissement pécuniaire, mais aussi un investissement en temps de formation à l'utilisation d'un nouvel outil.

Fiabilité de la transmission des données

Le système doit assurer une transmission fiable des données. En effet, les conséquences d'une interprétation erronée de données modifiées à la suite d'une transmission de mauvaise qualité pourraient être graves pour le patient concerné.

Résultats d'analyses et dossier médical

Les résultats des analyses doivent pouvoir être récupérés par le médecin et introduits dans un dossier médical informatisé. Il s'agit d'un élément fondamental qui interviendra surtout dans le choix d'un service de transmission. Ce sont des données qui sont transmises et qui doivent être récupérées et exploitées par un système informatisé, chez le médecin.

Ergonomie

Le système doit être simple à mettre en oeuvre et facile d'utilisation.

Tant pour le laboratoire que pour le médecin prescripteur, il ne doit occasionner qu'un minimum de travail lors de la phase d'introduction et, si possible, permettre un gain de temps par la suite.

Ce système s'adressant à des non-informaticiens, il doit présenter un caractère convivial indispensable, nécessitant un nombre réduit de manipulations et une interface utilisateur adaptée aux besoins.

Contraintes de performances

Aucune contrainte de performances n'est énoncée, car il s'agit d'une caractéristique propre à chaque laboratoire et médecin. Elle doit donc être évaluée au cas par cas.

Contraintes d'environnement

L'indépendance la plus grande possible vis-à-vis de l'environnement est requise pour garantir l'indépendance entre le médecin et le laboratoire et, par là, la notion de libre choix.

Conclusion

En conclusion, nous retiendrons les principes suivants : la plus grande liberté possible doit être laissée au médecin et les techniques mises en oeuvre doivent assurer une protection optimale des résultats d'analyses.

1. Le réseau et les appareils terminaux

Notre problème étant celui de la transmission de données, c'est parmi ces services que nous rechercherons une solution. Pour nous déterminer dans ce choix, nous allons passer en revue ces différents services et comparer leurs avantages et désavantages respectifs. Ce qui nous permettra de les répartir en deux groupes, selon qu'ils sont utilisables ou non, en fonction des critères énoncés plus haut.

11. Les services non utilisables

Le circuit d'abonnement

Le circuit d'abonnement permet de relier de façon permanente deux ou plusieurs interlocuteurs. Le médecin ne s'adressant à un laboratoire qu'occasionnellement et pour échanger des quantités réduites d'informations, cette caractéristique est parfaitement inutile. D'autre part, la permanence de la liaison entre le médecin et le laboratoire pourrait être perçue comme une incitation pour le médecin de ne s'adresser qu'à ce seul laboratoire. Ce qui est contraire à la notion de libre choix du médecin. Reste le coût d'un tel service : la redevance bimestrielle peut varier de 2000 à 50000 FB en fonction de la qualité demandée et de la distance à couvrir.

Le vidéotex

Le chiffrement produit des données dont il n'est, en principe, pas possible de prévoir la nature à l'avance. Or, le vidéotex ne permet pas la transmission de données quelconques, celles-ci pouvant perturber le bon déroulement des échanges. En conséquence, il est impossible d'assurer une protection efficace des résultats des analyses lors de leur transmission.

12. Les services utilisables

Les services utilisables sont ainsi réduits au nombre de deux : DCS et Datel. Les avantages de DCS sont ceux d'un service spécifiquement dédié à la transmission de données et normalisé. Comme inconvénients, on peut relever la nécessité de souscrire un abonnement et le coût plus élevé que Datel. Et c'est, en définitive, ce dernier critère qui nous permettra de choisir. Selon une étude menée par P. Bielande en 1988, il ressort que "le RTC apparaît comme un moyen très économique pour effectuer du transfert de fichiers. (...) Le réseau DCS, que la RTT défend plus particulièrement, ne soutient que rarement la comparaison avec le RTC, sauf lors de communications en interzonal à 2400 bps." Ces observations sont toujours d'actualité. En conséquence, notre choix se porte sur Datel.

Nota bene

Le lecteur trouvera en annexe une comparaison des tarifs de DCS et de Datel.

13. Choix des ETTD et ETCD

Le choix d'un ETTD est fonction des besoins de l'utilisateur en matière de capacités de traitement et de stockage de l'information. Quant au choix d'un ETCD, il est dicté par la nature du support de transmission et l'obligation d'être compatible avec celui de l'ETTD du système auquel on veut se connecter.

Le médecin

L'ETTD type est un micro-ordinateur pourvu d'une interface série sur laquelle pourra se connecter l'ETCD. L'ETCD est un modem capable de fonctionner sur le réseau téléphonique commuté. Nous conseillons un modem conforme à l'avis V23 du CCITT. Nous en verrons plus loin les raisons.

Le laboratoire

Pour des raisons de sécurité, il est préférable que L'ETTD responsable de la transmission des résultats des analyses constitue un système indépendant du système chargé de la gestion du laboratoire. La raison est que ce dernier ne puisse devenir la cible d'attaques extérieures via le premier cité.

Le choix d'un ETTD pour le laboratoire ne peut être défini à priori, chaque laboratoire constituant un cas particulier pour ce qui concerne les besoins en matière de capacité de traitement et de stockage de l'information. Le rôle de cet ETTD peut, par exemple, être tenu par un micro-ordinateur, tout comme chez le médecin. Il existe actuellement sur le marché des micro-ordinateurs aux performances de minis. Quant à l'ETCD, il s'agit d'un modem capable de fonctionner sur le réseau téléphonique et compatible avec celui du médecin.

La carte à microprocesseur

Peut-on envisager l'utilisation de la carte à microprocesseur ? Certainement. Cependant, à ce stade nous ne le ferons pas, pour des raisons pratiques. L'utilisation de la carte à microprocesseur nécessite un investissement de départ que nous n'avons pas jugé utile de faire. Nous indiquerons plus loin des pistes qui permettront de l'incorporer ultérieurement au système.

2. Le logiciel

21. Choix et contraintes

La protection des données et la gestion des transmissions sont assurées par logiciel. Pour cette raison, notre choix se portera sur les solutions les plus simples à implémenter, pour autant qu'elles respectent les critères énoncés plus haut.

211. L'algorithme de chiffrement

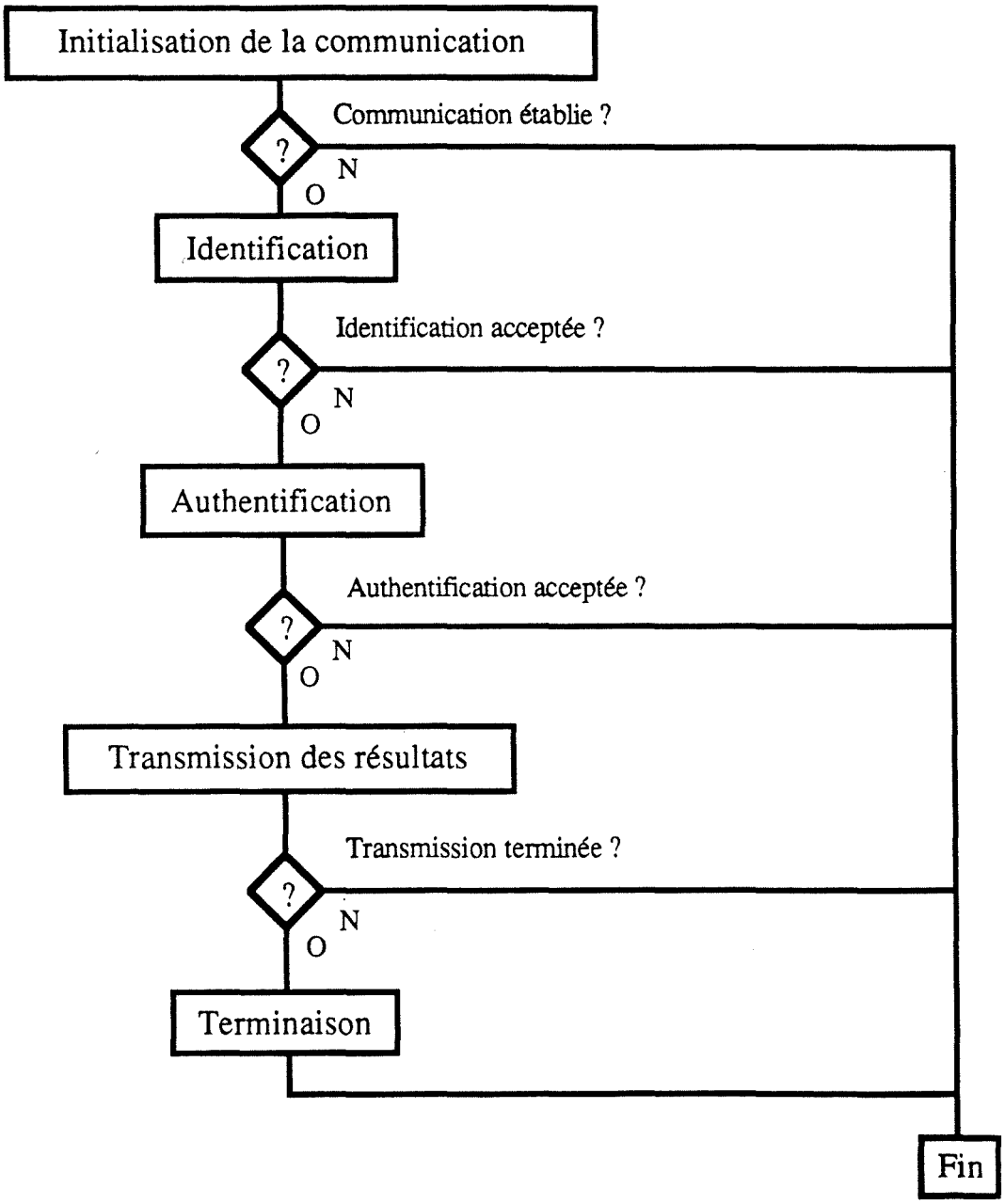
L'algorithme de chiffrement-déchiffrement utilisé est le DES. Ce choix est dicté par le souci d'adopter un standard reconnu, qui ait fait ses preuves, qui soit simple à implémenter et rapide à l'exécution.

