الجمهوريـــــــة الجزائريـــــة الديمقراطية الشعبيـــــة

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

وزارة التعليـــــم العـــــالي و البحـــــث العلمـــــي

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université d'Oran – Es-Sénia –
Faculté des Sciences
Département d'Informatique
1ère Année École Doctorale

Option : *Science et Technologie de l'Information et de la Communication (STIC)*
Module : *Sécurité des Systèmes d'Information*
Chargé du module : *Monsieur Kamel Rahmouni (professeur)*

Exposé N° 1

Sujet : LA SIGNATURE NUMÉRIQUE

Présenté par :
Monsieur Benaribi Fethi Imad **&** *Monsieur Bendriss Lahouari*

Avril, 2007

SOMMAIRE

1. INTRODUCTION

Le déploiement extraordinaire du réseau Internet est avant tout une révolution en matière d'expression humaine à l'échelle planétaire. Nous disposons à présent d'un gigantesque espace de communication permettant à notre économie de créer de nouveaux types d'entreprises, d'améliorer les canaux de distribution et d'information et de développer des méthodes originales pour prospecter le marché mondial.

Cet espace à la fois international, décentralisé et hétérogène où chacun peut agir, s'exprimer et travailler comme bon lui semble, n'est maîtrisé actuellement par aucun opérateur ni aucun Etat. C'est sur cette infrastructure prometteuse que le commerce électronique a vraiment fait son apparition. Il est aujourd'hui largement reconnu que cette nouvelle forme de commerce jouit d'un grand potentiel économique et qu'elle va jouer un rôle toujours plus grand dans le développement de notre société moderne.

Malheureusement, l'essor du commerce électronique se trouve freiné par une série de risques inhérents aux réseaux numériques ouverts du type Internet. Ceux-ci contribuent à miner la confiance des utilisateurs de cette nouvelle plate-forme de communication. L'importante croissance mondiale des réseaux numériques et le développement du commerce électronique ont ainsi entraîné inévitablement avec eux la question des mesures de sécurité prises dans ce domaine. En effet, ces réseaux, alors qu'ils sont de plus en plus importants pour notre économie avec l'augmentation de la valeur des données transmises et stockées par ces systèmes, deviennent également de plus en plus vulnérables à divers types de menaces.

L'infrastructure numérique qui se met actuellement en place constitue un environnement propice à toutes les formes de délits liés à l'informatique. Les messages confidentiels transmis sur un réseau ouvert comme le web peuvent facilement être interceptés, lus, copiés voire manipulés, et la validité des documents ou des contrats transitant par courrier électronique peut être contestée. Des informations sensibles peuvent ainsi tomber dans les mains d'un concurrent, d'un criminel ou d'un service de renseignements étranger.

Dans le monde entier par exemple, les télécommunications - téléphone, fax, courrier électronique - sont massivement surveillées par un dispositif titanesque appelé Echelon. Les services secrets américains, à la tête de ce réseau d'écoute, sont appuyés dans cette tâche par plusieurs pays alliés. On lit également fréquemment dans la presse que tel ou tel pirate s'est

introduit dans le réseau informatique d'un ministère de la défense ou d'une entreprise célèbre, par pure malice, ou alors, ce qui est plus grave, pour avoir accès à des données confidentielles ou encore pour manipuler ou détruire les réseaux attaqués.

Pour pouvoir profiter pleinement des nombreuses possibilités commerciales offertes par les réseaux numériques de communications ouvertes, il est indispensable de parvenir à sécuriser cette infrastructure. C'est précisément ici que la cryptographie intervient. Elle nous offre des outils performants, capables de contribuer de manière significative à la sécurité sur le réseau Internet. A l'aide de logiciels cryptographiques modernes et puissants, il devient possible de garantir la confidentialité des informations échangées sur les réseaux numériques, d'identifier de façon certaine la source des informations reçues et d'offrir l'assurance que le message attribué à quelqu'un n'a pas été modifié en transit par une personne non autorisée.

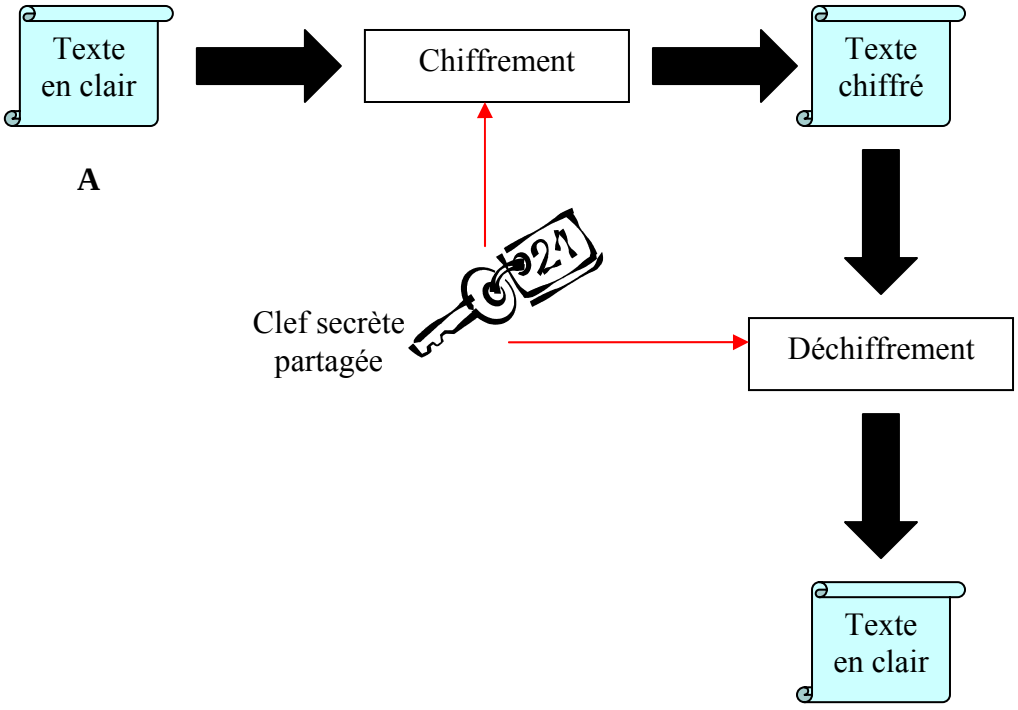
2. RAPPEL SUR LA CRYPTOGRAPHIE

Depuis l'ancienne Egypte, en passant par presque toutes les civilisations, la cryptographie n'a cessé d'évoluer pour devenir progressivement une technologie indispensable à notre société moderne d'information. Nous allons à présent vous présenter les trois types de cryptographie les plus employés sur les réseaux numériques.

