MASTER EN SCIENCES INFORMATIQUES

Infrastructure à clés publiques sous Windows 2000

De Belder, Nicolas

Award date:
2001

Facultés Universitaires Notre-Dame de la Paix, Namur
Institut d'Informatique.

Année académique 2000 - 2001

Infrastructure à clés publiques sous Windows 2000

Nicolas De Belder

Mémoire présenté en vue de l'obtention du grade de
Maître en Informatique.

Résumé

Avec l'émergence de nouveaux modes de communication tirant parti de l'ouverture des réseaux, les échanges d'informations et les possibilités de transactions se multiplient. Pour ces échanges, les individus doivent obtenir les mêmes garanties dans ce monde virtuel que dans le monde réel. C'est pourquoi il est nécessaire de disposer de moyens technologiques permettant d'authentifier les individus ainsi que d'assurer la confidentialité des informations. La cryptographie à clé secrète n'étant pas adaptée à de grands réseaux ouverts, la technologie à clé publique représente une alternative plus qu'avantageuse. Cependant, cette technologie à clé publique ne peut remplir son rôle d'une manière optimale que si elle est entourée d'une infrastructure bien définie.

Ce travail abordera progressivement les concepts importants des infrastructures à clés publiques pour permettre aux lecteurs de se familiariser avec cette technologie. Par la suite, il définira des critères d'évaluation afin de mettre en évidence les pré-requis indispensables de tels systèmes. A titre d'exemple, ces critères seront appliqués à deux types différents d'infrastructure à clés publiques.

Abstract

With the emergence of new methods of communication on open networks, information exchanges and transaction opportunities are increasing tremendously. People involved in such exchanges need to have the same level of confidence in this virtual world than in the real world. They thus need to be able to rely on technological means allowing people authentication and guaranteeing information confidentiality. As secret key cryptography is not suitable for large open networks, public key cryptography can be an extremely attractive alternative. However, the optimal implementation of public key technology requires a well-defined infrastructure.

In this paper, major concepts linked with public key infrastructure will be presented gradually to help readers familiarize with this technology. Evaluation criteria will then be defined in order to highlight the essential system components. As an example, those criteria will be applied to two different public key infrastructure systems.

Avant-propos

Je tiens tout d'abord à remercier mon promoteur, M. Jean Ramaekers, pour ses conseils ainsi que pour toute l'attention qu'il a accordée à la rédaction de ce mémoire.

Je remercie mes maîtres de stage, M. John Pyrgies et M. Chris Van der Straeten, de m'avoir fait bénéficier de leur expérience dans le domaine des infrastructures à clés publiques.

Je remercie aussi toutes les personnes que j'ai côtoyées lors de mon stage, parmi lesquelles Mme Vera De Breucker, M. Jean-Luc Bruwier, M. Pierre Rousseau, M. Jan Raes.

Je remercie tout particulièrement ma belle-sœur Marylène pour tout le temps qu'elle a consacré à la relecture de mon mémoire.

Enfin, je tiens à exprimer toute ma reconnaissance à mes parents, à mon frère ainsi qu'à toutes les personnes qui m'ont soutenu.

Table des matières

Table des figures

Glossaire

- **Active Directory** : Un répertoire de services inclus dans la version serveur du système d'exploitation Microsoft Windows 2000. Il stocke les informations à propos des objets sur un réseau et les rend accessibles aux utilisateurs et aux administrateurs réseaux.

- **Active Directory Service Interfaces (ADSI)** : Un ensemble d'interfaces qui permet aux applications (sous Windows 95, Windows 98, Windows NT et Windows 2000) d'accéder à différents services d'annuaires réseaux dont entre autres l'Active Directory.

- **American Standard Code for Information Interchange (ASCII)** : Un ensemble de caractères de 7 bits largement utilisés pour représenter les lettres et symboles trouvés sur les claviers U.S. Standards. Par la standardisation des valeurs utilisées pour ces caractères, ASCII permet aux ordinateurs et aux programmes de s'échanger de l'information.

- **Application Programming Interface (API)** : Un ensemble de routines que les applications utilisent pour demander et effectuer des services de bas niveau qui sont accomplis par le système d'exploitation de l'ordinateur.

- **Attaques** :

  - ***« Brute Force Attack »*** : Une attaque durant laquelle l'agresseur essaye toutes les combinaisons possibles de lettres, de chiffres et de symboles jusqu'à ce qu'il trouve le mot de passe.

  - ***« Buffer Overflow Attack »*** : Une attaque durant laquelle l'agresseur exploite les faiblesses d'un programme ou d'un service pour forcer une condition de « Buffer Overflow » et peut alors faire tourner un code malveillant (fourni par l'agresseur) dans la mémoire de l'ordinateur. Grâce à la réussite d'une « Buffer Overflow Attack », l'agresseur peut prendre le contrôle de l'ordinateur avec les droits et les permissions du système et de l'utilisateur qui était connecté.

  - ***« Denial of Service Attack »*** : Une attaque durant laquelle l'agresseur exploite une faiblesse ou une limitation d'un service d'un réseau pour surcharger ou arrêter le service, de sorte que le service ne soit plus disponible. Ce type d'attaque est généralement effectué pour empêcher les autres utilisateurs d'utiliser ce service réseau, comme par exemple des serveurs Web ou des serveurs de fichiers.

  - ***« Dictionary Attack »*** : Une attaque durant laquelle l'agresseur essaye des mots connus dans les dictionnaires et de nombreux noms habituels dans le but de deviner le mot de passe. Comme les personnes préfèrent des mots de passe faciles à retenir, ces attaques constituent souvent un raccourci pour trouver un mot de passe correct (elles prennent beaucoup moins de temps que les « Brute Force Attacks »).

  - ***« Factoring Attack »*** : Une attaque sur un algorithme de chiffrement à clés publiques dans laquelle l'agresseur essaye tous les facteurs possibles pour découvrir la clé

privée d'une paire de clés (publique/privée). Cette attaque est similaire à la « Key Search Attack » qui peut être effectuée sur les algorithmes de chiffrement à clés symétriques, mais le nombre de facteurs possibles varie par rapport au cas des algorithmes à clés publiques.

- *« Key Search Attack »* : Une attaque consistant à essayer tous les mots de passe ou clés possibles (clés symétriques uniquement) jusqu'à ce que le mot de passe correct ou la clé soit découvert. Aussi appelée « Brute Force Attack ».

- **Certificats X.509 Version 3** : Un standard concernant le format des certificats utilisés par les processus basés sur des certificats de Windows 2000. Un certificat X.509 contient la clé publique ainsi que des informations à propos de la personne ou de l'entité possédant ce certificat, des informations à propos du certificat et des informations optionnelles relatives à l'autorité de certification (CA) qui a émis le certificat.

- **Cryptographic Service Provider (CSP)** : Un module logiciel indépendant qui effectue des opérations cryptographiques comme l'échange de clés secrètes, la signature numérique de données et l'authentification à clés publiques.

- **Data Decryption Field (DDF)** : Un champ d'en-tête, dans un fichier chiffré au moyen de l'Encrypting File System (EFS), qui contient la clé symétrique qui a servi à chiffrer le fichier. Ce champ est chiffré avec la clé publique du propriétaire du fichier.

- **Data Recovery Field (DRF)** : Un champ d'en-tête, dans un fichier chiffré au moyen de l'Encrypting File System (EFS), qui contient la clé symétrique qui a servi à chiffrer le fichier. Ce champ est chiffré avec la clé publique d'un « Recovery Agent ».

- **Encrypting File System (EFS)** : Un nouveau dispositif dans Windows 2000 qui protège les données sensibles dans des fichiers qui sont stockés sur des disques utilisant le système de fichier NTFS. Il utilise le chiffrement à clés symétriques conjointement avec la technologie à clés publiques pour garantir la confidentialité des fichiers. Il tourne comme un service intégré au système, ce qui rend EFS facile à gérer, difficile à attaquer et transparent pour le propriétaire du fichier et pour les applications. Ce dispositif sera vu plus en détail dans le chapitre 2 au point 2.3.5.

- **File Transfer Protocol (FTP)** : Un protocole Internet standard pour le téléchargement (ou le transfert) de fichiers d'un ordinateur à un autre.

- **Hash Message Authentication Codes (HMAC)** : Un mécanisme qui génère un condensé du message pour chaque bloc de données transmis et utilise une clé symétrique aléatoire pour chiffrer ces condensés. La clé secrète est partagée de manière sécurisée entre les deux parties impliquées dans cette communication sécurisée. Quand la donnée est réceptionnée, la clé secrète est nécessaire pour déchiffrer le condensé du message et effectuer un contrôle d'intégrité des données.

- **Hardware Security Module (HSM)** : Un module matériel de sécurité résistant aux intrusions qui est connecté à un ordinateur hôte comme périphérique. Le HSM met à la

disposition de l'hôte un environnement sécurisé dans lequel il va effectuer ses processus cryptographiques.

- **Hypertext Transfer Protocol (HTTP)** : Un protocole à la base de la communication entre les clients et les serveurs sur Internet.