212. Le protocole de communication

Le protocole de communication utilisé est un protocole original. Une des raisons de ce choix est l'adaptation à des besoins spécifiques, comme nous le verrons lors de sa description détaillée, dans la partie implémentation.

22. Déroulement d'une communication type

Le déroulement d'une communication type recouvre les étapes suivantes, par ordre chronologique : initialisation de la communication, identification et authentification des interlocuteurs, transmission des résultats des analyses, terminaison de la communication.



Initialisation de la communication

L'initiative de l'appel revient au médecin. Ce choix est dicté par des raisons pratiques qui veulent que le médecin reste libre de faire appel aux services du laboratoire quand il le désire, sans être tenu par des obligations incompatibles avec la nature de ses occupations, qui induisent souvent des horaires irréguliers. Cela présente cependant l'inconvénient que le médecin n'est pas certain d'obtenir les résultats, si ceux-ci ne sont pas prêts. Le médecin peut alors convenir avec le laboratoire d'une heure à partir de laquelle les résultats seront disponibles.

Identification des interlocuteurs

Le laboratoire est déjà identifié puisque c'est le médecin qui a pris l'initiative de l'appel. Quant au médecin, il doit présenter un code d'identification permettant au laboratoire de le reconnaître.

Authentification des interlocuteurs

Une fois les interlocuteurs identifiés, il s'agit de vérifier l'authenticité de leurs identités respectives. Cette étape est rendue nécessaire par le fait que l'on ne peut être certain des identités des interlocuteurs, après leurs identifications respectives. En effet, d'une part, la RTT ne garantit pas que l'appel téléphonique demandé aboutira chez le bon destinataire, et, d'autre part, le code d'identification présenté par le médecin n'est pas protégé d'une éventuelle écoute lors de sa transmission. Une réutilisation frauduleuse est donc possible. Ces risques sont palliés par le mécanisme du code d'authentification qui sera décrit plus loin.

Transmission des résultats d'analyses

Tous les résultats sont transmis en une seule fois. Cela est rendu obligatoire par le fait que tous les résultats de toutes les analyses demandées par un médecin pour ses patients sont contenus dans un seul fichier, et que l'on ne peut faire aucune hypothèse sur l'organisation de ces données. Ce qui enlève la possibilité d'aller rechercher l'un ou l'autre résultat. La transmission concerne donc les données et la structure du fichier. Le contenu du fichier doit être chiffré avant transmission et déchiffré après.

Remarque.

Ces résultats n'étant intéressants que parce qu'ils sont nominatifs, on pourrait ne chiffrer que les noms des patients. Cependant cela impliquerait de connaître l'organisation des données du fichier des résultats. Or, on ne peut faire aucune hypothèse sur cette organisation. D'autre part, si les résultats étaient transmis en clair, à l'exception des noms, des recoupements seraient toujours possibles et représenteraient une menace pour le secret médical.

Terminaison de la communication

La transmission des résultats des analyses étant parachevée, la communication est coupée.

Messages échangés

Le déroulement d'une communication type peut être illustrée par les échanges de messages entre le médecin et le laboratoire, comme indiqué sur le schéma suivant. Par ordre chronologique :

Origine	Nature	Destination
médecin	initialisation	laboratoire
médecin	code d'identification	laboratoire
médecin	question du médecin	laboratoire
laboratoire	réponse du laboratoire	médecin
laboratoire	question du laboratoire	médecin
médecin	réponse du médecin	laboratoire
laboratoire	résultats des analyses	médecin
laboratoire	terminaison	médecin

23. Les informations relatives aux interlocuteurs

On désigne sous le terme "interlocuteur" le médecin ou le laboratoire. Ces informations sont celles qu'il est nécessaire de connaître pour mener à terme la transmission des résultats d'analyses, selon la méthode exposée.

Le nom de l'interlocuteur

Pour pouvoir reconnaître un interlocuteur, il faut lui donner un nom qui permette de l'identifier parmi les autres. Ainsi, le médecin doit donner un nom à chacun des laboratoires avec lesquels il est en relation, et vice-versa.

Le code d'identification

Le code d'identification permet l'identification du médecin par le laboratoire. Il doit être présenté par le médecin dès que la communication est établie. Le code d'identification est fourni par le laboratoire et ne doit identifier qu'un seul médecin par rapport au laboratoire. Le code d'identification est en fait le nom que le laboratoire donne au médecin.

La clé de transmission

Il s'agit de la clé utilisée pour le chiffrement-déchiffrement des résultats des analyses et pour l'étape d'authentification. Elle est fournie par le laboratoire qui la génère de façon aléatoire et la remet directement au médecin. Elle doit être unique pour chaque liaison entre le laboratoire et un médecin. Il s'agit d'un élément essentiel pour la protection des résultats des analyses. Cela signifie qu'elle ne peut pas être accessible à d'autres personnes que le médecin et les membres autorisés du laboratoire. Nous verrons plus loin comment sa protection est assurée.

Le numéro d'appel

Les numéros d'appels du laboratoire et du médecin doivent, si possible, être tenus secrets. Cela signifie ne pas figurer au bottin téléphonique et ne pas être accessibles à d'autres personnes que le médecin et les membres autorisés du laboratoire. Nous verrons plus loin comment cette protection est assurée.

24. Protection des données

Voyons maintenant comment assurer la protection des informations confidentielles relatives aux interlocuteurs, des résultats des analyses et de l'accès à l'application.

La clé personnelle

Cette clé est appelée ainsi car elle est utilisée par le médecin et le laboratoire pour leurs usages propres. Elle est générée par son utilisateur et connue de lui seul. Elle conditionne l'accès à l'application qui en demande la présentation au début de chaque session de travail. Elle sert aussi pour le chiffrement des numéros d'appels et des clés de transmissions préalablement à leurs stockages. Elle ne peut être conservée en clair par l'application. Elle est donc chiffrée par elle-même et conservée sous cette forme.

Le contrôle d'accès à l'application

Le contrôle d'accès à l'application est réalisé de la façon suivante : l'application demande à l'utilisateur de présenter sa clé personnelle. Celle-ci est chiffrée par elle-même et le résultat est comparé avec la clé personnelle connue de l'application sous sa forme chiffrée, comme ci-dessus.

Le code d'authentification

Le mécanisme du code d'authentification doit permettre de vérifier les identités respectives du médecin et du laboratoire. Cette authentification est basée sur un mot de passe obtenu par dérivation. Le principe est que chaque interlocuteur pose une question à laquelle seul l'autre interlocuteur est capable de répondre. La réponse constitue le mot de passe. La méthode de dérivation fait appel à un algorithme de chiffrement, à une information secrète et à une autre non secrète.

L'algorithme de chiffrement est le DES, l'information secrète est la clé de transmission commune au laboratoire et au médecin, et l'information non secrète est une chaîne de caractères quelconques : le code d'authentification.

Chaque interlocuteur génère un code d'authentification qu'il demande à l'autre de chiffrer à l'aide de la clé de transmission. Il compare les résultats obtenus par lui-même et par l'autre. S'ils sont identiques, l'authentification est réalisée. Le code d'authentification doit être différent lors de chaque communication, afin d'éviter sa réutilisation par un imposteur. L'élément authentifiant est donc la clé de transmission. Celle-ci ne circule pas sur le réseau, à la différence du code d'identification qui, lui, circule en clair, et ne peut donc être considéré comme une information confidentielle.

La protection des résultats des analyses

Si les résultats des analyses doivent être conservés sur un support, dans l'attente de leur émission, ils doivent être préalablement chiffrés. Cette condition assure qu'aucune personne non autorisée ne pourra en prendre connaissance avant leur émission. Après avoir été émis, ils doivent être effacés du support. Cette condition permet qu'ils ne soient transmis qu'une seule fois. Si un imposteur a pu obtenir leur émission, la fraude sera détectée car le médecin autorisé ne recevra rien. Il devra alors avertir le laboratoire et prendre avec lui les mesures qui s'imposent : changement de la clé de transmission, de la clé personnelle et, si possible, du numéro d'appel du laboratoire. La ligne de transmission doit aussi être vérifiée pour détecter d'éventuelles dérivations et écoutes.

25. Conception globale du logiciel[1]

La conception globale du logiciel a pour but l'élaboration d'une structure pour le logiciel. Toute structure est faite de composants et de relations qui lient ces composants.

Les composants (modules) comprennent différents traitements (modules de traitements) et structures de données (modules de données) qui réalisent les fonctions et les objets identifiés au cours de l'analyse fonctionnelle.

Les relations permettent d'organiser les composants en niveaux distincts et ordonnés. On définit ainsi une structure hiérarchique pour le système. Cette structure est appellée "architecture logique".

Pour le cas qui nous concerne, l'architecture logique est identique pour les deux sous-systèmes localisés chez le médecin et le laboratoire. Seules les implémentations différeront en fonction des besoins propres.