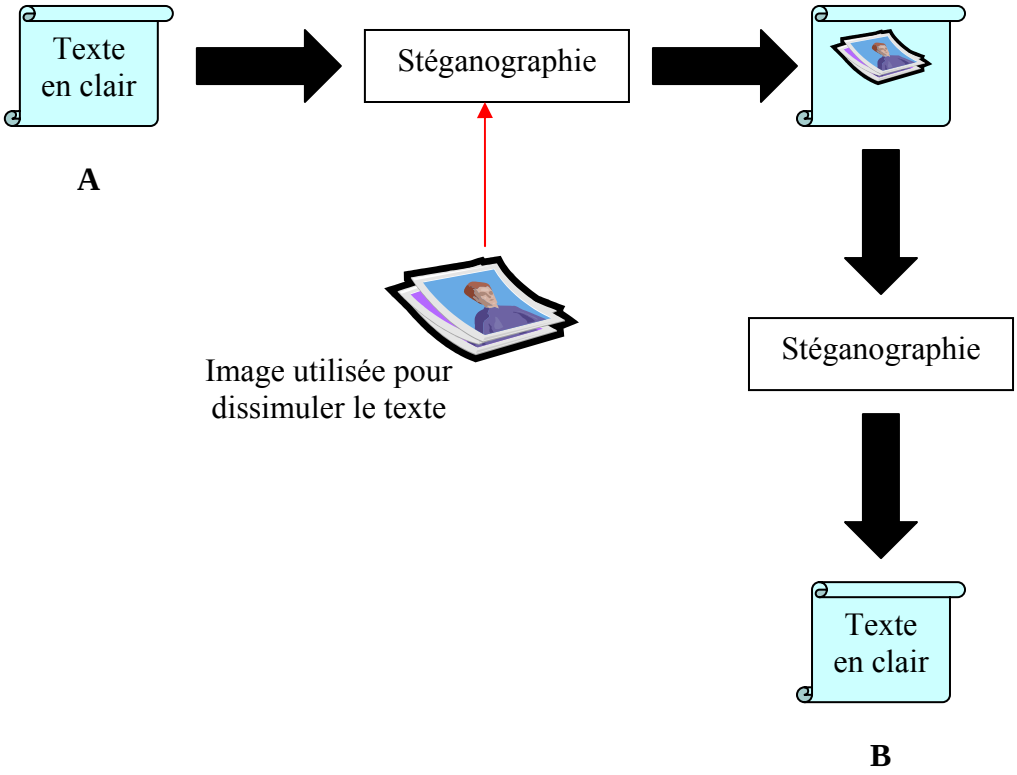
2.1. La cryptographie à clef secrète

Un des principaux buts de la cryptographie classique consiste à rendre incompréhensibles des messages secrets. En d'autres termes, il s'agit d'assurer la *confidentialité* de l'information susceptible de tomber dans de mauvaises mains.

Les systèmes de chiffrement traditionnels dits à *clef secrète*, ou *symétriques*, reposent sur le partage, entre deux interlocuteurs, d'une même clef secrète utilisée à la fois pour le chiffrement d'un message et pour son déchiffrement. Le but d'un tel système est de parvenir à garder une seule information secrète (la clef de chiffrement) à la place des messages proprement dits qui peuvent ainsi, une fois chiffrés, transiter sur des réseaux dits ouverts. La difficulté principale de cette technique est la suivante: la clef doit être remise aux interlocuteurs préalablement à la communication par un canal sûr, donc différent du canal prévu, de façon à ce qu'elle ne soit pas interceptée par des tiers non autorisés. Cette distribution préliminaire de clefs de vient cependant vraiment périlleuse et même impraticable lorsqu'il s'agit de communiquer des messages chiffrés à un grand nombre de participants que l'on ne connaît pas forcément, comme c'est le cas sur Internet. Par exemple, pour un réseau comportant 100 utilisateurs, il faudrait échanger préalablement près de 5000 clefs. En doublant le nombre d'usagers, l'échange de 20 000 clefs deviendrait nécessaire!



D'autres méthodes, comme la stéganographie, sont également fréquemment employées pour protéger des données confidentielles; ces procédés ont pour but de cacher le fait même de l'existence d'une information secrète (encres invisibles, etc.). Des techniques similaires sont encore utilisées de nos jours, par exemple la dissimulation d'un texte confidentiel dans les pixels numériques d'une photo digitale.



2.2. La cryptographie à clef publique

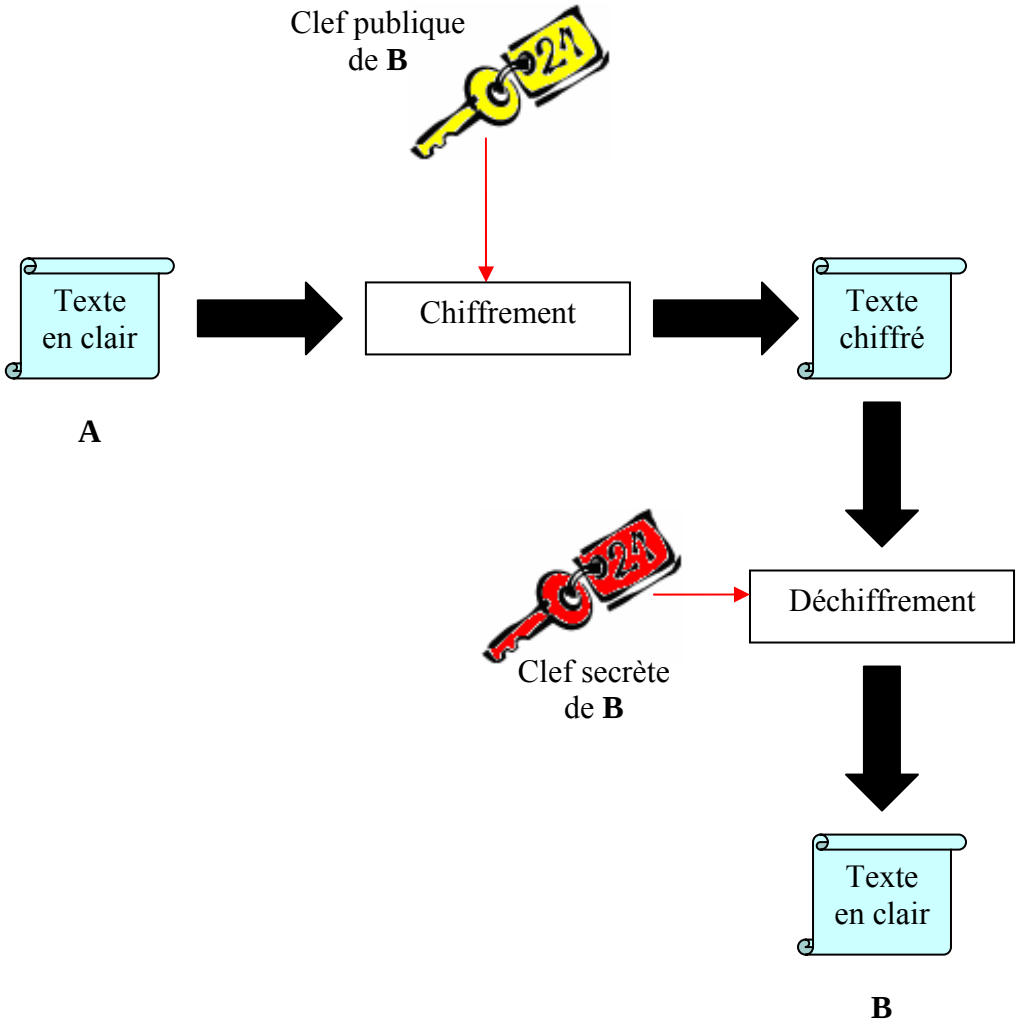
Avec l'avènement du chiffrement dit à *clef publique* ou *asymétrique*, qui caractérise la cryptographie moderne, les difficultés décrites plus haut ont été résolues. Cette technique a été développée en 1976 par Martin Hellman et Whitfield Diffie de l'université de Stanford et rapidement perfectionnée par trois mathématiciens américains du MIT[1]: Ronald Rivest, Adi Shamir et Leonard Adleman (créateurs du fameux algorithme RSA). Grâce à ce concept, qui a d'ailleurs complètement révolutionné le domaine du chiffrement, il est devenu possible, non seulement de chiffrer les informations, mais aussi d'authentifier les messages échangés. C'est cette dernière caractéristique qui a fourni la base des signatures digitales.