- **Information Technology Security Evaluation Criteria (ITSEC)** : Un système d'évaluation du niveau de sécurité atteint par des produits. Tous les produits autorisés à utiliser le label ITSEC ont atteint un certain niveau prédéterminé de fonctionnalité et de sécurité. Il existe six niveaux de sécurité allant de E0 (représentant un système avec un degré de confiance inadéquat) à E6 (désignant un produit pratiquement parfait). Pour les infrastructures à clés publiques, il est souhaitable que le système soit certifié au moins pour le niveau E3. Pour plus d'informations, allez voir sur le site Internet : http://www.itsec.gov.uk.

- **Internet Engineering Taskforce (IETF)** : Un groupe chargé de la définition et de l'entretien de standards techniques et de protocoles pour Internet.

- **Internet Protocol Security (IPSec)** : Un ensemble de services et de protocoles de protection basés sur la cryptographie.

- **Kerberos** : Un protocole permettant un usage sécurisé pour les logiciels distribués et basé sur la cryptographie à clés symétriques. Le protocole d'authentification Kerberos donne un mécanisme d'authentification mutuelle entre un client et un serveur ou bien entre un serveur et un autre, avant qu'une connexion réseau ne soit ouverte entre eux. Ce protocole sera vu plus en détail dans le chapitre 3.

- **Key Distribution Center (KDC)** : Un service réseau qui distribue des tickets de session et des clés de session temporaires utilisés dans le protocole d'authentification Kerberos. Dans Windows 2000, le KDC tourne comme processus privilégié sur tous les contrôleurs de domaine. Le KDC utilise l'Active Directory pour gérer les informations sensibles sur les comptes comme les mots de passe pour les comptes utilisateurs.

- **Lightweight Directory Access Protocol (LDAP)** : Un protocole utilisé pour l'accès à un répertoire (directory). C'est l'accès principal à l'Active Directory.

- **Multipurpose Internet Mail Extensions (MIME)** : Une méthode habituelle de transmission de données non-textuelles via du courrier électronique. MIME encode les données non-textuelles en texte ASCII et les décode dans leur format original lors de leur arrivée à destination. Un en-tête MIME est ajouté au fichier ; cet en-tête reprend le type de données que le message contient ainsi que la méthode d'encodage utilisée.

- **Online Certificate Status Protocol (OCSP)** : Un moyen permettant aux applications de déterminer l'état d'un certificat déterminé, c'est-à-dire de voir s'il a été révoqué ou non. Pour plus d'informations, allez voir sur le site Internet : http://www.ietf.org/rfc/rfc2560.txt.

- **PC/SC smart card specification** : Un standard ouvert pour les cartes à puce et les lecteurs de cartes publié par le groupe de travail PC/SC, un consortium de fabricants de logiciels et de matériels informatiques.

- **Public Key Cryptography Standards (PKCS)**[1] : Une famille de standards pour la cryptographie à clés publiques qui inclut le chiffrement RSA, la convention des clés de Diffie-Hellman, le chiffrement basé sur les mots de passe, la syntaxe des messages cryptographiques, la syntaxe des informations de la clé privée et la syntaxe des requêtes de certificats. Ils sont développés, détenus et gérés par « RSA Data Security ».

    - **PKCS #1 :** décrit une méthode pour le chiffrement et le déchiffrement RSA, principalement pour construire des signatures numériques et des enveloppes digitales décrites dans le standard PKCS #7.
    - **PKCS #7 :** décrit une syntaxe générale pour les données pouvant être chiffrées ou signées, comme les signatures numériques ou enveloppes digitales.
    - **PKCS #10 :** décrit une syntaxe standard pour les demandes de certificats.
    - **PKCS #11 (Cryptographic Token Interface Standard « Cryptoki ») :** définit la notion de système de sécurité cryptographique et l'API (aussi appelée Cryptoki) destinée à uniformiser les interfaces pour ces systèmes de sécurité. Les API font le lien avec les dispositifs qui conservent les données cryptographiques et qui effectuent les opérations cryptographiques.
    - **PKCS #12** : décrit la syntaxe utilisée pour le stockage logiciel des clés publiques des utilisateurs, la protection des clés privées, des certificats et toutes les autres informations relatives au chiffrement.

- **Public Key Infrastructure X.509 (PKIX)** : Un standard industriel soutenu par l'IETF pour les applications de l'infrastructure à clés publiques.

- **Recovery Agent** : Un compte utilisateur qui peut être utilisé pour déchiffrer un fichier chiffré en utilisant l' « Encrypting File System » (EFS) si la clé de déchiffrement du propriétaire du fichier est indisponible.

- **Réplication « multimaster »** : Un système de réplication dans lequel toutes les reproductions d'une partition d'un annuaire donné sont modifiables, acceptant que les mises à jour soient appliquées à n'importe quelle reproduction. L'Active Directory utilise ce système de réplication et réplique automatiquement et de manière transparente tous les changements d'une représentation donnée vers toutes les autres reproductions. Ce modèle varie des autres modèles de réplication dans lesquels un ordinateur garde l'unique copie modifiable de l'annuaire tandis que les autres ordinateurs gardent des copies de sauvegarde.

- **Secure/Multipurpose Internet Mail Extensions (S/MIME)** : Une extension de MIME pour supporter le courrier électronique sécurisé. Il autorise l'expéditeur à signer numériquement les messages pour prouver l'origine et l'intégrité de ceux-ci. Il permet également le chiffrement des messages pour garantir la confidentialité des communications.

---

[1] Source bibliographique : *[APC95]* p. 588

- **Secure Sockets Layer (SSL)** : Un protocole qui fournit des communications sécurisées de données au moyen du chiffrement et du déchiffrement. SSL utilise le chiffrement à clés publiques RSA pour des ports TCP/IP spécifiques. SSL est une méthode alternative à Secure-HTTP (S-HTTP) qui est utilisée pour le chiffrement de documents spécifiques World Wide Web plutôt que pour une session entière. Il peut être utilisé pour des applications Web exigeant un lien sécurisé, comme les applications d'e-commerce ou bien pour contrôler l'accès à certains services.

- **Simple Certificate Enrollment Protocol (SCEP)** : Un protocole dont le but est de supporter l'émission sécurisée de certificats à destination de dispositifs réseaux d'une manière pouvant évoluer, tout en utilisant, lorsque c'est possible, les technologies existantes. Pour plus d'informations, allez voir le site Internet : http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm.

- **Smart Card** : Un dispositif de la taille d'une carte de crédit qui est utilisé avec un code PIN pour autoriser l'authentification sur la base de certificats. Ces cartes à puce stockent en toute sécurité les certificats, les clés publiques et privées, les mots de passe et d'autres types d'informations personnelles.

- **Ticket-Granting Tickets (TGT)** : Une donnée issue par le KDC pour un utilisateur quand celui-ci ouvre une session. L'utilisateur doit présenter le TGT au KDC quand il demande un ticket de session pour un service.

Introduction

L'infrastructure à clés publiques, plus communément appelée PKI (Public Key Infrastructure), a pour but premier de permettre aux utilisateurs de réseaux publics, dont principalement Internet, de pratiquer le commerce électronique.

En effet, à l'époque actuelle, Internet se répand de plus en plus à travers le monde et rencontre un intérêt très important chez beaucoup de personnes et de sociétés. Les entreprises voient dans Internet une opportunité non négligeable de s'ouvrir vers le monde en développant un nouveau moyen de fournir leurs services.

Mais cette opportunité n'est pas sans risque sur un réseau public tel qu'Internet. Les communications entre les différents ordinateurs sur Internet se font via d'autres ordinateurs intermédiaires, il est toujours possible qu'une personne mal intentionnée intercepte la communication pour en tirer profit. Cette interception peut se faire de différentes manières :

- **Espionnage** : Les informations restent intactes mais leur confidentialité est compromise.

- **Détournement** : Les informations sont changées, remplacées ou détournées entre l'expéditeur et le destinataire.

- **Usurpation d'identité** : Une personne peut prétendre être une autre personne en vue d'actes malhonnêtes.

La sécurité sur ces réseaux est donc très importante dans le cas où un commerce électronique voudrait démarrer. Sans cette sécurité, il sera très difficile pour les entreprises de tirer profit de ce nouveau marché. Il est donc nécessaire d'avoir les mêmes niveaux de confiance dans ce mode électronique que dans le monde réel.

C'est l'infrastructure à clés publiques qui va permettre aux entreprises de tirer pleinement parti de ce nouveau marché sur les autoroutes de l'information.

Le commencement de l'utilisation des infrastructures à clés publiques date du début des années 90. A ce moment, le système PGP[2] utilisait déjà sa propre version de l'infrastructure à clés publiques pour authentifier les utilisateurs. Cependant, cette technologie n'était pas encore très répandue. Ce n'est qu'à partir de la fin des années 90 que ce système a commencé à se développer, mais dans de faibles proportions. La raison principale réside dans le fait qu'à cette période, les systèmes étaient difficiles à utiliser et à gérer et que la transparence d'utilisation pour les utilisateurs était quasi inexistante. De plus, le nombre d'applications pouvant tirer parti de l'infrastructure à clés publiques était très restreint ; il fallait donc attendre de nouvelles versions de ces applications supportant cette technologie.