251. Architecture logique

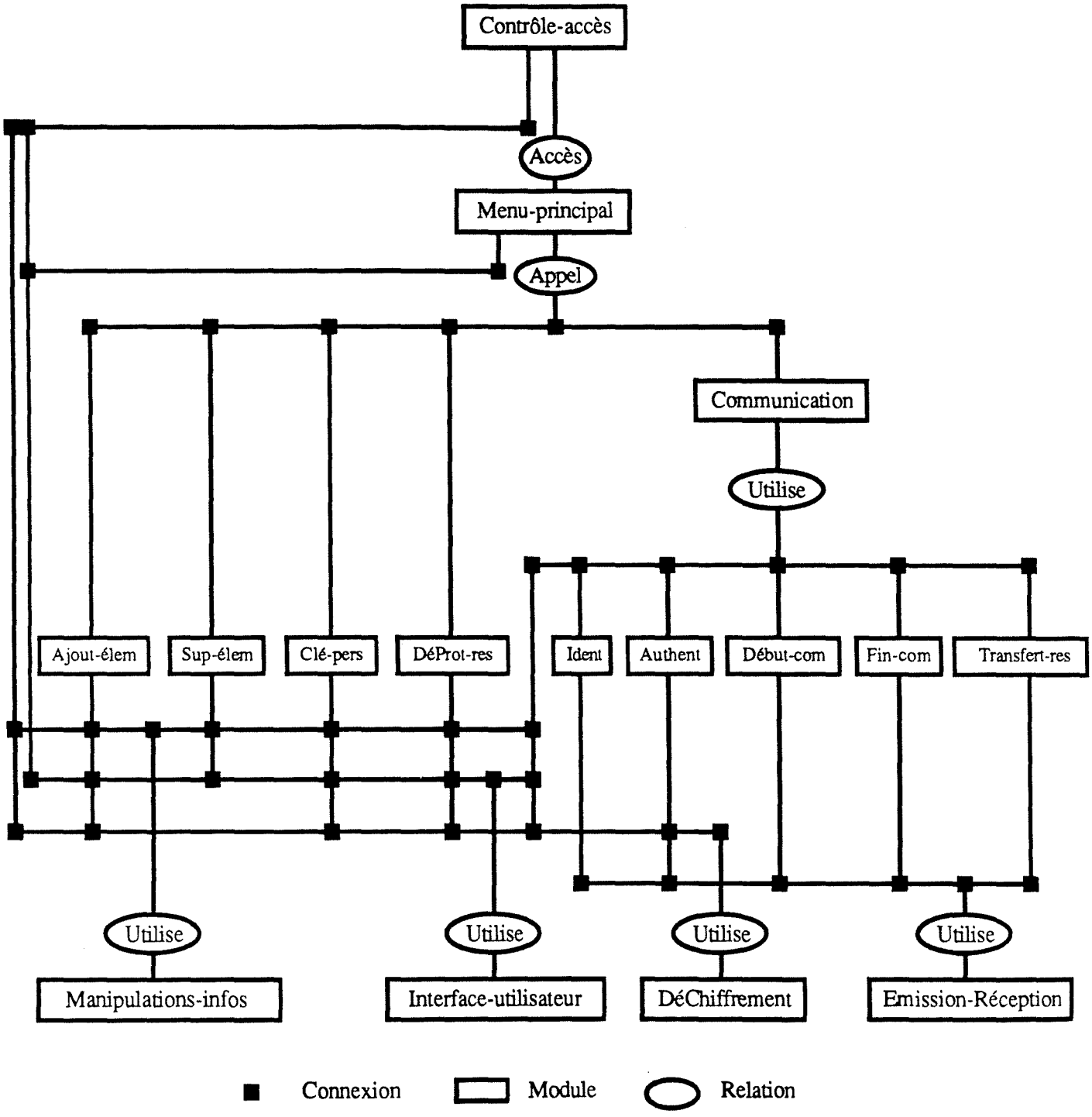
Les composants sont organisés en cinq niveaux distincts, numérotés de 1 à 5, en partant du sommet. Les fonctions réalisées par des composants regroupés sur un même niveau attribuent un rôle spécifique au niveau.

Le niveau 1 contrôle l'accès à l'application. Le niveau 2 est un niveau de branchement vers les différentes fonctions du système. Le niveau 3 est celui des fonctions de haut niveau. Le niveau 4 comprend les fonctions définies au cours de l'analyse fonctionnelle. Le niveau 5 regroupe les fonctions auxiliaires, constituant ainsi une sorte de boîte à outils.

L'architecture est illustrée par le schéma suivant, dont les relations et les composants sont définis par la suite.

[1] Partie plus spécifiquement destinée aux informaticiens

Conception globale du système



Nom	Nature	Relation appliquée	Niveau
Contrôle-accès	Traitement	-	1
Menu-principal	Traitement	Accès	2
Communication	Traitement	Appel	3
Ajout-élem	Traitement	Appel	4
Sup-élem	Traitement	Appel	4
Clé-pers	Traitement	Appel	4
DéProt-res	Traitement	Appel	4
Identification	Traitement	Utilise	4
Authentification	Traitement	Utilise	4
Début-com	Traitement	Utilise	4
Fin-com	Traitement	Utilise	4
Transfert-res	Traitement	Utilise	4
Manipulations-infos	Données	Utilise	5
Interface-utilisateur	Traitement	Utilise	5
DéChiffrement	Traitement	Utilise	5
Emission-réception	Traitement	Utilise	5

Relation Accès

Soit R(A,B), une relation binaire définie sur les modules A et B, telle que "A est accessible de B". On obtient ainsi un système à haut degré de sécurité/protection, car en introduisant cette relation dans une structure hiérarchique, on restreint les accès (Van Lamsweerde, Méthodologie de développement de logiciels).

Relation Appel

Soit R(A,B), une relation binaire définie sur les modules A et B, telle que "A appelle B". L'exécution de B est déclenchée par A. A et B s'exécutent indépendamment l'un de l'autre (Van Lamsweerde, Méthodologie de développement de logiciels).

Relation Utilise

Soit R(A,B), une relation binaire définie sur les modules A et B, telle que "A utilise B". La validité de A dépend de la disponibilité d'une version correcte de B (Van Lamsweerde, Méthodologie de développement de logiciels).

252. Spécifications externes des modules

La spécification externe d'un module définit ce que fait le module, mais pas comment il le fait.

La méthode employée est celle de la spécification par assertions. Cette technique consiste à expliciter pour chaque module et pour chaque opération ses arguments, ses résultats, leurs types et propriétés par une paire d'assertions : préconditions sur les arguments et postconditions sur les résultats. On définit, s'il y a lieu, les concepts auxiliaires auxquels le module fait référence et les relations entre ces modules et les modules cibles des relations.

Les spécifications externes sont données à titre d'aide à l'implémentation. Leur caractère général vise à laisser la plus grande liberté possible de choix à l'implémenteur.

Donnée partagée

La clé personnelle est une donnée partagée entre toutes les fonctions qui l'utilisent. Elle est disponible sous le nom de CléPers.

1. Contrôle-accès

Description.
Cette fonction permet de filtrer les accès à l'application.
Argument.
- Clé : une chaîne de caractères.

Précondition.
- Clé représente la clé personnelle.

Résultat.
- Code : un chiffre.

Postcondition.
- Code indique la façon dont s'est déroulée l'opération.
- Si la clé introduite est la bonne, CléPers est identique à Clé.
- Si l'application ne connaît pas encore de clé personnelle, Clé devient la clé personnelle.

Concepts auxiliaires.
- L'accès est autorisé si Clé correspond à la clé personnelle chiffrée par elle-même à l'aide du DES.
- L'argument est demandé par la fonction à l'utilisateur.

2. Menu principal

Description.
Cette fonction permet l'accès aux fonctions du système.
Argument.
- NomFonc : une chaîne de caractères.

Précondition.
- NomFonc représente le nom d'une fonction.

Postcondition.
- La fonction identifiée par NomFonc activée. Une alternative doit permettre de terminer la session de travail en cours.

Concept auxiliaire.
- L'argument est demandé par la fonction à l'utilisateur.

3. Communication

Description.
Cette fonction recouvre les différents aspects liés à la transmission des résultats d'analyses : établissement et rupture de la communication, identification et authentification des interlocuteurs et la transmission des résultats, proprement dite.
Argument.
- NomInter : une chaîne de caractères.

Précondition.
- NomInter identifie un interlocuteur connu.

Résultat.
- Code : un chiffre.

Postcondition.
- Code indique la façon dont s'est déroulée l'opération.

Concept auxiliaire.
- L'argument est demandé par la fonction à l'utilisateur.

4. Ajout-élem

Description.

Cette fonction réalise la collecte et l'ajout des informations relatives à un interlocuteur.

Arguments.

- NomInter : une chaîne de caractères.
- CodeIdent : une chaîne de caractères.
- NoTel : une chaîne de caractères.
- CléTrans : une chaîne de caractères.

Préconditions.

- NomInter représente le nom de l'interlocuteur, CodeIdent son code d'identification, NoTel son numéro d'appel et CléTrans la clé de transmission.
- NomInter, CodeIdent, NoTel et CléTrans sont tous identifiants d'un interlocuteur.

Résultat.

- Code : un chiffre.

Postconditions.

- Code indique la façon dont s'est déroulée l'opération.
- NoTel et CléTrans doivent avoir été chiffrés à l'aide de la clé personnelle, préalablement à leur stockage.

Concept auxiliaire.

- Les arguments sont demandés par la fonction à l'utilisateur.

5. Sup-élem

Description.

Cette fonction réalise la suppression des informations relatives à un interlocuteur.

Argument.

- NomInter : une chaîne de caractères.

Précondition.

- NomInter représente le nom d'un interlocuteur.

Résultat.

- Code : un chiffre.

Postcondition.

- Code indique la façon dont s'est déroulée l'opération.

Concept auxiliaire.

- L'argument est demandé par la fonction à l'utilisateur.

6. Clé-pers

Description.

Cette fonction permet de changer la clé personnelle et donc de modifier en conséquence le chiffrement des numéros d'appels et des clés de transmissions.

Argument.

- NlleCléPers : une chaîne de caractères.

Précondition.

- NlleCléPers représente la nouvelle clé personnelle.

Postcondition.

- La clé personnelle est changée et le chiffrement des numéros d'appel et des clés de transmissions a été modifié en conséquence.

Concept auxiliaire.

- L'argument est demandé par la fonction à l'utilisateur.

7. DéProt-res

Description.

Cette fonction permet de chiffrer ou de déchiffrer le contenu du fichier contenant les résultats des analyses.

Arguments.

- NomFich : une chaîne de caractères.
- CléCD : une chaîne de caractères.
- ChiDec : un caractère.

Préconditions.

- NomFich représente le nom d'un fichier existant.
- CléCD représente la clé utilisée pour l'opération.
- ChiDec indique s'il s'agit d'un chiffrement ou d'un déchiffrement.

Postcondition.

- Le contenu du fichier désigné par NomFich a été chiffré ou déchiffré, selon l'opération indiquée par ChiDec.