La cryptographie à clef publique repose sur une idée simple: au lieu de l'échange d'une seule clef secrète, chaque usager possède une paire de clefs mathématiquement liées (c'est-à-dire différentes mais complémentaires). Il s'agit alors d'une clef publique, largement diffusée par exemple dans un annuaire électronique, à laquelle correspond une seule autre clef, la clef privée, gardée secrète par son propriétaire. Il est actuellement impossible pour un pirate de déterminer la clef privée à l'aide de la clef publique. Ce système ne permet pas de chiffrer et

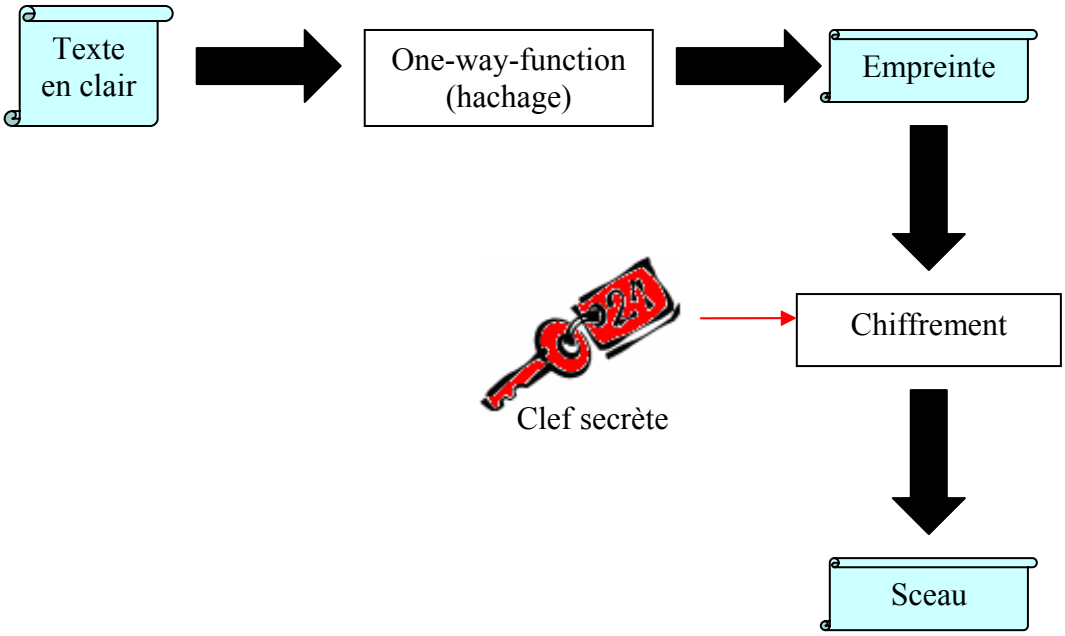
[1] MIT: ***Massachusetts Institute of Technology*** est une institution de recherche et une université américaine.

de déchiffrer un message avec une seule et même clef, il faut obligatoirement employer les deux clefs à disposition (privée et publique).

L'exemple suivant illustre ce procédé: un message chiffré par A avec la clef publique de B, ne peut être déchiffré que par la clef privée correspondante de B. De même, lorsqu'un message est signé numériquement par A à l'aide de sa clef privée, il peut être vérifié par Bob avec la clef publique correspondante de A.



Une fonction mathématique à sens unique (*one-way function*) se cache derrière ce procédé cryptographique. L'annuaire téléphonique peut illustrer ce concept: il est facile de trouver un numéro en connaissant le nom de l'interlocuteur recherché; il est cependant beaucoup plus difficile, à l'aide de l'annuaire, de trouver son nom en étant uniquement en possession de son numéro de téléphone!



Le système à clef publique permet donc d'échanger des informations confidentielles entre des interlocuteurs qui ne se sont jamais rencontrés auparavant. Il suffit de sélectionner la clef publique du destinataire se trouvant par exemple annexée dans un courrier électronique (e-mail) et de chiffrer le message avec celle-ci. Le destinataire se servira de sa clef privée pour déchiffrer la communication, que nul autre n'aura pu déchiffrer, même dans le cas où le message aurait été intercepté.

2.3. La cryptographie hybride

Les algorithmes de chiffrement asymétriques ont cependant également un désavantage, ils sont généralement beaucoup plus lents que les algorithmes symétriques. Ils ne conviennent donc guère au chiffrement de longs messages. Le moyen d'éviter ce désagrément est de combiner les mécanismes symétrique et asymétrique de chiffrement. Cette combinaison est appelée cryptographie hybride ou "enveloppe digitale". De nombreux biens cryptographiques fonctionnent sur ce principe, à l'exemple du logiciel culte PGP[2].

L'exemple suivant illustre de manière simplifiée ce procédé: le texte destiné à B est dans un premier temps chiffré par A avec un algorithme symétrique rapide (p.ex. IDEA[3]) qui emploie une clef secrète. Dans un second temps, le logiciel de A va coder cette clef secrète avec la clef publique de B. L'algorithme de chiffrement asymétrique chiffre uniquement la clef secrète utilisée pour coder le message et non pas le message en tant que tel. Il est donc

[2] PGP: ***Pretty Good Privacy*** est système de protection du e-mail conçu en 1991 par **Philip Zimmermann.**
[3] IDEA: ***International Data Encryption Algorithm***, développé par Xuejia Lai et James Massey en 1992.

possible de chiffrer très rapidement les messages tout en bénéficiant des avantages indéniables de la cryptographie à clef publique. Ces étapes sont à présent exécutées de manière tout à fait transparente pour les usagers.

2.4. Quels sont les standards actuels ?

En matière d'algorithmes symétriques, la longueur des clefs de chiffrement recommandée s'élève à 128 bits. Pour les algorithmes asymétriques, le standard conseillé est de 1024 bits.

2. LA SIGNATURE NUMÉRIQUE

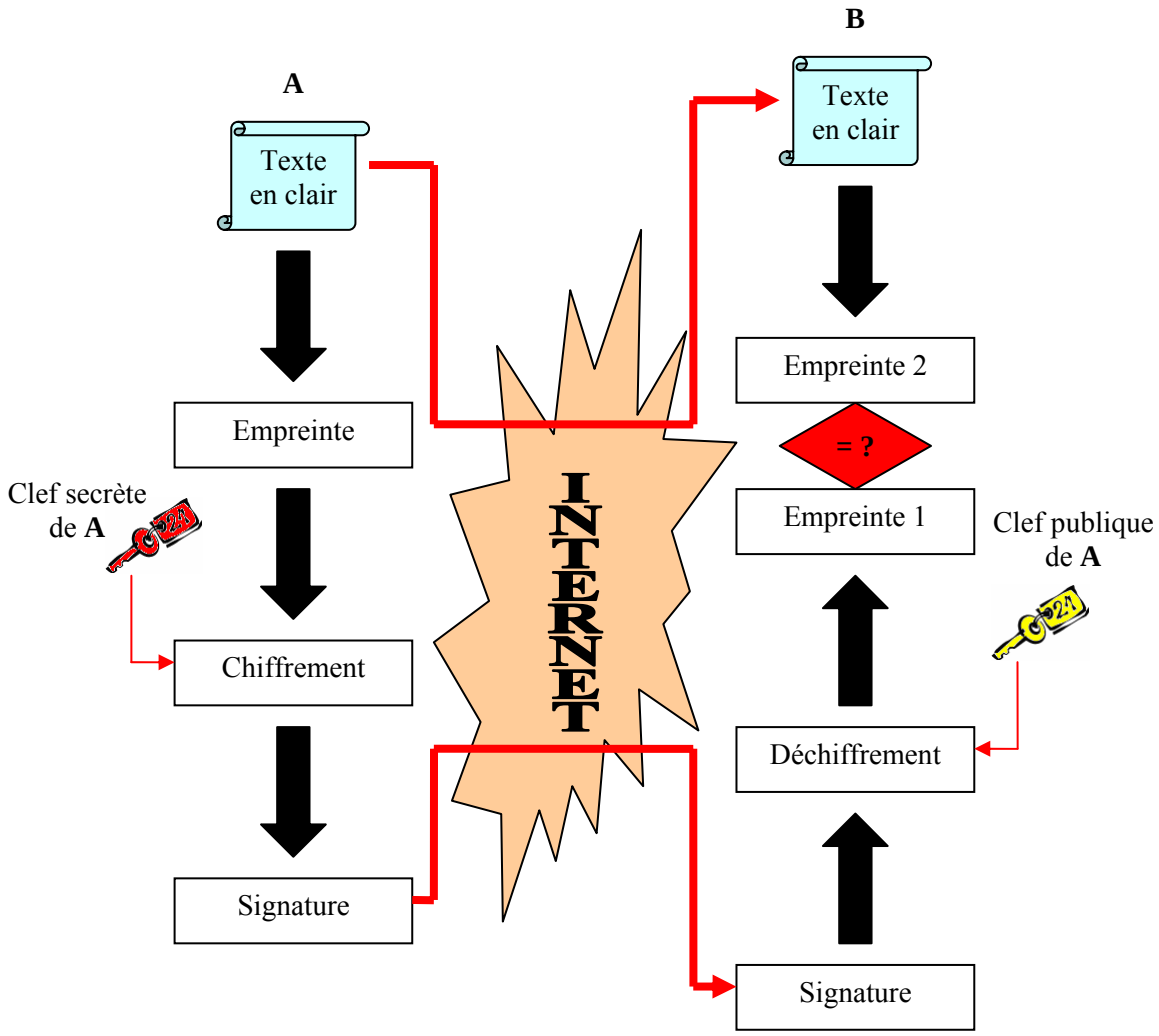
La signature numérique est une dématérialisation de la signature manuscrite par un code numérique qui assure la sécurisation technique et juridique des échanges électroniques.