A la fin des années 90, l'avènement des réseaux et surtout d'Internet a ouvert la porte à de nouvelles possibilités de communication et de commerce nécessitant une sécurité de plus en

[2] Pretty Good Privacy

plus importante. En outre, l'avancement du développement des applications et des systèmes à clés publiques du point de vue facilité et transparence d'utilisation a favorisé l'adoption de tels systèmes.

Ce travail se base sur l'expérience acquise lors d'un stage de fin d'études effectué au début de l'année académique 2000-2001 dans une institution financière de la Région bruxelloise. Durant cette période, j'ai eu l'occasion d'utiliser les différents logiciels étudiés dans la suite de ce document, ce qui m'a permis de découvrir leurs différentes fonctionnalités ainsi que de me faire une idée des avantages et inconvénients de chacun d'entre eux. De plus, de longues recherches sur Internet et dans la documentation disponible pendant ce stage m'ont aidé à approfondir les différents points examinés.

Ce mémoire abordera les différents concepts importants d'une infrastructure à clés publiques après avoir défini les concepts cryptographiques sur lesquels repose cette infrastructure. Parmi ces concepts importants, on retrouve les certificats électroniques, les composants de l'architecture, comme les autorités de certification, ainsi que les différentes applications tirant parti de cette technologie. Par la suite, les aspects de sécurité du système d'exploitation Microsoft Windows 2000 seront passés en revue pour définir l'environnement dans lequel les systèmes d'infrastructures à clés publiques ont été analysés.

Du fait du nombre croissant de systèmes différents d'infrastructures à clés publiques, il est indispensable d'établir des critères d'évaluation pour déterminer la solution la plus appropriée aux exigences des parties concernées. Ces critères seront ensuite appliqués à deux systèmes bien différents : UniCERT de Baltimore Technologies et la Windows 2000 PKI de Microsoft. Enfin, ce mémoire abordera une méthode de test, du nom de *Test Requirement Hierarchy*, pour souligner l'importance de procéder à la vérification du bon fonctionnement de l'infrastructure dans son ensemble avant sa mise en place.

Chapitre 1 : La cryptographie

Ce premier chapitre abordera les différents aspects de la cryptographie à clé secrète et à clé publique afin d'expliquer les mécanismes qui sont à la base des infrastructures à clés publiques. Les sources bibliographiques utilisées sont : *[BtInt00], [CertPCrypt], [HAC96], [iPlan00], [MsCry&Pki], [MsPkiInt], [MsRkit00b], [RSA00].*

Définition 1.1 : « La cryptographie, c'est l'étude de techniques mathématiques liées aux aspects de la sécurité de l'information comme la confidentialité, l'intégrité des données, l'authentification des sujets et l'authentification de l'origine des données ».[3]

Traditionnellement, la cryptographie était utilisée pour permettre des communications sécurisées entre les individus, les gouvernements et l'armée. Aujourd'hui, la cryptographie est un élément important des technologies modernes de sécurité employées pour protéger les informations et les ressources à la fois des réseaux ouverts et fermés.

La cryptographie sert donc à protéger des informations lors d'échanges sur ces réseaux. Pour ce faire, ces informations peuvent être chiffrées et déchiffrées ensuite. Le chiffrement consiste à transformer les données de telle sorte qu'il soit pratiquement impossible de les lire sans avoir la clé de déchiffrement. Les données sont ainsi rendues inutilisables pour les personnes non concernées, alors que celles-ci ont accès aux informations sous leur forme chiffrée.

Un autre aspect de la cryptographie très important dans la vie de tous les jours est l'authentification (quand on doit signer des documents par exemple). Dans le monde électronique, il est également indispensable d'avoir un moyen de s'authentifier pour des transactions électroniques. C'est ce que propose la cryptographie avec les signatures numériques qui lient un document à une personne possédant la clé ainsi que le « timbre dateur » qui lie le document avec le moment auquel il a été créé.

Définition 1.2 : « La signature numérique est une primitive cryptographique qui est fondamentale dans l'authentification, l'autorisation et la non-répudiation. Le but de la signature numérique est de fournir un moyen à une entité de lier son identité à une information ».[4]

L'objectif de la cryptographie n'est pas de fournir une protection sans faille, ce qui serait impossible à atteindre, mais de protéger les informations en rendant l'accès non autorisé à celles-ci ou en rendant l'espionnage plus coûteux que la valeur potentielle que cela pourrait rapporter.

---

[3] Source bibliographique : *[HAC96]*, Chapitre 1 p. 4

[4] Source bibliographique : *[HAC96]*, Chapitre 1 p. 22

La cryptographie offre les fonctions de base suivantes :

- **Confidentialité de l'information** : assurance que seules les personnes autorisées pourront lire ou utiliser les informations confidentielles. Les systèmes de cryptographie utilisent des techniques pour assurer la confidentialité de l'information. Les utilisateurs non autorisés sont susceptibles d'intercepter les informations mais celles-ci sont transmises sous forme chiffrée, ce qui les rendent inutilisables sans la clé de déchiffrement qui n'est connue que des utilisateurs autorisés impliqués dans cette communication.
- **Intégrité des données** : vérification que le contenu original de l'information n'a pas été modifié ou corrompu. Sans cette intégrité, une personne pourrait modifier une information sans que cela puisse être détecté ! Les signatures numériques permettent d'assurer l'intégrité de toutes les informations échangées.
- **Authentification des utilisateurs** : vérification de l'identité des parties qui communiquent à travers un réseau. Sans cette authentification, une personne sur le réseau dotée d'un accès peut facilement se faire passer pour quelqu'un d'autre. Les systèmes cryptographiques utilisent des techniques pour authentifier à la fois l'expéditeur et le destinataire d'une information. Les signatures numériques et les certificats électroniques d'utilisateurs permettent d'assurer l'authentification de toutes les personnes et ressources.
- **Non-répudiation** : assurance qu'une partie impliquée dans une communication ne peut nier avoir pris part à la transaction. Avec une signature numérique valide et le certificat électronique qui l'accompagne, les risques que le message soit falsifié ou qu'il vienne d'ailleurs sont vraiment très faibles.

Cependant, la cryptographie ne peut pas tout faire. La cryptographie apporte seulement une partie de la sécurisation des réseaux et de l'information. La force d'un système de sécurité dépend de beaucoup de facteurs, comme l'adéquation de la technologie, des procédés et procédures de sécurité et la manière dont les personnes utilisent ces procédés, procédures et technologies.

Il existe deux méthodes cryptographiques de chiffrement : la cryptographie à clé symétrique (clé secrète) et la cryptographie à clé asymétrique (clé publique). Le plus souvent, ces deux techniques sont utilisées conjointement pour sécuriser les réseaux et les informations.

1.1 Cryptographie symétrique : clé secrète

Dans la cryptographie symétrique ou à clé secrète, une clé est une combinaison unique de nombres que les algorithmes de cryptographie utilisent pour chiffrer et déchiffrer des informations.

Cette clé unique est possédée par les deux protagonistes de l'échange. La sécurité de ce processus dépend de la sécurité liée à la clé, une personne qui n'est pas autorisée à participer à la communication ne peut avoir accès à cette clé. Les deux parties doivent s'échanger cette clé de façon très sécurisée avant de commencer à s'échanger des données chiffrées. Car si la clé a pu être interceptée par une tierce personne, cette dernière peut accéder à toutes les données chiffrées mais aussi envoyer des messages chiffrés à une des parties en se faisant passer pour la seconde qui utilise habituellement cette clé.

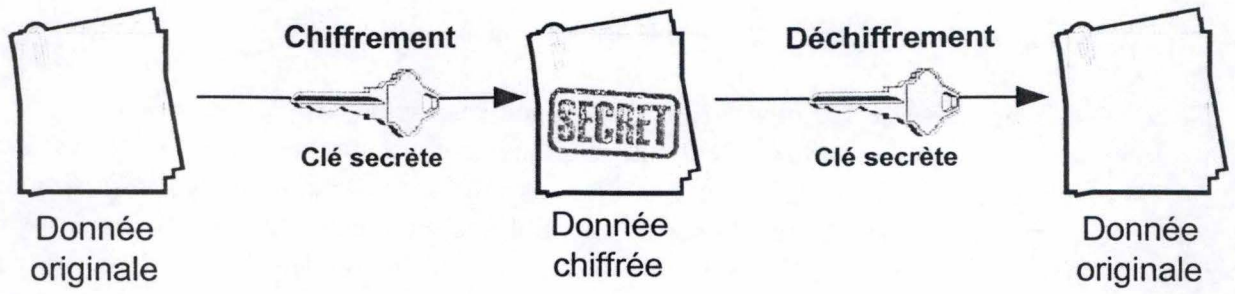

Figure 1 : Cryptographie symétrique

1.2 Cryptographie asymétrique : clé publique

Dans la cryptographie asymétrique ou à clé publique, c'est une paire de clés qui est utilisée dans les échanges. Il y a d'une part la clé publique qui peut être distribuée aux autres personnes, et d'autre part la clé privée qui doit rester secrète et qui est seulement utilisée par le possesseur de la paire de clés. Cette paire est bien sûr unique, c'est-à-dire qu'à une clé privée donnée correspond une et une seule clé publique et inversement.