Concept auxiliaire.

- Les arguments sont demandés par la fonction à l'utilisateur.

8. Début-com

Description.

Cette fonction permet d'établir une communication avec un interlocuteur.

Argument.

- NoTel : une chaîne de caractères.

Précondition.

- NoTel représente le numéro d'appel de l'interlocuteur avec lequel on souhaite établir une communication.

Résultat.

- Code : un chiffre.

Postcondition.

- Code indique la façon dont s'est déroulée l'opération.

9. Fin-com

Description.

Cette fonction permet de couper une communication.

Postcondition.

- La communication est coupée.

10. Identification

Description.

Cette fonction réalise l'identification du médecin. Les implémentations chez le médecin et le laboratoire seront différentes, selon le mécanisme explicité plus haut.

Argument.

- CodeIdent : une chaîne de caractères.

Préconditions.

- CodeIdent représente le code d'identification du médecin.
- La communication doit avoir été préalablement établie entre les interlocuteurs.

Résultat.

- Code : un chiffre.

Postcondition.

- Code indique la façon dont s'est déroulée l'opération.

11. Authentification

Description.

Cette fonction permet de vérifier l'authenticité des identités du laboratoire et du médecin. Les implémentations chez le médecin et le laboratoire seront différentes, selon le mécanisme explicité plus haut.

Argument.

- CléTrans : une chaîne de caractères.

Préconditions.

- CléTrans représente la clé de transmission associée au code d'identification présenté.
- L'étape d'identification doit s'être préalablement déroulée avec succès.

Résultat.

- Code : un chiffre.

Postcondition.

- Code indique la façon dont s'est déroulée l'opération.

12. Transfert-res

Description.

Cette fonction assure le transfert des résultats d'analyses entre le laboratoire et le médecin. Les implémentations chez le médecin et le laboratoire seront différentes, selon le mécanisme explicité plus haut.

Argument.

- NomFich : une chaîne de caractères.

Préconditions.

- NomFich représente le nom du fichier contenant les résultats des analyses à transférer.
- Les résultats d'analyses ont été préalablement chiffrés à l'aide de la clé de transmission commune aux interlocuteurs.
- L'étape d'authentification doit s'être préalablement déroulée avec succès.

Résultat.

- Code : un chiffre.

Postcondition.

- Code indique la façon dont s'est déroulée l'opération.

13. Manipulations-infos

Description.

Il s'agit d'un module données qui permet de gérer la clé personnelle et les informations relatives aux interlocuteurs, grâce à un certain nombre de fonctions détaillées ci-après.

Informations relatives à un interlocuteur

- NomInter : une chaîne de caractères.
- CodeIdent : une chaîne de caractères.
- NoTel : une chaîne de caractères.
- CléTrans : une chaîne de caractères.

Conditions

- NomInter représente le nom de l'interlocuteur, CodeIdent son code d'identification, NoTel son numéro d'appel et CléTrans la clé de transmission.
- NomInter, CodeIdent, NoTel et CléTrans sont tous identifiants d'un interlocuteur.

131. Fonction Ajout

Description.

Cette fonction réalise l'ajout des informations relatives à un interlocuteur.

Arguments.

- NomInter : une chaîne de caractères.
- CodeIdent : une chaîne de caractères.
- NoTel : une chaîne de caractères.
- CléTrans : une chaîne de caractères.

Préconditions.

- NomInter représente le nom de l'interlocuteur, CodeIdent son code d'identification, NoTel son numéro d'appel et CléTrans la clé de transmission.
- NomInter, CodeIdent, NoTel et CléTrans sont tous identifiants d'un interlocuteur.
- L'interlocuteur n'est pas connu.

Résultat.
- Code : un chiffre.

Postcondition.
- Code indique la façon dont s'est déroulée l'opération.

132. Fonction Suppression

Description.
Cette fonction réalise la suppression des informations relatives à un interlocuteur.

Argument.
- NomInter : une chaîne de caractères.

Précondition.
- NomInter représente le nom d'un interlocuteur connu.

Résultat.
- Code : un chiffre.

Postcondition.
- Code indique la façon dont s'est déroulée l'opération.

133. Fonction ExistenceNom

Description.
Cette fonction permet de vérifier l'existence d'un interlocuteur identifié par son nom et d'obtenir l'ensemble des informations qui lui sont reliées.

Argument.
- NomInter : une chaîne de caractères.

Précondition.
- NomInter représente le nom d'un interlocuteur.

Résultats.
- Code : un chiffre.
- NomInter : une chaîne de caractères.
- CodeIdent : une chaîne de caractères.
- NoTel : une chaîne de caractères.
- CléTrans : une chaîne de caractères.

Postconditions.
- Code indique la façon dont s'est déroulée l'opération.
- NomInter représente le nom de l'interlocuteur, CodeIdent son code d'identification, NoTel son numéro d'appel et CléTrans la clé de transmission.

134. Fonction ExistenceCodeIdent

Description.

Cette fonction permet de vérifier l'existence d'un interlocuteur identifié par son code d'identification et d'obtenir l'ensemble des informations qui lui sont reliées.

Argument.

- CodeIdent : une chaîne de caractères.

Précondition.

- CodeIdent représente le code d'identification d'un interlocuteur connu.

Résultats.

- Code : un chiffre.
- NomInter : une chaîne de caractères.
- CodeIdent : une chaîne de caractères.
- NoTel : une chaîne de caractères.
- CléTrans : une chaîne de caractères.

Postconditions.

- Code indique la façon dont s'est déroulée l'opération.
- NomInter représente le nom de l'interlocuteur, CodeIdent son code d'identification, NoTel son numéro d'appel et CléTrans la clé de transmission.

135. Fonction ListeInter

Description.

Cette fonction permet d'obtenir la liste des noms des interlocuteurs connus.

Résultat.

- La liste des noms des interlocuteurs connus est fournie.

Postcondition.

- Les noms des interlocuteurs sont classés par ordre alphabétique.

136. Fonction LireCléPers

Description.

Cette fonction permet de connaître la clé personnelle utilisée par l'application.

Résultat.

- CléPers : une chaîne de caractères.

Postcondition.

- CléPers représente la clé personnelle chiffrée par elle-même.

137. Fonction EcritureCléPers

Description.
Cette fonction permet la conservation par l'application de la clé personnelle.
Argument.
- CléPers : une chaîne de caractères.

Précondition.
- CléPers représente la clé personnelle chiffrée par elle-même.

Postcondition.
- CléPers est conservée par l'application.

14. Interface-utilisateur

Description.
Ce module regroupe les fonctions permettant le dialogue entre l'utilisateur et l'application. Ces fonctions sont détaillées ci-après.

141. Fonction EffaceEcran

Description.
Cette fonction permet d'effacer le contenu de l'écran.
Postconditions.
- L'écran est effacé.
- Le curseur est positionné dans le coin supérieur gauche.

142. Fonction Ecrit

Description.
Cette fonction permet d'afficher un texte à l'écran.
Argument.
- Texte : une chaîne de caractères.

Postcondition.
- Texte est affiché à l'écran, à partir de la position du curseur, dans le sens gauche-droite et haut-bas.

143. Fonction Demande

Description.

Cette fonction permet à l'utilisateur de fournir une information à l'application.

Résultat.

- Texte : suivant le type de l'information demandée.

Postcondition.

- Texte est du type spécifié.

144. Fonction Curseur

Description.

Cette fonction permet de déplacer le curseur à un endroit déterminé sur l'écran.

Arguments.

- Ligne : un nombre entier positif.
- Colonne : un nombre entier positif.

Préconditions.

- Ligne indique le numéro de la ligne de la nouvelle position du curseur. Les lignes sont numérotées à partir de 1 du haut vers le bas, avec incrément de 1.
- Colonne indique le numéro de la colonne de la nouvelle position du curseur. Les colonnes sont numérotées à partir de 1 de gauche à droite, avec incrément de 1.

Postcondition.

- Le curseur est positionné à l'endroit indiqué par Ligne et Colonne.

15. DéChiffrement

Description.

Cette fonction permet de chiffrer ou de déchiffrer un texte.

Arguments.

- Texte : une chaîne de caractères.
- CléCD : une chaîne de caractères.
- ChiDec : un caractère.

Préconditions.

- Texte représente le texte à chiffrer ou à déchiffrer.
- CléCD représente la clé de chiffrement ou de déchiffrement.
- ChiDec indique s'il s'agit d'un chiffrement ou d'un déchiffrement.

Résultat.
- Texte : une chaîne de caractères.

Postcondition.
- Texte représente le texte chiffré ou déchiffré.

16. Emission-Réception

Description.
Ce module regroupe les fonctions de commandes de l'ETCD et de transmissions de données. Ces fonctions sont détaillées ci-après.

161. Fonction Commande

Description.
Cette fonction permet d'émettre des commandes vers l'ETCD.

Argument.
- Texte : une chaîne de caractères.

Précondition.
- Texte représente les commandes à émettre vers l'ETCD.

Résultat.
- Code : un chiffre.

Postcondition.
- Code indique la façon dont s'est déroulée l'opération.

162. Fonction Emission

Description.
Cette fonction permet l'émission de caractères selon le protocole utilisé.

Argument.
- Texte : une chaîne de caractères.

Précondition.
- Texte représente les caractères à émettre.

Résultat.
- Code : un chiffre.

Postcondition.
- Code indique la façon dont s'est déroulée l'opération.

163. Fonction Réception

Description.

Cette fonction permet la réception de caractères selon le protocole utilisé.

Résultats.

- Code : un chiffre.
- Texte : une chaîne de caractères.

Postconditions.

- Code indique la façon dont s'est déroulée l'opération.
- Texte représente les caractères reçus.

3. Critiques et perspectives

31. ETTD et ETCD

Le choix d'un micro-ordinateur comme ETTD est justifié par la nécessité de disposer d'une puissance de traitement et de capacités de stockage de l'information. Ce choix présente en outre des avantages certains. Les nombreuses et diverses utilisations potentielles en font un outil polyvalent : traitement de texte, tableur, gestion de bases de données et dessin en sont les exemples les plus classiques. Il rend parfaitement réalisable l'accès à des banques de données médicales pour l'aide au diagnostic. Cette demande est souvent exprimée par les médecins. Tout cela apporte des garanties pour la rentabilité de l'investissement.