Les signatures numériques (traduites parfois "digitales" ou "électroniques") sont fondamentales au niveau de l'authentification, de l'identification d'entité, de l'autorisation et de la non-répudiation. Le but est de fournir des moyens à une entité de pouvoir lier son identité à une information.

Son fonctionnement général est l'inverse du système à clef publique et implique aussi la paire de clefs publique/privée. Une personne voulant assurer le destinataire qu'il est bel et bien la bonne personne chiffrera un message avec sa clef privée et le destinataire déchiffrera le message chiffré avec la clef publique correspondante de l'expéditeur. Habituellement, une fonction de hachage est utilisée pour créer une empreinte du message et la transformation à l'aide de la clef privée est appliquée sur l'empreinte.

2.1. Fonctionnement :

- L'expéditeur calcule l'empreinte de son message à l'aide d'une fonction de hachage.
- L'expéditeur chiffre l'empreinte avec sa clef privée.
- L'expéditeur chiffre l'empreinte chiffrée avec le texte clair à l'aide de la clef publique du destinataire.
- L'expéditeur envoie le message chiffré au destinataire.
- Le destinataire déchiffre le message avec sa clef privée.
- Le destinataire déchiffre l'empreinte avec la clef publique de l'expéditeur.
- Le destinataire calcule l'empreinte du texte clair à l'aide de la même fonction de hachage que l'expéditeur.
- Le destinataire compare les deux empreintes.



Les systèmes de chiffrement à clef publique peuvent habituellement aussi servir à générer des signatures numériques. Néanmoins, le standard américain est le DSS, lequel spécifie trois algorithmes: le DSA (*Digital Signature Algorithm*), RSA et ECDSA (*Elliptic Curves Digital Signature Algorithm*).

Les algorithmes de signatures numériques ne sont jamais utilisés pour le chiffrement de données.

2.2. Propriétés :

Une signature numérique doit :

- dépendre du message signé.
- employer une information unique propre à l'expéditeur pour empêcher la contrefaçon et le démenti.
- être relativement facile à produire, à reconnaître et à vérifier.

- être mathématiquement infaisable à forger (par construction de nouveaux messages pour une signature numérique existante, ou par construction d'une signature numérique frauduleuse pour un message donné).
- être facile à stocker.

Enfin, la signature numérique est liée à la notion de *certificat numérique* (ou passeport électronique) qui est un petit fichier de 8 à 10 Ko qui voyage avec tous les envois certifiés et qui est public. Il identifie l'émetteur en fournissant le nom de la personne (Physique ou morale) associé à une clef publique.

Pour utiliser en confiance la clef publique d'un interlocuteur, il faut qu'elle soit certifiée par une autorité de confiance, appelé *Prestataire de Service de Certification Electronique* (PSCE) par les textes. En effet, contrairement à la signature manuscrite, la signature électronique ne comporte aucun élément permettant de l'attribuer à une personne donnée c'est pourquoi on recourt à des services de certification qui garantissent l'appartenance d'une signature à une personne.

4. INFRASTRUCTURE DE GESTION DE CLEFS

4.1. Besoin d'un organisme de gestion de clés :

L'utilisation massive de messages électroniques et l'expansion du commerce électronique dans le domaine professionnel comme privé est devenu une tendance de plus en plus populaire.

De ce fait, de plus en plus d'informations sensibles transitent par le réseau Internet, ces informations peuvent être sujettes à diverses attaques malveillantes comme la célèbre attaque du "l'homme du milieu" lorsque les intervenants échangent leurs clefs publiques lors d'un cryptage asymétrique. Dans une petite communauté, il pourrait être envisageable de générer sa paire de clés localement et d'échanger les clés publiques hors ligne, mais qu'en est-il pour une communication internationale où les échanges concernent des milliers d'utilisateurs. Dans ce cas de figure, une authentification automatique des clés publiques est indispensable.

C'est dans ce contexte que la NIST (*National Institut of Standards and Technologie*) s'est vu imposer en 1994 la tâche d'étudier et de définir un standard dans la manière de gérer l'authentification des clés publiques pour le territoire des Etats-Unis en premier lieu, puis ce standard devait être étendu à un environnement international. Le projet IGC (*Infrastructure de Gestion de Clefs*) est construit autours des discutions et d'interviews effectués auprès de divers agence fédérales, comité de standard et d'organisation commerciale. L'étude a porté sur la manière de générer les clefs, de les distribuer, d'obtenir les clefs publiques au moyen de certificats, et la publication des certificats obsolètes.

4.2. Définition :

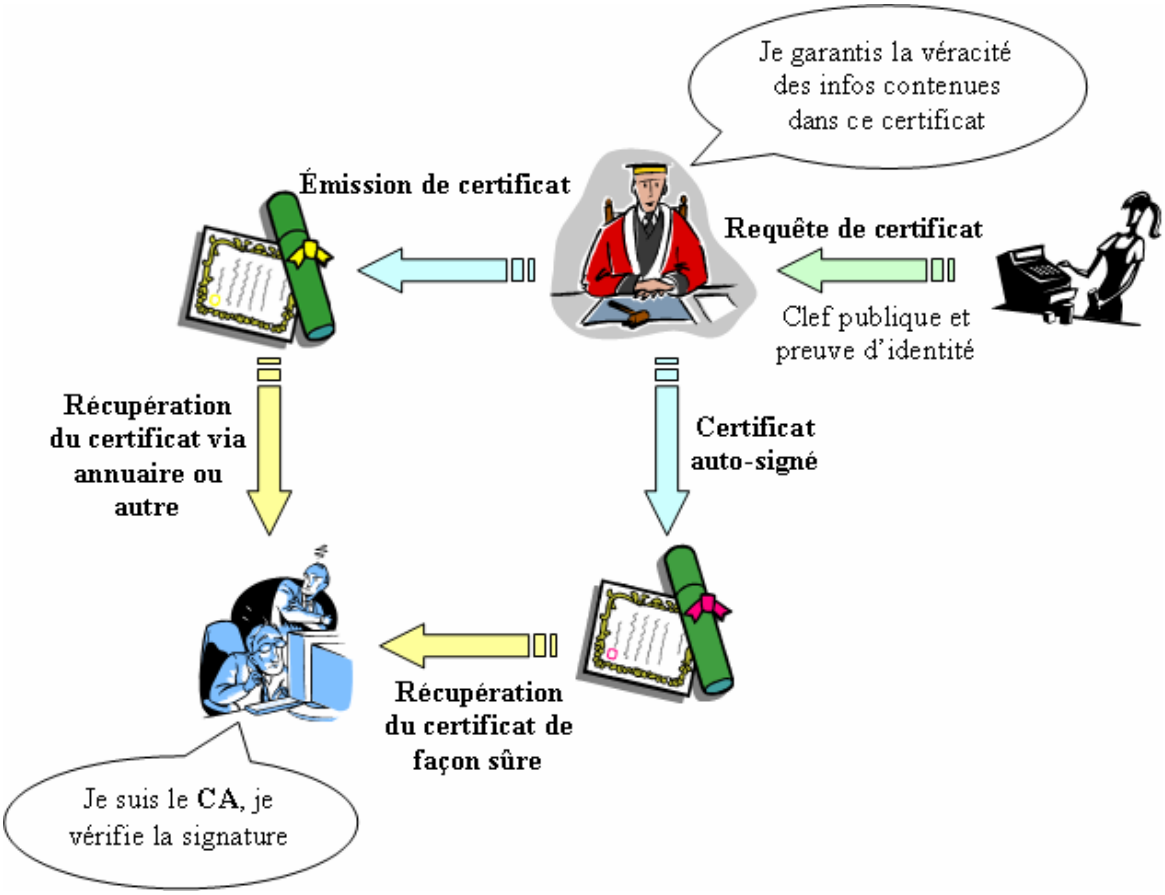
L'utilisation massive de la cryptographie à clef publique dans les échanges informatiques engendre un problème circonstanciel de taille. Peut-on être sûr du propriétaire ou est-ce « l'homme du milieu » ?