La gestion des clés est plus aisée dans ce cas-ci vu que la clé publique peut être distribuée. Si une personne veut envoyer des données chiffrées à une autre personne, il lui suffit de prendre la clé publique du destinataire et celui-ci pourra déchiffrer les données au moyen de sa clé privée. En effet, des données chiffrées avec une clé publique ne peuvent être déchiffrées qu'avec la clé privée associée et des données chiffrées avec une clé privée ne le peuvent qu'avec la clé publique correspondante.

Cette paire de clés permet non seulement de chiffrer des informations mais aussi de s'authentifier. L'expéditeur peut utiliser sa clé privée pour faire une signature numérique. Celle-ci sera vérifiée par le destinataire à l'aide de la clé publique de l'expéditeur du message. Par ce moyen, le destinataire sera certain de l'origine du message.

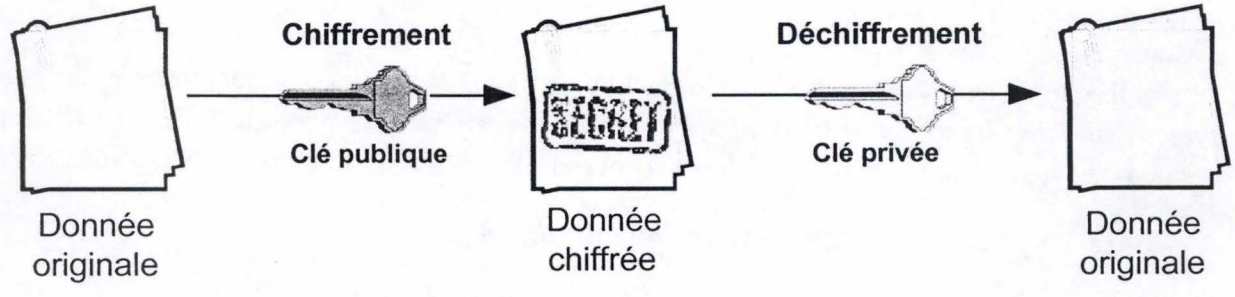

Figure 2 : Cryptographie asymétrique

1.3 Comparaison des deux techniques

Le premier avantage de la cryptographie à clé publique est l'augmentation de la sécurité liée à la gestion des clés. En effet, la clé privée ne doit jamais être transmise ou révélée à quiconque. Dans la cryptographie à clé secrète, la clé secrète doit être transmise entre plusieurs personnes pour établir un échange de données sécurisé. La difficulté d'établir un tel échange augmente le risque qu'une tierce personne puisse avoir accès aux données chiffrées après interception de la clé secrète.

Un autre avantage de la cryptographie à clé publique est qu'elle apporte les signatures numériques qui ne peuvent être reniées. L'authentification dans la cryptographie à clé secrète exige le partage d'un secret (la clé) entre plusieurs parties. Une des parties peut renier un message précédemment authentifié si le secret a été d'une façon ou d'une autre compromis. Par contre, dans le cas de la cryptographie à clé publique, chaque utilisateur est seul responsable de la protection de sa clé privée, il n'est donc pas possible de renier une authentification.

Un troisième avantage de la cryptographie à clé publique est la gestion des clés. Dans le système symétrique, si une personne veut communiquer de manière sécurisée avec plusieurs autres, il lui faudra posséder autant de clés secrètes que de personnes avec qui elle veut dialoguer. La gestion de ces clés secrètes devient rapidement très lourde et donc source de défaillance. Par contre, avec les clés publiques, il suffit de connaître la clé publique pour communiquer en sécurité. Cela facilite grandement la gestion des clés privées qui sont sous l'unique responsabilité de leur détenteur.

Un désavantage de la cryptographie à clé publique réside dans la lenteur du chiffrement. Les algorithmes à clé secrète sont souvent plus rapides. C'est pourquoi la cryptographie à clé secrète est souvent utilisée pour de grandes quantités de données et celle à clé publique, pour des données sensibles. La meilleure solution étant de combiner ces deux méthodes pour en tirer le plus d'avantages. En effet, dans ce cas la clé secrète peut être chiffrée avec la clé publique du destinataire pour être transmise, puis c'est cette clé secrète qui sera utilisée dans les échanges ; on parle alors de « clé de session ».

Dans certain cas, la cryptographie à clé publique n'est pas nécessaire et celle à clé secrète est suffisante. C'est principalement vrai dans des environnements où les échanges de clés secrètes peuvent se faire de manière sécurisée et où il n'y a pas beaucoup d'utilisateurs. La cryptographie à clé publique est quant à elle destinée à des environnements ouverts multi-utilisateurs.

1.4 Algorithmes et longueurs de clés utilisés

La force du chiffrement est en rapport avec la difficulté liée à la découverte de la clé, qui à son tour dépend de l'algorithme de chiffrement utilisé et de la longueur de la clé. Pour chacune des méthodes vues précédemment, il existe plusieurs algorithmes.

1.4.1 Algorithmes pour la cryptographie à clé secrète

- « Block cipher »

Ce type d'algorithme de chiffrement à clé symétrique transforme un bloc de données (non chiffrées) en des blocs de données (chiffrées) de longueur fixe. Cette transformation utilise la clé secrète fournie par l'utilisateur. Le déchiffrement s'effectue par la transformation inverse, à partir des données chiffrées, avec la même clé secrète. Le chiffrement avec ce type d'algorithme donnera toujours le même résultat sur des données identiques si on utilise la même clé secrète.

Exemple : DES , RC2

➢ « Stream cipher »

Ce type d'algorithme de chiffrement à clé symétrique a été conçu pour être très rapide, plus rapide que l'algorithme ci-dessus. Un algorithme « block cipher » travaille sur de larges blocs de données, tandis qu'un algorithme « stream cipher » travaille sur des éléments plus petits, généralement des bits. Dans cet algorithme, la transformation de ces données en clair va varier selon le moment où elles ont été rencontrées lors du processus de chiffrement.

1.4.2 Algorithmes pour la cryptographie à clé publique

➢ « RSA » : Rivest-Shamir-Adleman

Cet algorithme de cryptographie est celui qui est le plus utilisé pour les clés asymétriques, spécialement pour les données envoyées sur Internet. Il permet à la fois le chiffrement et les signatures numériques (pour l'authentification). La sécurité de ces algorithmes est basée sur la difficulté (en temps processeur machine) de factoriser de grands nombres.

➢ « DSA » : Digital Signature Algorithm

Cet algorithme permet uniquement les signatures numériques. La sécurité de cet algorithme repose sur la difficulté de calculer les logarithmes discrets.

➢ Diffie-Hellman

C'est le premier algorithme à clés publiques qui a été inventé, il est seulement utilisable pour le chiffrement de données. La sécurité de cet algorithme repose sur le calcul de logarithmes discrets dans un domaine fini.

1.4.3 Quelle longueur de clé utiliser ?

Une clé est un nombre ou un couple de nombres. Le nombre de bits d'une clé correspond à sa taille. Plus la taille est importante, plus cette clé sera difficile à compromettre. Il faut distinguer deux cas, les algorithmes symétriques et asymétriques.

Algorithmes symétriques

Les clés symétriques de chiffrement sont confrontées à des « Key Search Attacks ». Les attaquants essayent toutes les clés possibles jusqu'à ce qu'ils trouvent la bonne clé pour décrypter le message. La plupart de ces attaques réussissent avant que toutes les possibilités aient été essayées.

Le seul moyen d'éviter ces attaques, c'est de limiter la durée de validité des clés et d'en augmenter la taille. L'augmentation de la longueur de la clé d'un bit double l'effort nécessaire pour réussir une attaque. Cependant, le temps requis pour lancer une attaque avec un résultat positif a beaucoup diminué suite à l'augmentation continue de la puissance des ordinateurs. De plus, le prix de ce matériel est en constante diminution.

Les clés symétriques d'au moins 64 bits de longueur apportent une protection importante contre ces attaques, mais les clés de plus de 128 bits sont considérées aujourd'hui comme incassables. Ce ne sera sans doute pas longtemps le cas, vu l'évolution rapide du matériel informatique.

Algorithmes asymétriques

Pour une longueur de clé donnée, les clés publiques sont plus susceptibles d'être attaquées que les clés secrètes, principalement par des « Factoring Attacks ». Les attaquants essayent toutes les combinaisons de nombres qui pourraient être utilisées par l'algorithme pour décrypter. Les « Factoring Attacks » sont similaires aux « Key Search Attacks » mais le nombre de facteurs possibles varie selon l'algorithme utilisé et la longueur de la clé privée et publique.

Les « Factoring Attacks » sur les clés publiques demandent moins d'essais que les « Key Search Attacks » pour les clés secrètes. C'est pourquoi les clés symétriques de 128 bits sont considérées comme incassables et que les clés asymétriques de la même longueur ne le sont pas. Les clés asymétriques doivent au moins avoir une longueur supérieure à 512 bits pour protéger efficacement les informations.