Comme ETCD, nous avons conseillé le choix d'un modem conforme à l'avis V23 du CCITT. Nous en avons indiqué la raison principale qui est de définir un standard afin de permettre la connexion du laboratoire et du médecin. Ce choix est aussi fait dans la prévision d'une utilisation possible du réseau vidéotex, à partir d'un micro-ordinateur émulant un terminal compatible avec le réseau. Comme inconvénient, on peut relever la faible vitesse de transmission. Mais, comme les quantités de données à transférer sont peu importantes en moyenne, cela ne devrait représenter une limitation que dans de rares cas.

Le choix des ETTD et ETCD offre ainsi des garanties d'évolution en douceur du système au niveau matériel. De plus, la baisse constante des prix du matériel et des logiciels permet leur diffusion dans un public de plus en plus large.

32. Les informations relatives aux interlocuteurs

La solution "tout logiciel" pour assurer la sécurité des données pose un certain nombre de problèmes. En effet, les données confidentielles telles que les numéros d'appels et les clés de transmissions sont conservées dans des fichiers qu'il est difficile de protéger des attaques extérieures. Les données contenues dans ces fichiers ne devraient pouvoir être gérées que via l'application qui, elle-même, ne devrait pas être modifiable par une personne non autorisée (entendez "non dépourvue de mauvaises intentions"). La protection de l'application et de ses fichiers de travail peut être assurée par divers moyens logiciels et matériels existant sur le marché.

Cependant, à défaut de pouvoir protéger efficacement le contenant, on peut essayer de rendre le contenu inutilisable en cas d'attaque : c'est pourquoi les données essentielles comme les numéros d'appels et les clés de transmissions sont chiffrées pour leur conservation. C'est le rôle de la clé personnelle. D'où l'importance que celle-ci soit tenue secrète. La conservation de ce secret repose, d'une part, sur la discrétion de son utilisateur et, d'autre part, sur la protection de l'application qui pourrait être modifiée de telle sorte que la sécurité des données soit menacée. On constate donc que si on a rajouté un niveau supplémentaire de sécurité, on n'a pas résolu le problème de la protection de l'application.

Alors, que faire ? L'idéal serait d'avoir un support inviolable pour conserver les données confidentielles. Ce qui résoudrait du même coup le problème de la protection de l'application elle-même. En attendant, on peut toujours conserver l'application et les données confidentielles sur une disquette que l'on enfermera dans un coffre-fort pour ne l'en sortir que si nécessaire !

33. La carte à microprocesseur

En réponse au problème de la conservation des informations confidentielles sur un support inviolable, la carte à microprocesseur semble être la meilleure candidate pour cette fonction.

Nous avons déjà évoqué la raison qui nous a amené à postposer son utilisation. L'absence actuelle d'un protocole standard pour les transmissions des résultats d'analyses rend aléatoire tout investissement dans un procédé quelconque, celui-ci risquant d'être remis en cause à tout moment.

D'autre part, nous pensons que l'utilisation de la carte à microprocesseur devrait être considérée dans un cadre plus large que la seule transmission des résultats des analyses. Diverses expériences ont été et sont toujours menées pour étudier les possibilités d'utilisation de la carte à microprocesseur comme support d'un RCM (**R**ésumé **C**linique **M**inimum). Cette carte, appellée biocarte, serait conservée par le patient et contiendrait les données essentielles de son dossier médical. Le médecin posséderait sa propre carte qui définirait ses droits d'accès aux informations contenues dans la carte du patient. Pourquoi ne pas essayer de combiner les deux cartes du médecin pour n'en avoir qu'une qui regrouperait les fonctions et informations nécessaires à la mise-à-jour du RCM et à la transmission des résultats des analyses ? Une réponse à ces deux problèmes permettrait d'éviter une multiplication anarchique des procédés de transmission des résultats et des cartes.

Un autre avantage serait le passage d'une authentification par mot de passe à une authentification par badge, plus sécurisante. De plus, l'intérêt du système proposé est de permettre l'introduction de la carte à microprocesseur chez le médecin et le laboratoire, indépendamment l'un de l'autre. Ce qui garantit une grande souplesse d'évolution du système.

34. Les télécommunications

L'intérêt d'un système de télécommunications standard, accepté par tous, assurant une qualité de service optimale, aussi polyvalent que possible et de faible coût a été souligné. Les avantages et désavantages des différents services actuellement disponibles ont été discutés. Celui qui présente les caractéristiques les plus proches de celles énoncées plus haut est sans conteste le vidéotex. Il lui reste cependant à compléter l'éventail de ses possibilités, notamment en matière de protection des données transmises et de transfert de fichiers. A suivre.

35. La transmission des résultats des analyses

La transmission des résultats concerne tous les résultats de toutes les analyses demandées par un médecin pour ses patients. Le médecin n'a pas le choix d'un résultat particulier qu'il souhaiterait avoir avant les autres. Nous en avons vu la raison : on ne peut faire aucune hypothèse sur l'organisation des données dans le fichier des résultats. Si cela peut représenter un léger inconvénient du point de vue de certains médecins, cela permet, en contrepartie, plusieurs avantages. Le déroulement des opérations peut être entièrement automatisé, puisqu'aucun dialogue manuel n'est nécessaire. Cela facilite l'utilisation du système. La durée de connexion est réduite au strict minimum puisque le médecin ne perd pas de temps pour choisir ce qu'il souhaite recevoir, d'où une meilleure utilisation du système et une réduction des coûts de communication. De plus, un résultat isolé ne sert pas à grand chose. C'est seulement au vu de l'ensemble des résultats que le médecin peut établir un diagnostic précis et fiable.

36. Les conditions du succès

Quelles sont les conditions du succès ? En d'autres termes, qu'attend l'utilisateur de toute application informatique ? Nous distinguerons principalement deux conditions.

Premièrement, l'application doit respecter ses spécifications telles que décrites dans l'analyse des besoins. Ce point est crucial et pas toujours évident. En effet, rare est l'utilisateur qui sait exactement ce qu'il veut dès le début et qui ne change pas d'avis en cours de route. La méthode de conception de l'application doit donc permettre des modifications et des évolutions ultérieures, suite à l'apparition de nouveaux besoins ou de changements dans l'environnement. Dans le cas présent, cet aspect des choses est rendu encore plus difficile de par le nombre des utilisateurs potentiels. Par exemple, tout changement dans le protocole de communication des analyses d'un laboratoire implique la même modification chez tous les médecins qui lui sont reliés. D'où l'importance de bien définir les besoins et les règles à respecter, pour éviter de tels chambardements qui mèneraient inévitablement à l'anarchie la plus complète. Nous en avons vu les dangers, notamment pour le libre choix du médecin et du patient.

Deuxièmement, l'application doit être facile d'utilisation et ne nécessiter qu'un nombre réduit de manipulations. Il s'agit là surtout de problèmes techniques qui peuvent être résolus au cas par cas.

37. L'expérience des autres

L'expérience des autres peut être utile. Ainsi, les français ont déjà expérimenté un système de transmission des résultats d'analyses par le minitel. Après une courte période d'engouement pour ce nouveau procédé, on a constaté une forte diminution de l'intérêt d'abord manifesté. La raison est simple. La solution minitel ne présentait aucun avantage sur la communication téléphonique simple, le minitel ne permettant que la simple consultation des résultats et non leur transfert. De plus les mesures de sécurité étaient et restent assez sommaires, l'authentification étant réalisée par simple mot de passe émis en clair et les résultats n'étant pas protégés au cours de leur transmission. Le système que nous proposons corrige ces deux faiblesses. D'une part, il est possible de récupérer les résultats des analyses, par exemple pour les introduire automatiquement dans un dossier médical informatisé. D'autre part, les techniques utilisées assurent une protection bien meilleure du secret médical. La sécurité du système peut encore être améliorée par l'emploi de la carte à microprocesseur.

38. Généralisation aux autres laboratoires

Nous avons signalé au début de ce travail que nous limitions notre étude à la transmission des résultats d'analyses biomédicales, en milieu extra-hospitalier. Le système élaboré est-il applicable en milieu hospitalier et pour d'autres types d'analyses ? D'emblée, on peut répondre que c'est parfaitement faisable, moyennant quelques adaptations. En effet, les contraintes fondamentales restent les mêmes pour ce qui est du respect du secret médical et, dans une certaine mesure, du libre choix du médecin. Les seules adaptations à apporter concernent le mode de connexion au laboratoire, le support de transmission dans un hôpital étant alors un réseau local et plus le réseau téléphonique public. Quant à la nature des résultats des analyses, cela ne pose pas de problème, puisque aucune hypothèse n'est faite à leur sujet. Tout ceci, bien sûr, sous réserve de caractéristiques particulières que nous ne saurions considérer ici.

39. Polyvalence du système proposé

Le système proposé permet non seulement la transmission des résultats des analyses du laboratoire vers le médecin, mais peut aussi être utilisé pour l'échange d'informations du médecin vers le laboratoire, d'un laboratoire vers un autre laboratoire et d'un médecin vers un autre médecin.

Implémentation[1]

La partie implémentation a pour double but de confronter la théorie à la pratique et de montrer que le système proposé est parfaitement réalisable par un développeur indépendant.

Nota bene

Les sources du programme sont disponibles sur simple demande au secrétariat de l'Institut d'Informatique des FUNDP.

1. Caractéristiques générales

Le logiciel implémente les fonctions du laboratoire et du médecin. Il peut donc être utilisé pour émettre ou pour recevoir des résultats d'analyses, et, de façon plus générale, des données sous forme de fichier informatique. Le système supporte une communication à la fois. Cette caractéristique le destine plus spécialement au médecin, les besoins du laboratoire en puissance de traitement des informations nécessitant souvent la possibilité d'accepter plusieurs accès simultanés.