L'IGC permet de résoudre ce problème en permettant une authentification univoque des clefs publiques.

À la façon d'un passeport ou d'une carte d'identité, l'IGC va fournir une garantie d'identité numérique aux utilisateurs. Cette pièce d'identité numérique, appelée certificat numérique, contient la clef publique de l'utilisateur, mais également des informations

personnelles sur l'utilisateur du certificat. Comme tout document formel, le certificat numérique est signé par l'autorité de certification et c'est cette signature qui lui donnera toute crédibilité aux yeux des utilisateurs.

Mais contrairement à un passeport, le certificat numérique est largement publié, il n'a pas à être tenu secret, bien au contraire.



L'autorité de certification publiera le certificat signé comportant la clef publique et l'identité précise du propriétaire, quiconque consultera ce certificat aura l'assurance dans l'authenticité de la clef publique contenue dans celui-ci car il a confiance dans l'autorité de certification qui a délivré ce certificat. Par confiance il est entendu, que l'autorité est reconnue par l'utilisateur et que la clef publique de l'autorité soit préalablement connue.

4.3. Gestion de clefs :

Les organismes d'infrastructure à clef publique ont besoin d'une discipline rigoureuse dans la gestion des clefs, car il a été constaté qu'il est à l'heure actuelle beaucoup plus simple

de s'introduire dans un système en se procurant les clefs de manière illicite plutôt que d'essayer de casser un des algorithmes à clef asymétrique.

Et un des instants les plus propices pour oser espérer se procurer les clefs est sans conteste le moment où l'échange des clefs aura lieu, il en résulte que cet échange doit être fait avec la plus grande prudence car il représente le point de voûte de tout le système.

La gestion des clefs proprement dite se compose des opérations suivantes :

- **Génération :** il s'agit du moment où les clefs sont initialement crées. Les clefs sont générées de façon aléatoire, de manière à ce qu'elles soient non prédictibles.

- **Distribution :** la distribution est l'action de déplacer une clef de cryptage. Il existe deux étapes distinctes pour la distribution de clefs, créer la clef initiale et créer les clefs ultérieures. La clef initiale est établie et utilisée pour distribuer les autres clefs.

- **Stockage :** l'étape qui suit la distribution des clefs, est le stockage de la clef de façon sûre. La clef doit être protégée et doit garder à tout prix son intégrité et sa confidentialité.

- **Suppression :** la suppression de clefs intervient quand la clef à atteint sa fin de cycle, cela peut arrivé à la fin de sa validité soit une suspicion quant à la confidentialité de la clef pousse à la faire.

- **Archivage :** l'archivage des clefs permet de conserver une copie des clefs même si elles ne sont plus utilisées, le but est de pouvoir valider des données qui ont été précédemment protégées par la clef.

- **Recouvrement : l**e recouvrement des clefs est une procédure délicate qui permet de retrouver la clef privée d'un client. Elle peut être envisagée dans le cas où le client a perdu sa clef privée.

4.4. Composants d'une IGC :

L'IGC est une association de plusieurs composants qui interviennent à différentes étapes mises en œuvre depuis la création du certificat jusqu'à la l'utilisation de celui-ci.

- Autorité de certification RA (Registration Autority) ;
- Autorité de certification CA (Certification Autority) ;

- Application compatible IGC.

4.4.1. Autorité d'enregistrement (RA) :

Cette autorité à la tâche d'enrôler des nouveaux utilisateurs dans l'IGC, elle reçoit des utilisateurs candidats et les demandes de certificats CSR (Certificate Signing Request), ensuite elle à la responsabilité de vérifier la teneur de la demande.

Les méthodes de vérification utilisées dépendent de la nature du certificat demandé et de la politique de certification choisie. La vérification peut être limitée à l'identité du demandeur sur un formulaire HTML, mais on peut aussi vérifier s'il possède bien la clé privée associée, s'il a bien l'autorisation de son organisation pour demander ce type de certificat, etc. Les moyens mis en oeuvre pour assurer cette vérification peuvent aller du simple échange de courriers électroniques à une véritable enquête effectuée par les renseignements généraux.

Si la demande de certificats est acceptée, la demande est ensuite passée à l'autorité de certification CA qui n'a connaissance que des informations strictement indispensables à l'établissement du certificat. La requête est transmise suivant un format standardisé PCKS#10.

Il y a trois avantages à utiliser une autorité d'enregistrement indépendante de la CA au sein d'une IGC :

- Les centres d'enregistrement peuvent être distribués géographiquement.
- Séparer les opérations effectuées par le RA et le CA permet de séparer le processus de requête du processus de génération proprement dit et de signature.
- La tâche d'enrôler un nouvel utilisateur peut être très fastidieuse, surtout si la politique d'enregistrement est stricte. En déléguant cette opération à une autorité autonome, on soulage l'organisme de certification de manière sensible.

4.4.2. Autorité de certification (CA) :

Cette autorité est une autorité de confiance qui a pour but de créer les certificats des utilisateurs. La certification est l'opération qui consiste à lier l'identité d'un utilisateur à sa clef publique.

Le certificat généré contient entre autre le nom du demandeur (*Distinguished Name*), sa clef publique et une date d'expiration ainsi que la fonction du certificat.

La date d'expiration stipule la durée de validité du certificat, alors que la fonction précise dans quel contexte sera utilisé le certificat, par exemple pour un serveur HTTPS ou pour une signature S/MIME.

Le CA signe finalement le certificat créé à l'aide de sa clef privée. Etant donné que tout le système IGC est basé sur une chaîne de confiance, la clef privée de la CA est un élément vital qui doit être protégé par tous les moyens, de ce fait la CA n'est pas nécessairement connectée à Internet. Dans des IGC de grande envergure, la CA est confinée dans un bunker protégé par des mesures exceptionnelles (blindage, contrôle de température, contrôle d'intrusion), celle-ci est bien évidemment isolée complètement du réseau.

Suivant la politique de certification choisie, la CA peut prendre à sa charge une partie ou la totalité des opérations de la RA, c'est-à-dire vérifier l'identité de l'utilisateur et la teneur du certificat.

La CA garde une responsabilité sur la mise à jour des certificats qu'elle a générés, par exemple il est envisageable qu'un utilisateur change de secteur d'activité, rendant les informations contenues dans le certificat obsolètes, ou bien si l'utilisateur n'a plus confiance dans l'intégrité de sa clef privée; la CA doit prendre en compte cette modification en révoquant son certificat quand bien même le certificat n'a pas atteint sa date d'expiration.