Durée de validité des clés

La longueur n'est qu'un des facteurs de la force d'une clé, qu'elle soit symétrique ou asymétrique. Plus la clé est longue, mieux elle pourra résister aux attaques. De même, plus la durée de validité de la clé est courte, moins les attaquants posséderont de temps pour exploiter les faiblesses de l'algorithme de cryptographie.

Pour des informations qui ont beaucoup de valeur, la durée de validité de la clé doit être la plus courte possible. Une durée très courte minimise le nombre d'échantillons de données chiffrées pouvant être analysés et limite également les dommages causés dans le cas où une clé serait compromise après une attaque réussie.

1.5 Fonctions de hashing

Définition 1.3 : « Une fonction de hashing est une des primitives dans la cryptographie moderne. C'est une fonction de calcul efficace qui fait correspondre à une chaîne de caractères binaires de longueur variable, une chaîne de caractères binaires de longueur fixe, appelée condensé [5] ».[6]

Définition 1.4 : Un condensé est une conversion d'un morceau de donnée de longueur quelconque en un nombre non-réversible de longueur fixe par l'application d'une fonction mathématique à sens unique appelée fonction de hashing.

[5] Traduction du mot anglais « hash value »

[6] Source bibliographique : *[HAC96]*, Chapitre 1 p. 33

La longueur du condensé résultant doit être assez importante pour qu'il soit pratiquement impossible de trouver deux morceaux de données avec un même condensé. Un condensé possède les deux caractéristiques suivantes :

- La valeur de ce condensé est unique pour la donnée traitée par l'algorithme. Tout changement dans la donnée, que ce soit l'effacement ou la modification d'un élément, provoquera une valeur de condensé différente de celle de départ.
- Le contenu de la donnée traitée par l'algorithme ne peut en aucun cas être déduite à partir de ce condensé. C'est pour cela que les algorithmes sont dits **à sens unique**.

L'expéditeur génère un condensé du message qu'il veut envoyer, le chiffre et l'envoie avec le message de départ. Le destinataire déchiffre le condensé, génère également un condensé à partir du même message et compare les deux condensés. S'ils sont égaux, il y a énormément de chances pour que le message reçu soit intact.

Il existe également plusieurs algorithmes de hashing :

- « SHA » : Secure Hash Algorithm

Cet algorithme prend des messages de moins de 2^{64} bits de longueur et génère un condensé de 160 bits. C'est l'algorithme de hashing à sens unique le plus populaire pour créer des signatures numériques.

- « MD5 » : Message Digest Algorithm

Cet algorithme sert principalement pour les signatures numériques de messages de longueur assez importante. Il prend un message de longueur quelconque et génère un condensé (aussi appelé « Message Digest ») de 128 bits. Cet algorithme a été dévalorisé depuis que certaines parties en ont été compromises.

1.6 Signatures numériques : Algorithmes de hashing & cryptographie à clé publique

Tout comme les signatures manuscrites servent à identifier les personnes dans des procédures légales ou dans des transactions, les signatures numériques sont utilisées pour identifier les entités électroniques pour des transactions on-line. Une signature numérique identifie de manière unique l'expéditeur de la donnée signée et assure également l'intégrité de celle-ci contre toutes modifications.

Pour créer une signature numérique, on peut utiliser un algorithme de hashing avec la cryptographie à clé publique. Cette signature numérique permet au destinataire de vérifier l'intégrité des données ainsi que la preuve de la possession de la clé privée.

Un des protocoles de communication utilisant la signature numérique est le suivant :

- ✓ Un condensé est généré à partir du message original.
- ✓ Avec sa clé privée, l'expéditeur chiffre ce condensé en signature numérique.
- ✓ L'expéditeur envoie le message avec la signature numérique.
- ✓ Le destinataire applique un algorithme de hashing sur le message qu'il vient de recevoir.
- ✓ Le destinataire se procure le certificat de l'expéditeur.
- ✓ Il utilise la clé publique trouvée dans le certificat avec la signature numérique et retrouve le condensé de départ. Il peut alors comparer ce condensé avec celui qu'il vient de générer pour vérifier la signature.

→ Si les deux condensés correspondent, le message n'a pas été modifié depuis qu'il a été signé. Le destinataire est alors certain que la clé publique utilisée pour déchiffrer correspond bien à la clé privée utilisée pour faire la signature numérique. Cela confirme l'identité de la personne qui a signé.

→ Dans le cas contraire, le message a été altéré depuis la signature, ou bien la clé privée utilisée pour chiffrer le condensé ne correspond pas à la clé publique donnée par l'expéditeur.

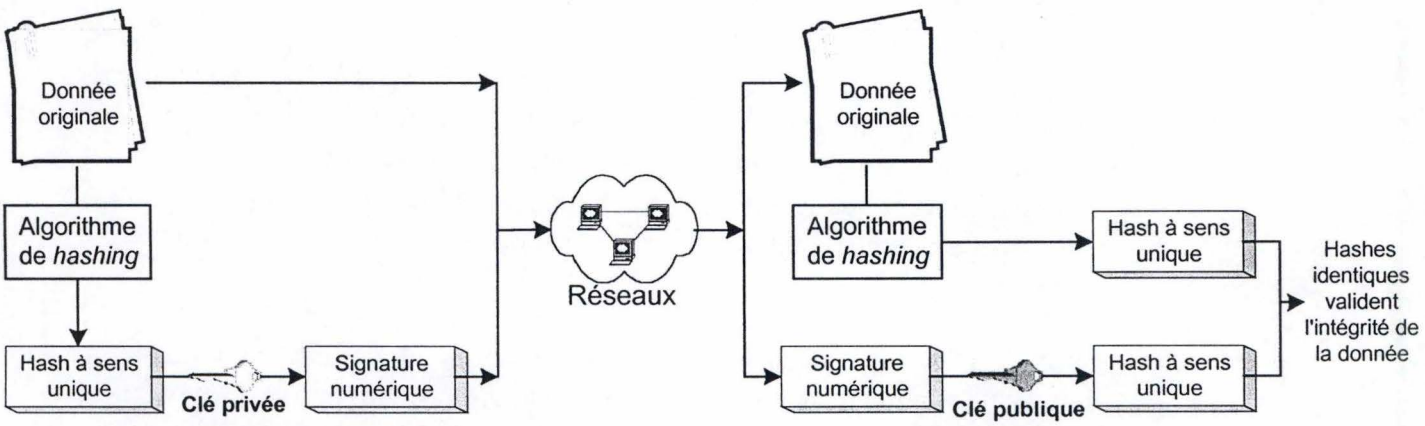

Figure 3 : Utilisation d'une signature numérique pour valider l'intégrité d'une donnée

Chapitre 2 : PKI « Public Key Infrastructure »

Ce chapitre définira les différents concepts associés aux infrastructures à clés publiques, parmi lesquels on retrouve l'authentification, la certification, les différents composants de l'infrastructure ainsi que les applications qui tirent parti de cette technologie . Les sources bibliographiques utilisées sont : *[BtInt00], [CertPCN], [iPlan00], [MsCry&Pki], [MsPkiInt], [MsRkit00b], [MsSDG00]* et *[RSA00]*.

2.1 Qu'est-ce qu'une infrastructure à clés publiques ?

La cryptographie à clé publique n'est pas suffisante pour établir la même confiance dans le monde électronique que dans le monde réel. Il faut également d'autres éléments pour permettre le commerce électronique (e-business) :

- des politiques de sécurité qui définissent les règles de fonctionnement des systèmes cryptographiques,
- des produits destinés à la génération, au stockage et à la gestion des clés,
- des procédures spécifiant comment les clés et les certificats doivent être générés, distribués et utilisés.

Une infrastructure à clés publiques (PKI) fournit un ensemble de services, technologies, protocoles et standards pour permettre de déployer et gérer un système de sécurité des informations performant basé sur la technologie à clés publiques. Les composants de base de cette infrastructure sont les certificats électroniques, les autorités de certification (CA) et les listes de révocation (CRL). Avant que la technologie de cryptographie à clé publique ne puisse être utilisée à grande échelle et facilement gérable sur les réseaux publics, une infrastructure à clés publiques doit être en place.

La cryptographie à clé publique utilise les clés publiques et privées pour permettre l'authentification, la confidentialité, l'intégrité et la non-répudiation. Pourtant, les clés en elles-mêmes ne fournissent pas la preuve que la paire de clés appartient bien au prétendu propriétaire. Il doit y avoir un moyen de vérifier l'identité du propriétaire de la paire de clés avec un haut niveau de confiance, ainsi qu'un moyen d'établir la confiance dans des paires de clés d'entités géographiquement éloignées sur des réseaux internes ou externes comme Internet.

Pour que la confiance soit établie entre deux parties qui communiquent, ces parties doivent avoir l'assurance de l'identité de l'autre et la preuve que la clé publique appartient bien à l'autre partie. Si elles peuvent s'échanger les clés publiques personnellement, il est possible de vérifier les signatures numériques avec un niveau de confiance très élevé. Ce type de confiance n'est possible que pour des groupes restreints qui décident de faire confiance aux clés publiques. Ce n'est évidemment pas envisageable sur des réseaux publics tels qu'Internet ou pour de grandes entreprises dispersées géographiquement.