Toutes les tâches sont caractérisées par un haut degré d'automatisation. Les échanges entre l'utilisateur et le système sont réduits au strict minimum. Ainsi, l'exécution d'une fonction nécessite au maximum trois ordres élémentaires. On peut encore accentuer l'automatisation par l'utilisation de macros. Des contrôles avec reprise des erreurs d'introduction sont prévus.

2. Plate-forme de développement

Le système décrit est implémenté sur micro-ordinateurs Apple Macintosh, sous Mac-OS version 6, et sur PC-compatible, sous MS-DOS version 3. Le logiciel permet l'utilisation de modems compatibles Hayes Smartmodem.

Le langage de programmation adopté est le TurboPascal qui présente l'avantage de permettre l'obtention d'un code source assez proche sous Mac-OS et MS-DOS. Sous Mac-OS, il s'agit de la version 1 et sous MS-DOS, de la version 5.

[1] Partie plus spécifiquement destinée aux informaticiens

3. Les informations relatives aux interlocuteurs

Les informations relatives à un interlocuteur sont : son nom, le code d'identification qui permet de s'identifier auprès de lui, son numéro d'appel et la clé de chiffrement-déchiffrement utilisée pour les communications avec lui. Considérons deux interlocuteurs A et B, les informations sont définies comme suit :

Interlocuteur A	Interlocuteur B
NomA	NomB
CodeIdentA	CodeIdentB
NoAppelA	NoAppelB
CléTransA	CléTransB

- NomA est le nom que A donne à B, et vice-versa ;
- CodeIdentA est le nom que B donne à A. CodeIdentA est donc équivalent à NomB, et vice-versa ;
- NoAppelA est le numéro d'appel de B, et vice-versa ;
- CléTransA est la clé de chiffrement-déchiffrement utilisée pour les communications avec B. CléTransA est donc équivalent à CléTransB.

Les informations confidentielles à protéger sont NoAppel et CléTrans. Elles sont chiffrées à l'aide de la clé personnelle de l'utilisateur pour leur conservation dans un fichier avec Nom et CodeIdent. Ce fichier est constitué d'enregistrements ayant la structure suivante :

- Nom : 16 caractères alphanumériques ;
- CodeIdent : 16 caractères alphanumériques ;
- NoAppel : 16 caractères alphanumériques ;
- CléTrans : 8 caractères alphanumériques.

Ce type de fichier permet un accès direct aux enregistrements qui sont classés par ordre alphabétique sur le nom. Le premier enregistrement du fichier est réservé pour la conservation de la clé personnelle chiffrée par elle-même et mise à la place de CléTrans. La clé personnelle compte 8 caractères alphanumériques.

Remarque.

Le code d'identification ne sert à rien pour le laboratoire dans le système proposé. Cependant, il pourrait être utile. Si le laboratoire sous-traite une partie de ses analyses à un autre laboratoire, il pourrait demander la transmission des résultats de la même façon que le médecin. Il devra alors s'identifier auprès de l'autre laboratoire. Le même système pourrait être appliqué en cas d'échanges entre deux médecins. Ce qui ajoute encore à la souplesse et à la polyvalence du système proposé.

4. Le protocole de communication XYModem

Le protocole décrit ci-après ne peut prétendre qu'à une plus ou moins lointaine descendance de XModem. Il inclut certaines caractéristiques absentes du protocole original, mais qu'il nous a semblé utile, sinon indispensable, d'inclure. Outre sa destination première qui est le transfert de fichiers, il est adapté pour assurer les fonctions d'identification et d'authentification.

Principales caractéristiques

Le protocole, que nous baptiserons XYModem, réalise un transfert par paquets avec accusé de réception pour chaque paquet transmis. Cela signifie qu'il découpe le fichier à transmettre en morceaux (paquets) et qu'avant d'émettre un paquet, il attend un accusé de bonne réception du paquet précédent. En cas de mauvaise réception d'un paquet, celui-ci est retransmis. Des contrôles de flux, de séquence et des erreurs de transmission sont assurés.

Nature des échanges

Dans tout transfert de fichier, il y a un émetteur et un récepteur, mais l'initiative du transfert peut être prise par l'un ou l'autre. Ici, c'est le récepteur qui prend l'initiative.

Une fois la communication établie, le transfert peut commencer. L'émetteur émet le premier paquet. Après réception de celui-ci, le récepteur vérifie si la transmission s'est déroulée sans erreurs et si le numéro d'ordre du paquet correspond à la séquence logique. Si tout s'est bien passé, le récepteur émet le caractère ACK (ASCII n° 6), sinon il émet le caractère NAK. Si l'émetteur reçoit le caractère ACK, il émet le paquet suivant. Tandis que s'il reçoit le caractère NAK, il retransmet le même paquet. La fin de transmission est signalée par le caractère CAN (ASCII n° 18) émis par l'émetteur ou le récepteur.

Dans le cas où un caractère NAK ou ACK serait perdu en cours de transmission, l'émetteur laisse s'écouler un délai de 10 secondes après avoir cessé d'émettre, puis émet un caractère CAN pour interrompre la communication. De même, si le récepteur ne reçoit pas de réponse après l'émission d'un caractère NAK ou ACK, il émet un caractère CAN après un délai de 10 secondes.

Format général des paquets

Octet	Nature
0	Octet de poids faible du numéro de paquet
1	Octet de poids fort du numéro de paquet
2 à n	Caractères de données
n + 1	Octet inférieur du contrôle des erreurs de transmission
n + 2	Octet supérieur du contrôle des erreurs de transmission

Le numéro du paquet est un entier codé sur 2 octets. Il peut prendre une valeur entre 0 et +32767 inclus. Les paquets sont numérotés à partir de 0 avec incrément de 1. **n** est un entier compris entre 3 et 1025 inclus.

Détection des erreurs de transmission

Les algorithmes habituellement employés pour la détection des erreurs de transmission font appel à la technique des codes polynomiaux. Cependant, leur programmation est assez lourde. On peut avantageusement les remplacer par une technique alternative connue sous le nom de ISO Checksum Algorithm. Cet algorithme est plus facile à implémenter et donne d'aussi bons résultats (Stallings, Data and Computer Communications).

La technique utilisée consiste en une somme de contrôle calculée sur les n premiers octets, codée sur 16 bits et attachée au paquet par l'émetteur. Le récepteur applique le même algorithme, cette fois aux n+2 octets, et doit obtenir un reste nul, s'il n'y a pas d'erreurs. Cette technique assure la détection des erreurs de transmission dans 99,99 % des cas. De plus, le chiffrement des données apporte une garantie supplémentaire. Si une erreur n'est pas détectée, le déchiffrement aura pour effet de produire des informations inintelligibles. On peut encore réduire le risque de non-détection des erreurs de transmission en employant un modem autocorrecteur.

Contrôle de flux

Le contrôle de flux doit permettre de moduler la cadence de transfert des informations entre deux entités distinctes, en fonction de leur capacités respectives d'émission et de réception des informations. Dans le cas de XYModem, ce contrôle est assuré par l'émission d'un caractère NAK entre les paquets, si le récepteur n'était pas prêt pour la réception d'un nouveau paquet au moment de son émission par l'émetteur ou si un problème est survenu au cours de la transmission.

Descriptions des paquets

Identification-authentification, émetteur : médecin

Octet	Valeur
0	0
1	0
2 à 17	Code d'identification du médecin
18 à 25	Code d'authentification en clair du médecin
26	Octet inférieur du contrôle des erreurs de transmission
27	Octet supérieur du contrôle des erreurs de transmission

Authentification1, émetteur : laboratoire

Octet	Valeur
0	0
1	0
2 à 9	Code d'authentification chiffré du médecin
10 à 17	Code d'authentification en clair du laboratoire
18	Octet inférieur du contrôle des erreurs de transmission
19	Octet supérieur du contrôle des erreurs de transmission

Authentification2, émetteur : médecin

Octet	Valeur
0	0
1	0
2 à 9	Code d'authentification chiffré du laboratoire
10	Octet inférieur du contrôle des erreurs de transmission
11	Octet supérieur du contrôle des erreurs de transmission

Transmission des résultats des analyses, émetteur : laboratoire

Paquet d'initialisation des échanges

Octet	Valeur
0	0
1	0
2	Octet de poids faible du nombre de paquets à transférer
3	Octet de poids fort du nombre de paquets à transférer
4	Octet de poids faible de la taille du dernier paquet
5	Octet de poids fort de la taille du dernier paquet
6	Octet inférieur du contrôle des erreurs de transmission
7	Octet supérieur du contrôle des erreurs de transmission

Le nombre de paquets à transférer et la taille du dernier paquet sont des entiers codés sur 2 octets. Ces valeurs sont comprises entre 1 et +32767 inclus pour la première et entre 1 et +1028 inclus pour la seconde.

N - 1 premiers paquets

Octet	Valeur
0	Octet de poids faible du numéro de paquet
1	Octet de poids fort du numéro de paquet
2 à 1025	Résultats chiffrés
1026	Octet inférieur du contrôle des erreurs de transmission
1027	Octet supérieur du contrôle des erreurs de transmission

Dernier paquet

Octet	Valeur
0	Octet de poids faible du numéro de paquet
1	Octet de poids fort du numéro de paquet
2 à n	Résultats chiffrés
n + 1	Octet inférieur du contrôle des erreurs de transmission
n + 2	Octet supérieur du contrôle des erreurs de transmission

n est un entier compris entre 3 et 1025 inclus.

Accusés de réception

Après réception d'un paquet, le récepteur émet un accusé de réception constitué d'un seul caractère qui peut être :

- ACK : pas d'erreurs de transmissions ni de séquence, on continue.
- NAK : présence d'erreurs de transmission, demande de réémission.
- CAN : présence à répétition d'erreurs de transmission, de séquence, tentative de fraude ou fin normale. On arrête tout.

Conclusions

Les conclusions ci-après concernent les garanties apportées par le système proposé au respect du secret médical et du libre choix du médecin et du patient. Une conclusion générale vient clôturer ce dernier chapitre.

1. Protection du secret médical

Garanties apportées au respect du secret médical :

- Un médecin ne peut avoir accès aux résultats d'analyses qui ne lui sont pas destinés.