La CA doit donc transmettre la liste des certificats révoqués (CRL) de la même manière que les certificats générés. Les applications devront donc contrôler systématiquement cette CRL lorsqu'un certificat numérique leur est présenté.

4.4.3. Application compatible IGC :

Un des plus grands avantages d'utiliser une IGC et plus particulièrement les certificats numériques pour l'authentification, est que la norme est supportée par un nombre d'équipements et de logiciels : navigateurs web, e-mails, VPN hardware et software, W2k login, etc.

Les deux navigateurs les plus communément utilisés qui sont Netscape Navigator et Microsoft Internet Explorer sont compatibles avec l'IGC. Ils permettent aux utilisateurs d'effectuer une génération de clefs et un téléchargement de certificats numériques.

Les logiciels de messagerie comme Microsoft Outlook et Netscape Messanger sont aussi compatibles avec l'IGC. Les utilisateurs peuvent signer leur courrier électronique par un simple clic de souris.

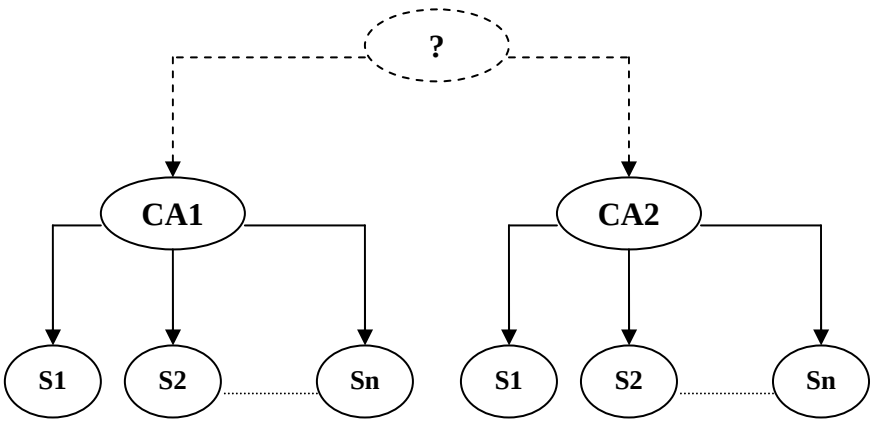
Grand nombre d'entreprises ont choisi une solution VPN (*Virtual Private Network*) pour interconnecter leurs différents réseaux. Le protocole IPsec peut utiliser les certificats numériques pour authentifier les intervenants.

Les utilisateurs qui accéderont à ces applications présenteront leur certificat numérique, soit directement à l'application, soit à une passerelle. Les applications vérifieront la teneur du certificat, d'une part à l'aide de la date de validité, puis en comparant la signature du certificat à l'aide des signatures de confiance déjà en leur possession. Puis, suivant les cas, l'application vérifiera dans la CRL si le certificat n'a pas été révoqué, et éventuellement les extensions ajoutées au certificat.

Ces étapes correspondent à la procédure de contrôle effectué lors d'un payement par carte de crédit: validité, signature et révocation.

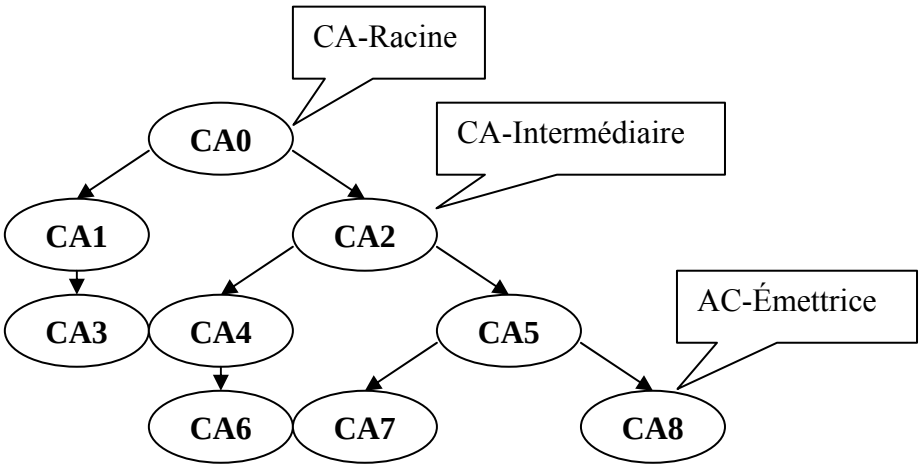
4.5. Répartition des CA :

Les certificats générés pour la population de la terre ne peuvent pas être issus d'une même CA, il est donc nécessaire de répartir le travail à travers plusieurs CA.



4.5.1. Modèle hiérarchique :

Le modèle hiérarchique présenté sur la figure suivante permet de résoudre ce problème.

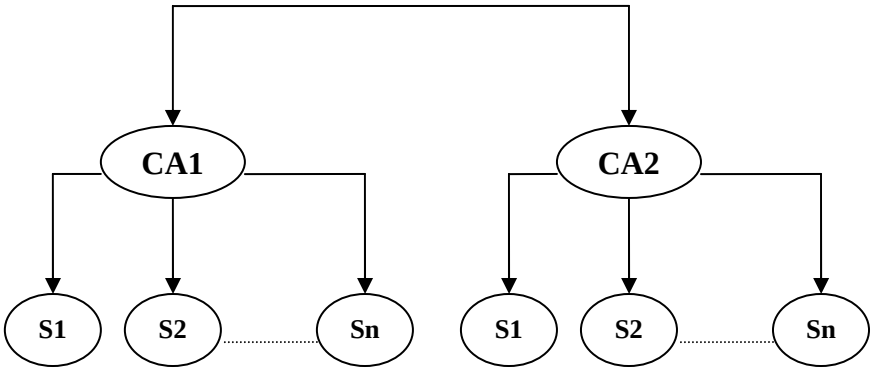


Les autorités CA1 et CA2 ont soumis leurs clefs publiques à un CA-Root qui leur a généré un certificat (CA1 et CA2 deviennent des CA subordonnées). L'autorité CA-Root peut être défini comme le plus haut niveau d'autorité; c'est le seul composant qui ait un certificat auto-signé. Un certificat auto-signé est le seul certificat qui permet d'assurer l'intégrité mais pas l'authenticité.

Ce modèle hiérarchique définit une relation entre la CA-Root et les CA subordonnés, une chaîne de confiance est ainsi établie. Les utilisateurs ont confiance dans la CA-Root, mais par la définition de la chaîne de confiance, ils ont également confiance dans les CA subordonnées. Etant donné que tout le système repose sur la confiance accordée au CA-Root, il est primordial que sa clef privée soit maintenue dans un endroit *absolument sûr*. La CA-Root représente un point de faiblesse potentiel de toute l'IGC, si la clef privée du CA-Root venait à être compromise, tous les certificats générés par les CA subordonnées deviendraient suspects avec toutes les implications dramatiques que cela produirait, tous les certificats devraient alors être retirés.

4.5.2. Modèle point à point :

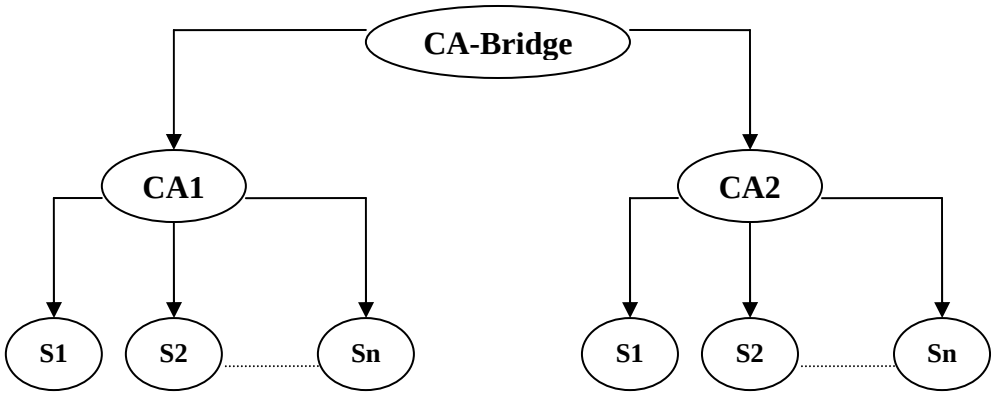
Dans ce modèle, les CA travaillent au même niveau hiérarchique, un ou plusieurs CA peuvent générer des certificats de manière croisée dans la relation point à point, les certificats ainsi générés portent le nom de certificats co-signés ou co-certifiés.