Afin qu'une confiance s'établisse en des paires de clés sur des réseaux ouverts, des autorités de confiance doivent exister pour certifier l'identité des individus, organisations et ordinateurs sur le réseau et également pour assurer que les clés privées et publiques

correspondent bien à ces entités. Ces autorités de confiance, appelées autorités de certification, apportent un haut niveau d'assurance de l'identité des entités sur le réseau.

Afin d'établir la confiance sur Internet ou sur d'autres réseaux, l'infrastructure à clés publiques utilise des certificats électroniques qui sont émis par les autorités de certification. Un certificat électronique fournit la preuve que l'entité nommée dans le certificat est bien détentrice de la paire de clés publique et privée. De cette manière, les autres entités sur le réseau peuvent avoir la confirmation qu'une clé publique appartient bien au propriétaire d'une clé privée.

L'infrastructure à clés publiques définit l'ensemble des éléments nécessaires à une autorité de certification pour émettre des certificats électroniques et pour permettre leur administration (c'est-à-dire la révocation des certificats, leur renouvellement, leur suspension...). Cette infrastructure peut être définie comme une couche intermédiaire entre une infrastructure de communication (reposant sur de technologies IP) et des applications comme un programme de messagerie.

Deux opérations de base sont communes à toutes les infrastructures à clés publiques :

- **La certification** : processus qui consiste à lier un individu à une paire de clés.
- **La validation** : processus qui consiste à vérifier cette certification.

2.1.1 La certification

La certification est une fonction fondamentale des infrastructures à clés publiques. Elle définit les moyens par lesquels les informations concernant les clés publiques sont publiées, c'est-à-dire les certificats électroniques.

Certificat électronique

Définition 2.1 : Un certificat pour clés publiques est une déclaration signée numériquement qui lie une valeur d'une clé publique à l'identité du sujet (personne, service, etc.) qui détient la clé privée correspondante.

En signant le certificat, l'autorité de certification confirme que la clé privée associée à la clé publique se trouvant dans le certificat est bien en possession de la personne citée dans ce certificat.

Un certificat pour clés publiques est utilisé pour l'authentification et les échanges sécurisés d'informations sur Internet et sur des réseaux internes ou externes au moyen des signatures numériques et du chiffrement. L'émetteur et le signataire du certificat sont l'autorité de certification (communément appelée « Certification Authority » (CA)). L'entité pour qui le certificat a été émis s'appelle le sujet du certificat.

Les certificats électroniques sont des informations publiques disponibles pour tout le monde. Ils peuvent être distribués via des répertoires, des e-mails ou des pages Web. De cette manière, la clé publique du propriétaire du certificat est également distribuée. Les autres personnes vont faire confiance au propriétaire de la clé privée en se basant sur la réputation de

l'autorité de certification, ainsi qu'aux procédés de publication de certificats de cette même autorité.

Dans un certificat, on retrouve un ensemble d'informations qui comprend les éléments suivants :

- **Des informations sur le détenteur du certificat** : le « distinguished name ». C'est une série de valeurs qui identifie de manière unique le propriétaire du certificat. On y retrouve principalement un nom, un prénom, une adresse e-mail, une organisation, un pays et éventuellement un numéro d'identification.
- **La clé publique** associée au certificat ainsi que l'algorithme utilisé pour générer la paire de clés.
- **Le nom qui identifie l'autorité de certification** qui a émis le certificat.
- **La signature numérique de l'autorité de certification** qui a émis le certificat. Elle résulte d'un condensé de tout le contenu du certificat chiffré avec la clé privée de cette autorité. On retrouve également l'algorithme utilisé pour générer cette signature.
- **Le type d'usage de ce certificat**. Il peut par exemple servir à chiffrer des e-mail, à se connecter avec une carte à puce (Smart Card).
- **La version du standard X.509** supportée par ce certificat.
- **Le numéro de série du certificat** : Tout certificat émis par une autorité de certification a un numéro unique. Un historique de tous les certificats émis et révoqués peut être géré facilement.
- **La période de validité du certificat (date de début et fin)** : La date de fin de cette période ne peut être postérieure à la date de fin de validité du certificat de l'autorité de certification qui a émis le certificat.
  Cette période dépend de plusieurs facteurs importants :
  - la longueur des clés,
  - la sécurité associée à la protection de la clé privée de l'autorité,
  - la sécurité associée aux certificats émis et à leur clé privée,
  - les risques d'attaques.
- **La localisation de la liste de révocation** (CRL : Certificate Revocation List) : La liste de révocation est un document qui reprend l'ensemble des certificats qui ont été révoqués. L'autorité de certification signe ce document avec sa clé privée pour en assurer l'intégrité.