- Le laboratoire ne peut prendre connaissance des dossiers médicaux des patients d'un médecin.

- Les risques d'atteintes à la confidentialité et l'intégrité des résultats d'analyses au cours de leur transmission sont palliés par un système de chiffrement-déchiffrement basé sur un algorithme standard qui a fait ses preuves.

- Le nombre d'intermédiaires est réduit. Le laboratoire contrôle l'ensemble des opérations de la réception de la demande d'analyses à la remise des résultats.

Bien sûr, une sécurité totale ne peut être assurée uniquement par des moyens techniques. L'influence du facteur humain est prépondérante. Tous les moyens mis en oeuvre et les mesures prises pour augmenter le niveau de sécurité d'un système sont parfaitement inutiles si on n'obtient pas en même temps la collaboration de ses utilisateurs.

2. Libre choix du médecin

Garanties apportées à la notion de libre choix du médecin et, par là, du patient :

- Le matériel nécessaire (ordinateur personnel équipé d'un modem) devient un produit de consommation presque courant dont le prix se démocratise chaque jour un peu plus. Cela garantit l'indépendance financière du médecin.

- Les principes à la base du logiciel peuvent servir de point de départ à la définition d'un règlement standard pour les aspects techniques de la transmission des résultats des analyses. Leur simplicité rend la réalisation du logiciel accessible à un développeur indépendant. Ces deux aspects garantissent l'indépendance technique du médecin vis-à-vis du laboratoire.

3. Conclusion générale

Au terme de ce mémoire, nous pensons avoir atteint nos objectifs et espérons avoir fourni au lecteur l'information la plus objective et la plus indépendante possible sur des problèmes se rapportant à un sujet sensible : la santé. En effet, à côté de la raison fondamentale de l'activité médicale qui est de soigner, il existe des aspects économiques et juridiques importants qui interfèrent souvent avec celle-ci. Nous ne pouvions les ignorer. Cependant, ne voulant en aucun cas prendre position pour quelque partie que ce soit, nous avons volontairement limité notre travail à l'aspect scientifique et technique du problème, en tenant le moins compte possible d'autres aspects pour lesquels nous ne pensons pas être en mesure de donner un avis. Les enseignements que nous avons pu tirer de notre étude peuvent, à notre avis, servir de point de départ pour des investigations ultérieures : utilisation de la carte microprocesseur, échanges d'informations du médecin vers le laboratoire, entre laboratoires et entre médecins, types des résultats des analyses, etc... .

Annexe1. Extraits du code de déontologie médicale

Les principaux articles du code de déontologie médicale sont repris afin de préciser la notion de secret médical, de définir le dossier médical et d'énoncer les principes à respecter en matière de publicité et pour garantir le caractère non commercial de la profession.

Chapitre 1.

Objet et champ d'application du code.

Art. 1 : La déontologie est l'ensemble des principes, des règles et des usages que tout médecin doit observer ou dont il doit s'inspirer dans l'exercice de sa profession.

Art. 2 : Les dispositions du présent code sont applicables à tout médecin inscrit au tableau de l'ordre. Elles sont énonciatives et non limitatives. Elles peuvent être appliquées par analogie.

Chapitre 2.

Devoirs généraux des médecins.

Art. 8 : Le médecin doit être conscient de ses devoirs sociaux envers la collectivité.

Art. 9 : Le médecin doit s'abstenir, même en dehors de l'exercice de sa profession, de tout acte de nature à entacher l'honneur ou la dignité de celle-ci.

Art. 10 : L'art médical ne peut en aucun cas, ni d'aucune façon, être pratiqué comme un commerce.

Chapitre 3.

La publicité.

Art. 12 : La publicité directe ou indirecte est interdite. La réputation du médecin est fondée sur sa compétence professionnelle et son intégrité.

Chapitre 4.

Le dossier médical.

Art. 38 : Le médecin doit, en principe, tenir un dossier médical pour chaque patient.

Art. 39 : Le médecin qui a établi et complété à lui seul le dossier médical est responsable de sa conservation. Il décide de la transmission de tout ou partie de ses éléments, en tenant compte du respect du secret médical.

Art. 40 : Par contre, si les dossiers médicaux sont l'oeuvre d'une équipe et s'ils sont centralisés dans un établissement de soins ou dans une autre institution, seuls les médecins qui sont appelés à donner des soins aux malades peuvent y avoir accès. La teneur de ces dossiers et leur conservation ne peuvent être confiées par ces médecins qu'à des personnes tenues également au secret professionnel.

Art. 41 : Le médecin est tenu, à la demande ou avec l'accord du patient, de communiquer dans un délai rapide, à un autre praticien traitant, toutes les informations utiles et nécessaires pour compléter le diagnostic ou pour poursuivre le traitement.

Art. 42 : Le médecin, lorsqu'il l'estime utile ou lorsque le malade lui en fait la demande, peut remettre au patient, dans la mesure où son intérêt l'exige, les éléments objectifs du dossier médical, tels que les radiographies et les résultats d'examens.

Chapitre 5.

Secret professionnel du médecin.

Art. 55 : Le secret professionnel auquel le médecin est tenu est d'ordre public. Il s'impose dans quelque circonstance que ce soit aux praticiens consultés par un patient ou amenés à lui donner des soins ou des avis.

Art. 56 : Le secret professionnel du médecin comprend aussi bien ce que le patient lui a dit ou confié que tout ce que le médecin pourra connaître ou découvrir à la suite d'examens ou d'investigations auxquels il procède ou fait procéder.

Art. 57 : Le secret professionnel s'étend à tout ce que le médecin a vu, connu, appris, constaté, découvert ou surpris dans l'exercice ou à l'occasion de l'exercice de sa profession.

Art. 70 : Le médecin veillera à faire respecter par ses auxiliaires les impératifs du secret médical.

Compléments

Droit de propriété sur le dossier médical.

En Belgique, aucune législation ne reconnaît un droit de propriété au patient. Le médecin est seul détenteur des renseignements confidentiels sur base du secret professionnel. Le fait que le médecin est propriétaire de ses notes de travail personnelles et que les radiographies ou résultats de laboratoire appartiennent au patient ou à celui qui les a payés n'est pas contesté.

Droit de regard du patient dans son dossier.

Il existe encore moins de dispositions légales à cet égard. Les conseils provinciaux de l'Ordre disent que le dossier ne peut être transmis directement à un patient.

Annexe 2. L'Ordre des médecins

Pour définir l'organisation et le rôle de l'Ordre des médecins, sont repris des extraits de l'arrêté royal n° 79 du 10 novembre 1967, relatif à l'Ordre des médecins qui modifie la loi du 25 juillet 1938 le créant. Cet arrêté royal a toujours cours.

Chapitre 1er.

Organisation.

Art. 1 : (...) Ses organes sont : les conseils provinciaux, les conseils d'appel et le conseil national. Il jouit de la personnalité civile de droit publique.

Art. 2 : L'Ordre des médecins comprend tous les docteurs en médecine, chirurgie et accouchements, domiciliés en Belgique et inscrits au tableau de l'Ordre de la province dans laquelle est situé leur domicile. Est considéré comme domicile au sens du présent arrêté, le lieu où le médecin exerce ses activités principales. (...)

Chapitre 2.

Les conseils provinciaux.

Art. 5 : Il est établi dans chaque province, un conseil provincial de l'Ordre des médecins qui a autorité et juridiction sur les médecins qui sont inscrits, conformément à l'article 2, au tableau de l'Ordre de cette province ainsi qu'au ressortissant d'un des Etats membres de la Communauté Economique Européenne qui est établi en tant que médecin dans un autre Etat membre et qui effectue dans le ressort du conseil provincial une prestation de services. Cette autorité et cette juridiction ne sont exercées à l'égard des médecins militaires que pour l'activité qui a requis leur inscription au tableau de l'Ordre conformément au même article. (...)

Le Roi règle l'organisation et le fonctionnement des conseils provinciaux. Il en fixe le siège. Chaque conseil provincial établit son règlement d'ordre intérieur ; celui-ci est soumis au conseil national qui en arrête définitivement le texte.

Art. 6 : Les attributions des conseils provinciaux sont :

1° Dresser le tableau de l'Ordre. (...)

2° Veiller au respect des règles de la déontologie médicale et au maintien de l'honneur, de la discrétion, de la probité et de la dignité des médecins. Ils sont chargés à cette fin de réprimer disciplinairement les fautes de ces médecins, commises dans l'exercice de la profession ainsi que les fautes graves commises en dehors de l'activité professionnelle, lorsque ces fautes sont de nature à entacher l'honneur ou la dignité de la profession.

3° Donner aux membres de l'Ordre d'initiative ou à leur demande, des avis sur des questions de déontologie médicale qui ne sont pas réglées dans le code ou par la jurisprudence. Les avis sont transmis au conseil national pour approbation puis communiqués au conseil provincial qui les transmet aux médecins intéressés.

4° Signaler aux autorités compétentes les actes d'exercice illégal de l'art médical dont ils ont connaissance.

(...)

Chapitre 4.

Le conseil national.

Art. 15, § 1er : Le conseil national élabore les principes généraux et les règles relatifs à la moralité, l'honneur, la discrétion, la probité, la dignité et le dévouement indispensables à 'exercice de la profession, qui constitue le code de déontologie médicale.

(...)

Le code comprend notamment les règles relatives à la continuité des soins en ce compris l'organisation des services de garde, au secret professionnel, à la transmission des documents ou d'informations médicales entre confrères, en particulier dans le cadre de l'exercice de la médecine préventive, ainsi qu'aux rapports individuels entre le médecin d'une part, les malades, les confrères, les praticiens de l'art dentaire, les pharmaciens, et les titulaires des professions paramédicales d'autre part.

Il énonce les principes sur base desquels sont déterminées les obligations sociales du médecin.

Il peut, s'il y a lieu, déterminer les clauses qui, en raison de leur incompatibilité avec les principes de la déontologie et en particulier avec la liberté thérapeutique du médecin, sont prohibées dans les conventions à conclure par les médecins au sujet de l'exercice de leur profession.