Les deux CA s'échangent mutuellement leurs clefs publiques; elles sont alors en mesure de générer un certificat pour leur homologue. Dans ce schéma, CA1 voit CA2 comme son CA-Root et réciproquement, il n'y a donc pas de point de faible unique. Toutefois étant donné que CA1 est responsable de l'authenticité de CA2, il se porte garant de tous les certificats délivrés par CA2, ce qui n'est pas une mince affaire suivant les politiques de certification.

4.5.3. Modèle en pont :

Le modèle hiérarchique a été jugé trop restrictif, ce qui a impliqué qu'aucune agence gouvernementale ne voulait porter la responsabilité d'être la CA-Root pour toutes les autres organisations. Le modèle de certification croisée, quant à lui, est difficile à mettre en œuvre lorsque le nombre de CA augmente. En effet, pour N autorités de certification, il fallait générer $N^2 - N/2$ certificats pour certifier toutes les autorités.



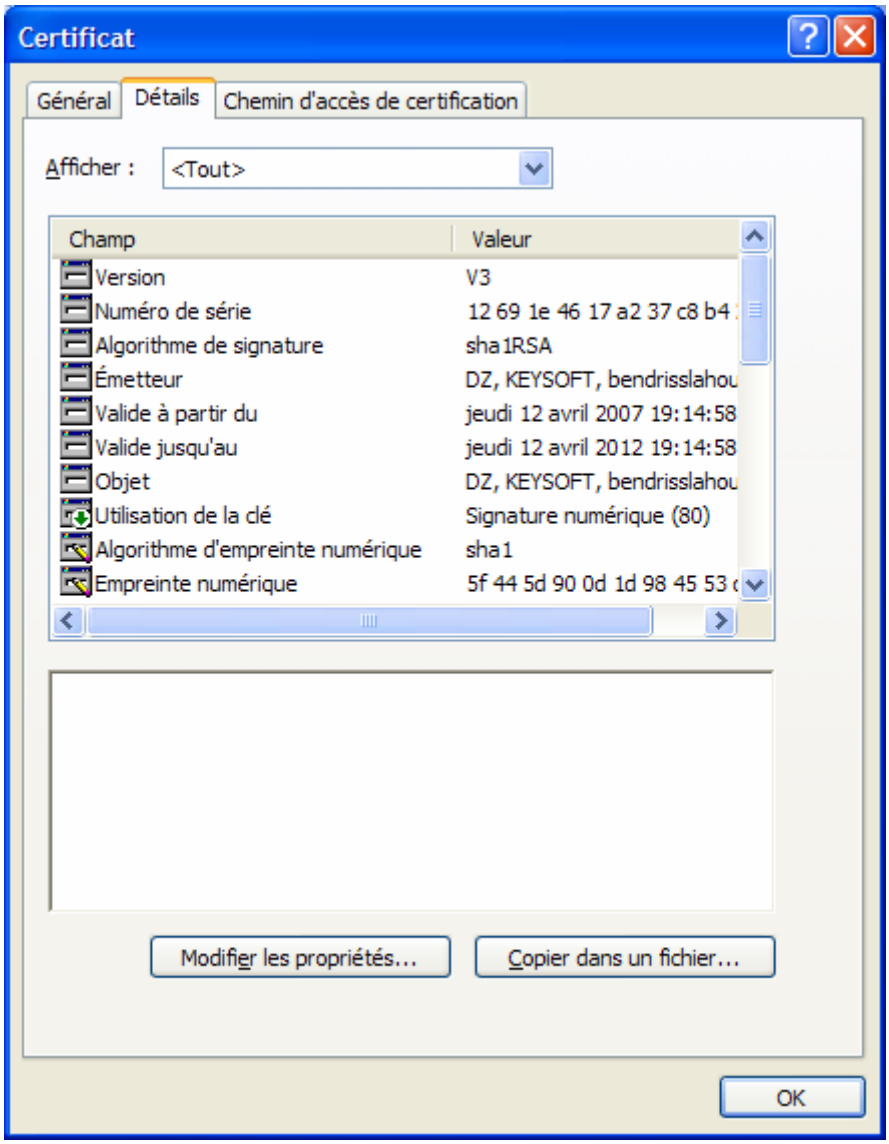
Dans ce modèle, CA1 et CA2 n'échangent leurs clefs publiques qu'avec la CA-Bridge, les échanges de certificats croisés suivent une complexité en N au lieu de N^2 pour le modèle sans pont. La politique de certification des CA doit être similaire afin d'assurer la compatibilité du modèle; cette remarque concerne bien évidemment le modèle de certification croisée précédent.

4.6. Le certificat X.509 :

Les utilisateurs de certificats étant de plus en plus nombreux, le format de ce certificat doit de ce fait, être commun à tous les utilisateurs. Sans cela, il serait impossible d'intégrer ces certificats dans des applications logicielles développées par des différents fournisseurs, pour cette raison, les certificats numériques sont soumis à un standard.

Le certificat X.509 fait l'objet d'une normalisation par l'ISO (*International Standard Organization*). Il a été réalisé par l'IETF (*Internet Engineering Task Force*) et est identifié par un DN (*Distinguished Name*). C'est concrètement un document électronique attestant qu'une clef publique est bien liée à une organisation, une personne physique, etc. Historiquement les certificats étaient utilisés pour protéger l'accès à des annuaires de type X.500. De ce fait, la structure d'un certificat X.509 se reflète à travers ses composants, le lien entre la nomenclature X.509 et X.500 est flagrant. Ce document électronique contient une clef publique, un certain nombre de champs à la norme X.509 et une signature. C'est la liaison des attributs des champs et la clef publique par une signature qui constitue un certificat. Un certificat peut être faux; c'est sa signature par une autorité de certification (CA) qui lui donne une authenticité.

Globalement, la composition d'un certificat X.509 est la suivante :



- *Version* : ce champ identifie à quelle version de X.509 correspond ce certificat.
- *Numéro de série* : numéro de série du certificat (propre à chaque autorité de certification).
- *Algorithme de signature* : algorithme utilisé pour signer le certificat.
- *Émetteur* : DN (*Distinguished Name*) de l'autorité de certification qui a émis ce certificat.
- *Valide à partir du/Valide jusqu'au* : c'est une paire de date pendant laquelle le certificat est valide.
- *Objet* : DN (*Distinguished Name*) du détenteur de la clef publique.
- *Algorithme de l'empreinte numérique* : le nom de l'algorithme à clef publique (RSA par exemple), ainsi que tous les paramètres concernent cette clef, et la clef proprement dite.
- *Utilisation de la clé* : extensions optionnelles introduites avec la version 2 de X.509.

- *Utilisation étendue de la clé* : extensions génériques optionnelles, introduites avec la version 3 de X.509.
- *Empreinte numérique* : signatures numériques de la CA sur l'ensemble des champs précédents.

Les extensions apportées par la version 3 du standard X.509 permettent de coupler un type et une valeur. Un paramètre supplémentaire "*témoin*" permet de déterminer si l'extension doit être prise en compte. Les extensions permettent de définir des profils de certificat: banques, organisations publiques, associations, etc.