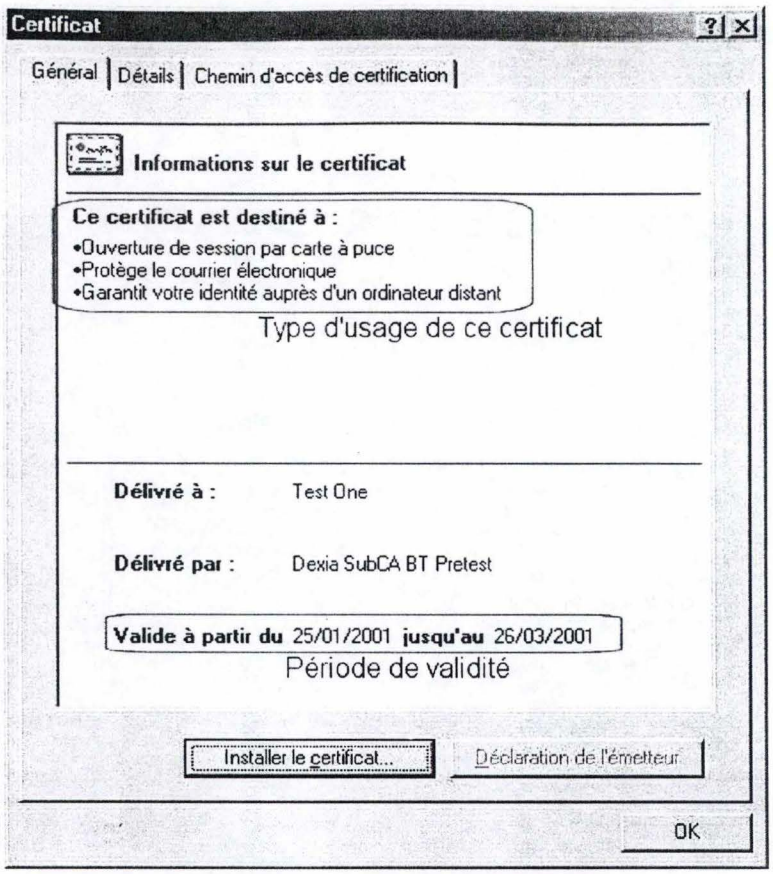

Figure 4a : Exemple de certificat

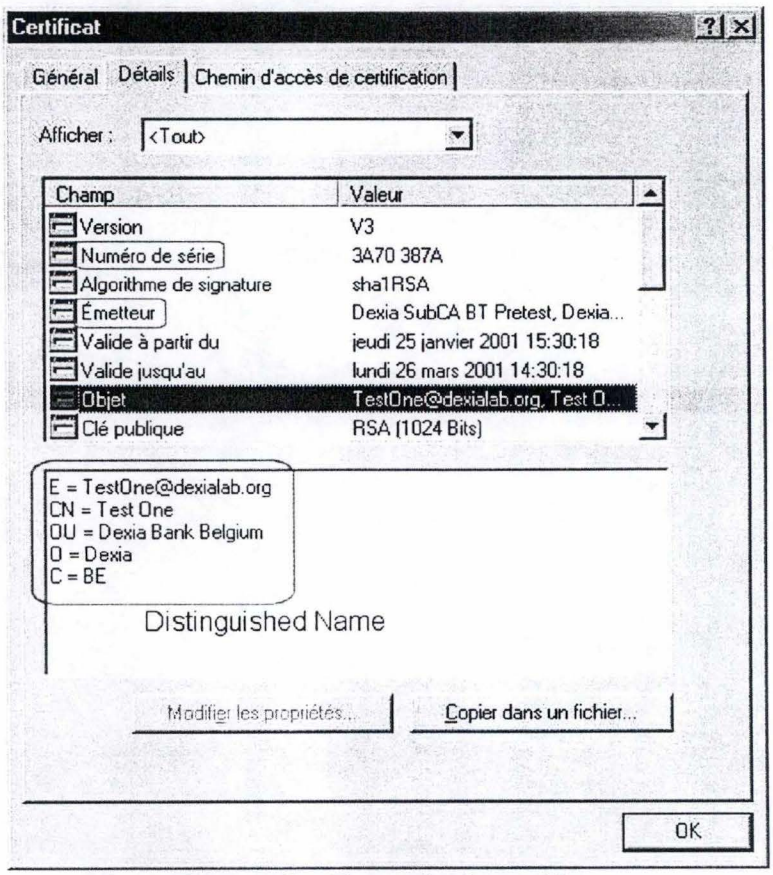

Figure 4b : Exemple de certificat

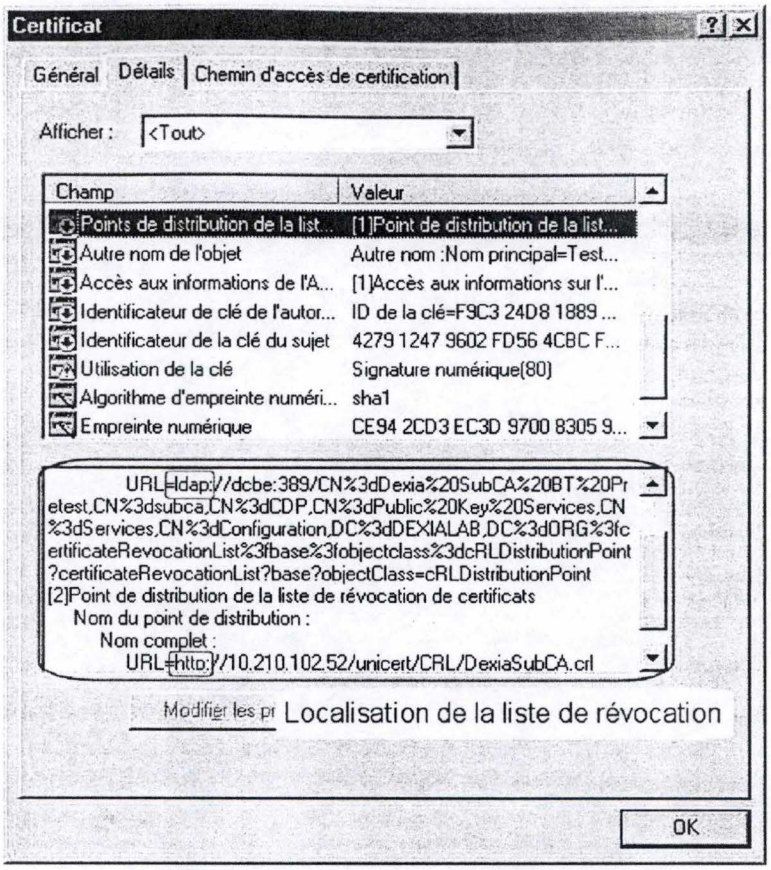

Figure 4c : Exemple de certificat

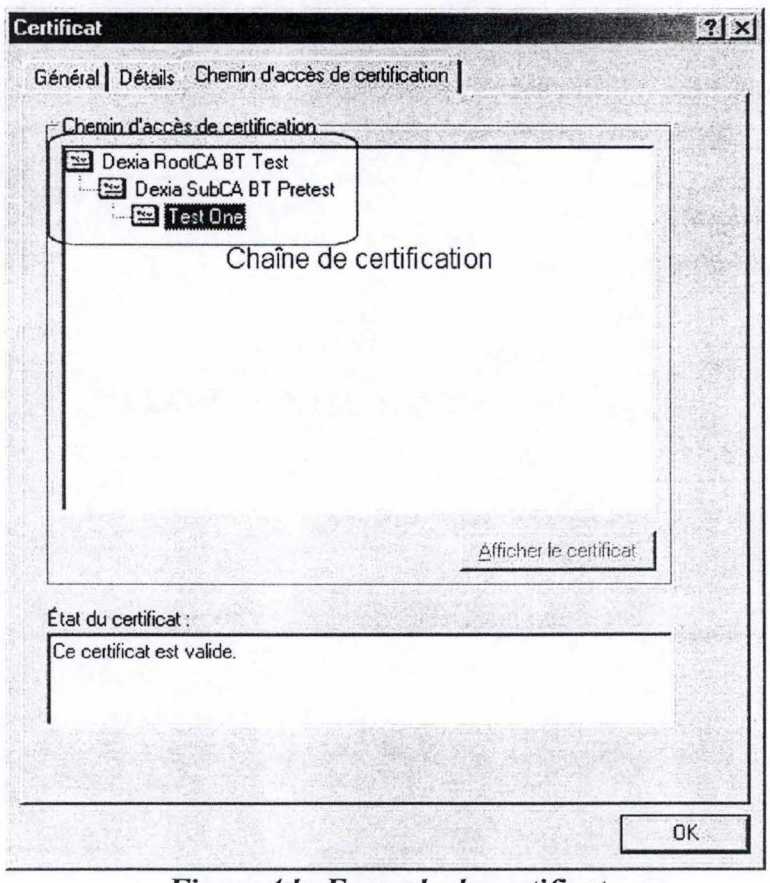

Figure 4d : Exemple de certificat

2.1.2 La validation d'un certificat

La validation est l'autre fonction fondamentale d'une infrastructure à clés publiques. L'information contenue dans les certificats peut changer tout le temps. C'est pourquoi la personne qui utilise un certificat doit être sûre que ce certificat est conforme. On dit qu'elle valide le certificat. Pour cela, il existe deux méthodes :

- **Validation on-line** : L'utilisateur peut demander directement à l'autorité de certification de vérifier la validité d'un certificat chaque fois qu'il est utilisé.
- **Validation off-line** : Le certificat contient une paire de dates qui définit l'intervalle de temps pendant lequel l'information contenue dans le certificat peut être considérée comme valide.

Validation de chaînes de certification

La validation d'une chaîne de certification est un processus servant à confirmer qu'un certificat est valide, correctement signé et donc fiable. La marche à suivre est la suivante :

1. La période de validité du certificat est vérifiée.
2. Le certificat de l'émetteur est localisé. Il peut se trouver dans une base de données de certificats ou bien via la chaîne de certification fournie par le sujet (indiquée dans son certificat).
3. La signature du certificat est vérifiée par l'utilisation de la clé publique figurant dans le certificat de l'émetteur.
4. Si le certificat de l'émetteur se trouve dans la base de données du vérificateur contenant tous les certificats dans lesquels il a confiance, alors la validation s'arrête ici avec succès. Sinon, si le certificat de l'émetteur contient des indications suffisantes pour prouver que c'est une autorité, la validation de la chaîne retourne au point 1 et recommence.

Exemple 1 : Seul le certificat de l'autorité racine (Root CA) se trouve dans la base de données du vérificateur. Il faut alors remonter toute la chaîne.

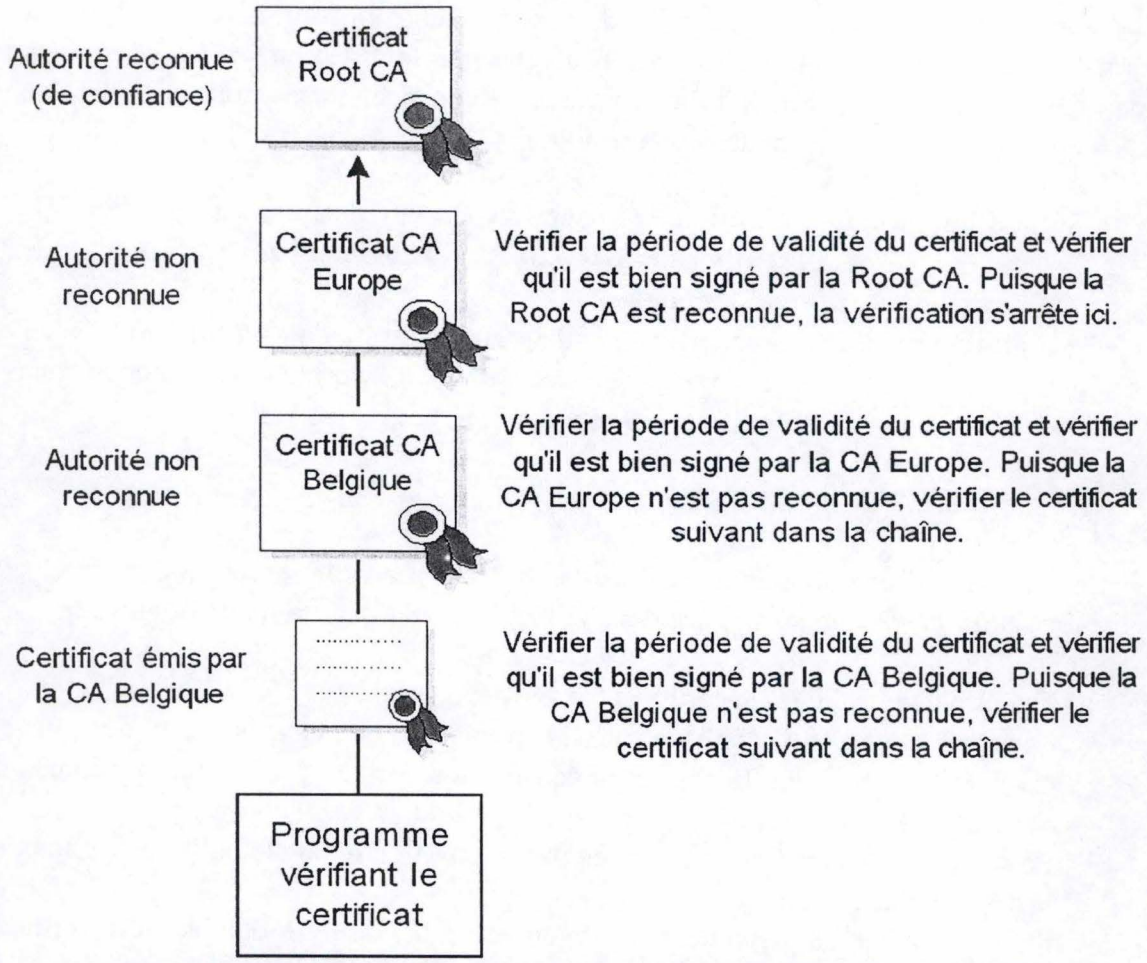

Figure 5 : Vérification d'une chaîne de certification jusqu'à la Root CA

Exemple 2 : Un certificat d'une autorité intermédiaire se trouve dans cette base de données. La validation peut s'arrêter ici avec succès.