(...)

Chapitre 5.

Sanctions et déchéances.

Art. 16 : Les sanctions dont dispose le conseil provincial sont : l'avertissement, la censure, la réprimande, la suspension du droit d'exercer l'art médical pendant un terme qui ne peut excéder deux années et la radiation du tableau de l'Ordre.

(...)

Annexe 3. Comparaison des coûts DCS-Datel[1]

DCS

1. Frais d'installation.

- Raccordements directs : de 17850 à 65450 FB, selon le débit.
- Raccordements via le RTC : 1785 FB par NUI.

2. Redevances bimestrielles d'abonnement.

- Raccordements directs : de 10710 à 59500 FB, selon le débit.
- Raccordements via le RTC : abonnement RTC + 535,5 FB.

3. Taxes d'utilisation.

- Taxe d'établissement d'appel : 0,1785 FB.
- Taxe d'accès en mode X32 : 1,19 FB par période de 30 secondes.
- Taxe d'accès avec usage du PAD : 0,708 FB par période de 30 secondes.
- Taxe à la durée : 0,119 FB par période de 30 secondes.
- Taxe au volume avec usage du PAD : 0,714 FB par décasegment.
- Taxe au volume sans usage du PAD : 0,238 FB par décasegment.

Un décasegment est équivalent à 640 octets.

Datel

1. Frais d'installation.

- Raccordement : 4165 FB.

2. Redevances bimestrielles d'abonnement.

- De 619 à 912 FB, selon la zone.

3. Taxes d'utilisation.

- 5,95 FB par tranche de 40, 180 ou 360 secondes selon la nature de la communication : zonale, interzonale contigüe ou non contigüe.

[1] Tarifs en vigueur pour le service intérieur, en janvier 1990, TVA 19 % comprise.

Annexe 4. Définitions des sigles

AFNOR	Association Française de NORmalisation
ANSI	American National Standard Institute
ASCII	American Standard Code for Information Interchange
bps	bits par seconde
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CEPT	Conférence Européenne des Postes et Télécommunications
CNIM	Cercle Namurois d'Informatique Médicale
Datel	Service de transmission de données par le RTC
DCS	Data Communication Service
DES	Data Encryption Standard
ECMA	European Computer Manufacturer's Association
ETCD	Equipement de Terminaison du Circuit de Données
ETTD	Equipement Terminal de Traitement de Données
FAMGB	Fédération des Associations de Médecins Généralistes de Bruxelles
FUNDP	Facultés Universitaires Notre-Dame de la Paix, Namur
ISO	International Organization for Standardization
MIM	Société belge d'informatique médicale
NBS	National Bureau of Standards
NUA	Number User Adress
NUI	Number User Identifier
OSI	Open Systems Interconnection
PAD	Packet Assembly Disassembly
RCM	Résumé Clinique Minimum
RNIS	Réseau Numérique à Intégration de Services
RTC	Réseau Téléphonique Commuté
RTT	Régie des Télégraphes et des Téléphones

Bibliographie

1. Ouvrages

Ancelin C. & Marchand M., 1984. Le vidéotex, contribution aux débats sur la télématique. Collection technique et scientifique des télécommunications. Masson.

Apple, 1988. Inside Macintosh. Volume 2. Eight Printing, July 1988. Addison-Wesley Publishing Company, Inc.

Association française de normalisation, 1983. Sécurité informatique et potection des données. Collection normes et techniques. AFNOR.

Borland, 1986. Turbo Pascal for the Mac. User's Guide and Reference Manual. Borland International, Inc.

Buitelaar M., Gallet J.-F., Labarde C. & Litré P., 1985. Cabinet médical et informatique. Eyrolles.

Cauchy A., 1987. Les vidéotex français et belges : étude comparative et prospective. Institut d'informatique. FUNDP.

Davies D. W. & Price W. L., 1984. Security for computer networks, an introduction to data security in teleprocessing and electronic fund transfert. Wiley series in computing. John Wiley & Sons.

Gofton P. W., 1987. Techniques de communication série sur PC et compatibles. Sybex.

Grémy F., 1987. Informatique médicale. Collection "De la biologie à la clinique". Médecine-Sciences. Flammarion.

Henshall J. & Shaw S., 1988. OSI explained. End to end computer communications standards. Ellis Horwood series in computer communications and networking. Ellis Horwood Limited.

Jan C. & Sabatier G., 1989. La sécurité informatique. Eyrolles.

Lachand-Robert J.-E., 1988. Turbo Pascal sur Macintosh. Sybex.

Longley D. & Shain M., 1989. Data & Computer Security. Dictionary of standards concepts and terms. Macmillan Reference Books. Macmillan Publishers LTD.

Macchi C. & Guilbert J.-F., 1987. Téléinformatique, transport et traitement de l'information dans les réseaux et systèmes téléinformatiques et télématiques. Collection informatique. Dunod.

Maiman M., 1986. Télématique, téléinformatique et réseaux. 2e édition. Masson.

Nussbaumer H., 1987. Téléinformatique 2. Conception des réseaux. Réseau. Transport. Presses Polytechniques Romandes.

Serpe J.-M., 1988. La sécurisation des systèmes informatiques par la carte à microprocesseur. Institut d'informatique. FUNDP.

Société belge d'informatique médicale, 1988. Numéro spécial : enquête. janvier 1988.

Stallings W., 1988. Data and computer communications. Second edition. Macmillan Publishing Company.

Stallings W., 1988. Handbook of computer-communications standars. Volume 3. Department Of Defense (DOD) protocol standards. First edition. Third printing. Howard W. Sams & Company.

Van Bastelaer P., 1989. Téléinformatique et réseaux : fonctions et concepts. Notes de cours. FUNDP.

Van Lamsweerde A., 1989. Méthodologie de développement de logiciels. Notes de cours. FUNDP.

Documents techniques

RTX-Gateway, technical interface specification. Edition 2 / Octobre 1985. N° 165. RTT, Videotex Service.

RTX-Gateway, test specification. Edition 1 / June 1986. N° 165. RTT, Videotex Service.

2. Articles

Amory B., 1987. Le droit des obligations de sécurité informatique. Securicom 87, pp 225-238.

Amory B. & Thunis X., 1988. Aspects juridiques de l'utilisation du télécopieur. Droit de l'informatique et des télécoms. N° 4, pp 35-39.

Bielande P., 1988. Etude comparative des coûts d'utilisation de divers services de télécommunications : DCS, RTC et lignes louées. Cas des transferts de fichiers en liaison point à point. Centre de Recherche Informatique et Droits, FUNDP.

Bourse R., 1984. Réflexions sur la télématique et le laboratoire de biologie clinique. Feuillets de biologie. Vol 25, n° 139, pp 23-27.

Brock N. Meeks, 1989. The ABCs of X-, Y- and ZMODEM. Byte, February 1989, pp 163-166.

Brock N. Meeks, 1989. The protocol pack. Byte, March 1989, pp 155-158.

Cannio S. & de Fooz A., 1990. Vie privée : tous fichés. Le Vif / L'Express, n° 2013, 2 février 1990, pp 18-21.

Celiktin S., 1986. Réflexions sur le protocole Kermit. Institut d'informatique, FUNDP.

Comité des Ministres du Conseil de l'Europe, 1981. Réglementation applicable aux banques de données médicales automatisées. Recommandation n° R(81) 1.

Comité scientifique, section de physiopathologie, commission informatique, 1985. La liaison télématique médecins-laboratoires de biologie médicale. ISB, 11, n° 4, pp 251-252.

Comité scientifique, section de physiopathologie, commission informatique, 1985. Recommandations relatives à la télétransmission de documents se rapportant aux analyses de biologie médicale. ISB, 11, n° 5, pp 330-333.

Bibliographie

Comité scientifique, section de physiopathologie, commission informatique, 1986. Le service télématique du laboratoire : solutions techniques simples. ISB, 12, n° 1, pp 38-40.

De Bisschop O. Le dossier médical en médecine générale : aspects juridiques et déontologiques.

De Coninck H. & De Coster A.-M., 1989. Le secret médical : une arme à double tranchant. Budget & Droits. Décembre 1989, n° 88, pp 4-8.

Leblanc A. et Richard L., 1984. Le laboratoire de biologie médicale et la télématique. Feuillets de biologie. Vol 25, n° 137, pp 59-62.

Meert-Van de Put R., 1986. La confidentialité des données et le secret médical : aspect juridique. Louvain Med., n° 105, pp 521-529.

Montagut J., 1984. A propos de connexions informatisées dans un laboratoire de biologie clinique. Feuillets de biologie. Vol 25, n° 141, pp 43-48.

Ordre des médecins, 1975. Code de déontologie.

Ordre des médecins. Bulletins du Conseil National. N° 34, p 40 ; n° 38, pp 11-12 et 16 ; n° 40, pp 12-13 et 26-28 ; n° 42, pp 11-12 ; n° 43, pp 40-42 ; n° 44, pp 17-18 ; n° 45, pp 20-22.

Poullet E., 1986. Sécurité informatique et données médicales. Louvain Med., n° 105, pp 531-537.

Poullet Y. & Warrant F., 1989. Nouveaux compléments au service téléphonique et protection des données : à la recherche d'un cadre conceptuel. Centre de Recherche Informatique et Droits, FUNDP.

Poullet Y., 1987. Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information. Droit de l'informatique, n° 4, pp 222-226.

Poullet Y., 1990. Informatique et libertés. Un débat en quête de solutions. La Semaine Informatique, n° 184, pp 32-44.

Roger F. H., 1989. Security threats and trends in society. MIM News 1989, pp 44-52.

Sokal G., 1986. Le secret médical. Point de vue du médecin. Louvain Med., n° 105, pp 511-514.

Warrant F., 1989. Recherche épidémiologique et protection des données médicales nominatives : état de la question en Belgique. Centre de Recherche Informatique et Droits, FUNDP.

Willems J. L. & Roger F. H., 1983. Recommendations of the belgian society for medical informatics (MIM) on medical data protection in automated informations systems. Medinfo-83, pp 980-983.