4.7. Service de révocation :

Un certificat numérique, comme une carte de crédit doit pouvoir être révoqué si un changement d'identité du propriétaire a lieu, ou si la clef privée de l'utilisateur est perdue ou divulguée. Les certificats ne peuvent pas être détruits ou retirés car leurs présences peuvent apparaître à des milliers d'endroits chez les participants de l'IGC.

Dans ce cas, le service de révocation mis en œuvre par la CA doit enregistrer la demande de révocation et vérifier son authenticité. Une fois la vérification effectuée, la liste des certificats révoqués est publiée.

Il appartient aux clients utilisateurs de vérifier les listes de révocation pour les certificats qu'ils utilisent. La révocation est un élément du service de publication.

L'accès aux listes de révocation peut être spécifié dans le certificat sous forme d'une URL. Les clients peuvent alors téléchargés la liste de révocation (CRL). Mais étant donné que cette liste est générée périodiquement par la CA, son utilisation n'est pas optimale car les utilisateurs doivent mettre à jour constamment cette liste. Cette politique n'est pas sans risque en terme de sécurité. Pour contrer cet inconvénient les utilisateurs doivent disposer de la liste de révocation en temps réel, cette vérification est possible par l'intermédiaire d'un élément OCSP (*Online Certificate Status Protocol*) qui se chargera d'interroger la CA sur la validité d'un certificat. De ce fait, la liste de révocation de l'IGC est le seul élément devant disposer d'un service d'annuaire obligatoirement connecté à Internet.

4.8. Service de publication :

Le service de publication permet l'accès à des utilisateurs aux certificats des correspondants afin d'en extraire la clef publique.

L'utilisation du service de publication n'est pas requise pour toutes les applications de chiffrement asymétrique. En particulier, l'accès à un serveur HTTPS (*HyperText Transfer Protocol Secured*) dans le but de chiffrer les échanges ou d'authentifier le serveur ne requiert pas un accès au service de publication car le serveur HTTPS communique lui-même son certificat lors de la connexion SSL (Socket Secure Layer). De même, il est possible d'échanger des messages S/MIME (*Secure/Multipurpose Internet Mail Extensions*) sans utiliser le service de publication (l'envoi d'un message signé permet de faire parvenir automatiquement au correspondant son certificat). Toutefois, l'utilisation du service de publication est un élément déterminant dès que le nombre d'utilisateurs augmente. L'identité de la personne certifiée est définie dans un DN (*Distinguished Name*), elle constitue donc une clef d'accès dans l'annuaire LDAP (Lightweight Directory Access Protocol). Par ailleurs, LDAP est la seule API normalisée et donc utilisable dans le contexte hétérogène d'Internet.

4.9. Annuaire et IGC :

Souvent le service d'annuaire est mentionné dans le même cadre que l'IGC. Les systèmes implémentant une IGC disposent également d'un système d'annuaire permettant la publication des certificats, mais ces deux entités ne sont absolument pas dépendantes l'une de l'autre.

LDAP (*Lightweight Directory Access Protocol*) est le protocole Internet d'annuaire. Il a été développé à l'*Université du Michigan à Ann Arbor* (Etats-Unis) en collaboration avec l'IETF (*Internet Engineering Task Force*). Ce protocole LDAP permet de créer et de gérer des annuaires de personnes, de services, etc.

Un annuaire est composé de plusieurs entrées ou enregistrements et chaque entrée contient des informations descriptives. Ainsi, un annuaire peut contenir des entrées décrivant des personnes ou du matériel informatique comme des imprimantes par exemple. Un utilisateur peut ainsi utiliser le service d'annuaire pour retrouver le numéro de téléphone d'une personne ou récupérer une liste d'adresse e-mail par exemple.

Les informations sont stockées dans les différents champs de chaque enregistrement. Chaque champ contient un type d'information bien spécifique. Par exemple, ceux servant à enregistrer une personne peuvent être le nom, le prénom, l'adresse e-mail, etc.

Donnons un exemple d'enregistrement pour éclairer les choses: l'enregistrement pour *Bendriss Lahouari* peut être écrit comme suit:

cn: *Bendriss Lahouari*
givenName: *Lahouari*
e-mail: *bendrisslahouari@yahoo.fr*

Les attributs utilisés sont: *cn* pour "*common name*", c'est-à-dire le nom utilisé pour nommer la personne (généralement Nom et Prénom), *givenName* pour le prénom, et *e-mail* pour l'adresse e-mail (courrier électronique).

Remarque :

Un attribut peut avoir plusieurs valeurs. Une personne peut donc avoir deux numéros de téléphone ou deux "*common name*" (le nom et le prénom utilisés couramment puis le diminutif en deuxième *cn*). Ceci donnerait un enregistrement du type :

cn: *Bendriss Lahouari*
cn: *toto2007*
givenName: *Lahouari*
telephoneNumber: *+213 41 01 02 03*
telephoneNumber: *+213 90 11 12 13*
e-mail: *bendrisslahouari@yahoo.fr*

Les attributs peuvent aussi contenir des données binaires comme des photos au format JPEG (*Joint Photographic Experts Group*) ou la voix d'une personne enregistrée dans un fichier audio.

Il existe des opérations qui permettent aux clients de rechercher ou de modifier l'annuaire afin de le mettre à jour. Pour faire ces opérations, le client LDAP doit se connecter au serveur LDAP.

Le protocole LDAP prévoit aussi un contrôle d'accès simple. En effet, avant d'effectuer une opération qui modifie l'annuaire, l'utilisateur doit fournir un nom de type *dn* (appelé *rootdn*) et un mot de passe.

Le protocole LDAP est basé sur un modèle client/serveur. Les serveurs LDAP fournissent le service d'annuaire et les clients LDAP utilisent le service d'annuaire pour accéder aux données.

L'annuaire est comparable à une base de données dans son fonctionnement. Toutefois, le rôle d'un annuaire est de:

- stocker les certificats pour que ces derniers puissent être récupérés facilement par les utilisateurs et les applications.
- stocker la liste des révocations CRL.
- stocker les clefs privées dans le cas d'utilisation du recouvrement de clefs.

Pour être compatible avec l'IGC, l'annuaire doit répondre à deux critères :

- L'annuaire doit supporter le standard X.509v3 et permettre de stocker des CRL.
- L'annuaire doit supporter le protocole LDAP: le standard pour l'accès aux données par annuaire.

5. CONCLUSION

Actuellement Internet est une nécessité dans la vie courante, plus besoin de se déplacer pour acheter, pour faire des transactions commerciales ou pour travailler et tous cela ce fait d'un poste nomade. Certes tous cela facilite les tâches à chacun de nous mais il faut se méfier des malveillants qui exploitent leur intelligence et les vulnérabilités des systèmes mis en place pour détourner de l'argent ou des informations confidentielles.

Doit on arrêter le progrès ou trouver une solution ? Pour contrer se problème de sécurité la signature numérique est un tés bon remède, elle permet l'authentification et la confirmation de l'identité d'un utilisateur ou d'un service grâce au certificat qui lui a été délivré. Pour conclure nous pensons qu'il faut sensibiliser les personnes concernées à adopter cette méthode et comme on dit *la méfiance est mère de la sécurité*.

RÉFÉRENCES :

http://www.ietf.org/html.charters/pkix-charter.html

http://www.freeswan.org

http://www.signatureelectronique.be

http://www.formation.ssi.gouv.fr/autoformation/signature.html

http://www.ssi.gouv.fr/fr/sigelec/index.html

http://fr.wikipedia.org/wiki/Signature_num%C3%A9rique

http://www.simovits.com/eng/artarch.html

http://www.xcert.com/~marcnarc/PKI/thesir

http://www.hsc.fr/ressources/presentations/pki/img8.htm

http://pki.cru.fr

http://www.cdt.org/crypto/risks98/

http://www.ietf.org/rfc/rfc1321.txt

http://www.ietf.org/rfc/rfc2560.txt

http://www.ietf.org/rfc/rfc3174.txt

http://www.biometrics.org/REPORTS/cert.pdf