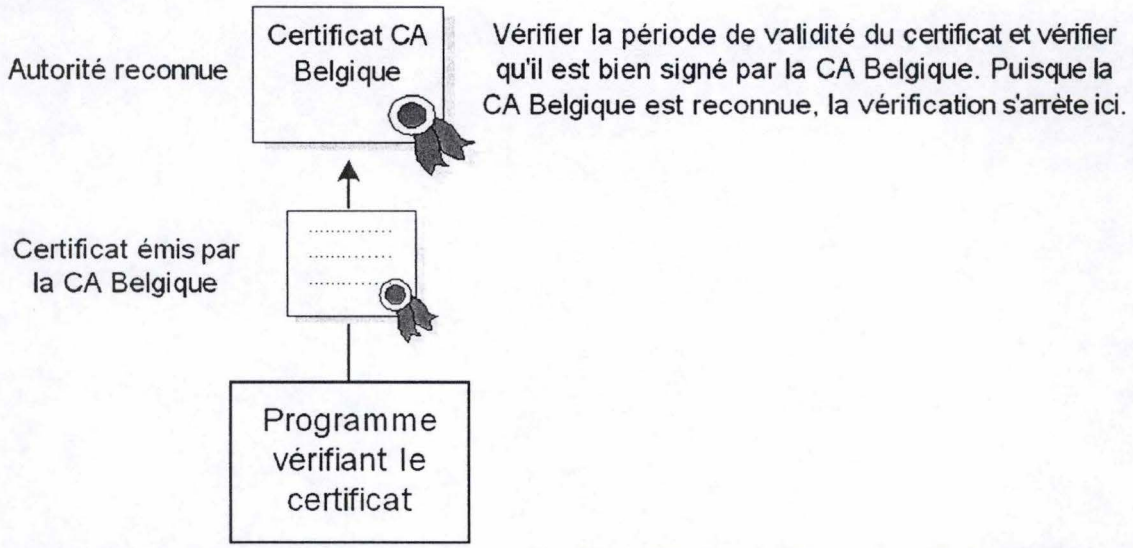

Figure 6 : Vérification d'une chaîne de certification jusqu'à une CA intermédiaire

Exemple 3 : Si le vérificateur trouve une date de validité dépassée, une signature invalide ou s'il ne trouve pas de certificat pour l'autorité émettrice à n'importe quel point de la chaîne de certification, c'est un échec. Le même résultat est obtenu si ni les autorités intermédiaires, ni l'autorité racine ne sont reconnues dans la base de données du vérificateur.

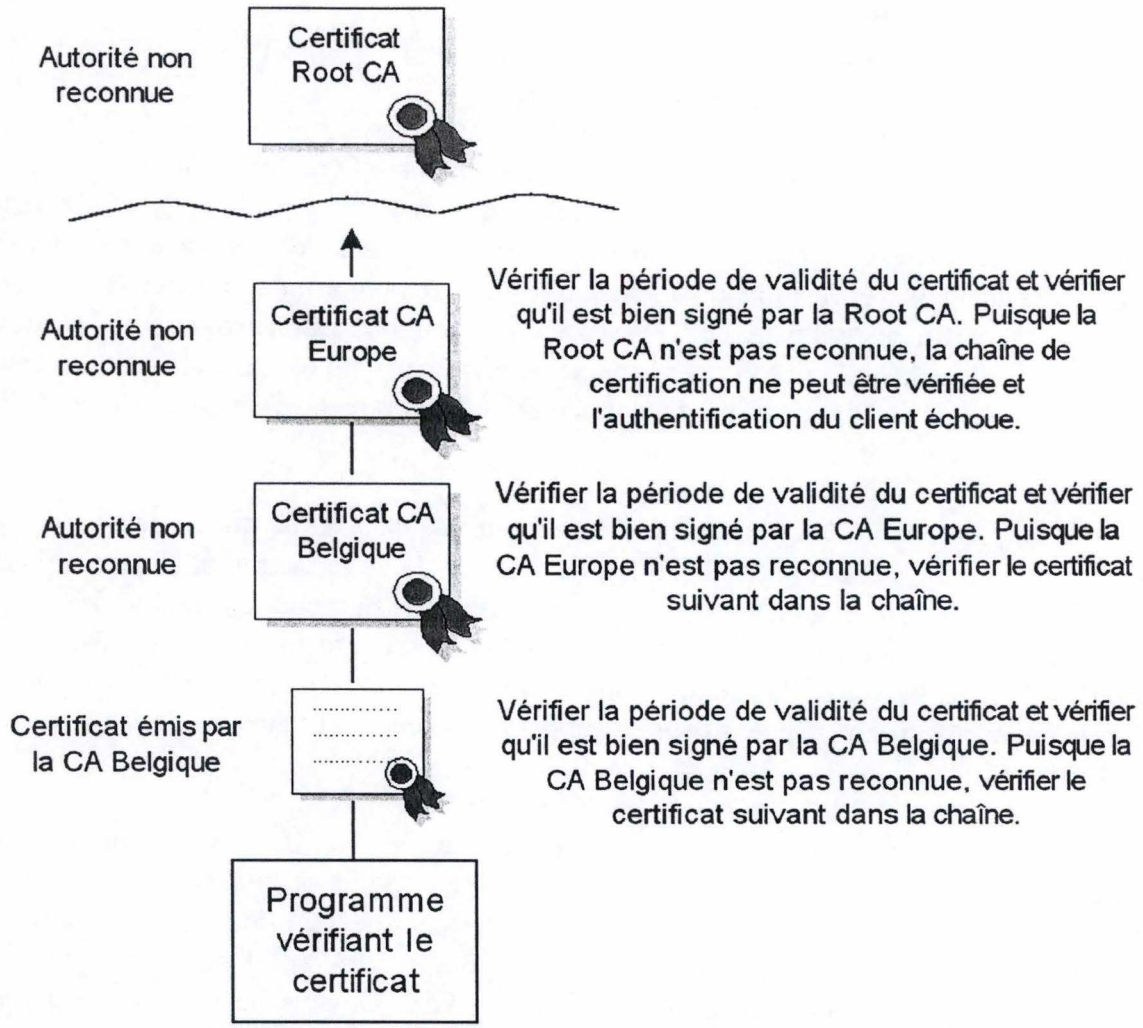

Figure 7 : Une chaîne de certification qui ne peut pas être vérifiée

Révocation d'un certificat

Les certificats émis ont une durée de vie limitée mais les autorités de certification peuvent réduire cette durée par le processus de révocation de certificats. L'autorité publie une liste des numéros de série des certificats qui ne peuvent plus être considérés comme valides, c'est la CRL : « Certificate Revocation List ». La durée de validité de cette CRL est plus courte que la durée de vie des certificats. L'autorité peut également spécifier dans cette liste la raison pour laquelle le certificat a été révoqué ainsi que la date à partir de laquelle le changement de statut du certificat doit être pris en compte. Un certificat peut être révoqué pour les raisons suivantes :

- La clé privée associée à la clé publique contenue dans le certificat est compromise, c'est-à-dire qu'une tierce personne a pris connaissance de cette clé et pourra à l'avenir se faire passer pour le sujet du certificat.

- La clé privée de l'autorité de certification a été compromise, ce qui implique que tous les certificats émis par celle-ci ne sont plus valides et doivent donc être également révoqués.
- Une des informations concernant le sujet du certificat a changé. Par exemple, le sujet peut avoir changé de division au sein d'une organisation. Son certificat peut à ce moment ne plus lui être utile.
- Le sujet du certificat n'est plus employé par l'organisation. Il faut donc éviter qu'il fasse encore usage de ce certificat par après.

La révocation d'un certificat signifie que l'autorité de certification annule son autorisation d'utiliser la paire de clés avant l'expiration normale du certificat. Quand la période de validité du certificat est dépassée, l'entrée dans la CRL est enlevée pour réduire la taille de cette CRL. Pendant la vérification d'une signature, le programme peut vérifier la CRL pour déterminer si le certificat et la paire de clés associée sont toujours valides. Si ce n'est pas le cas, le programme peut trouver la raison pour laquelle ce certificat a été révoqué ainsi que la date de révocation. Si la date de la signature est antérieure à la date de révocation du certificat, celle-ci peut être toujours considérée comme valide.

Un des problèmes liés aux listes de révocation réside dans le fait qu'il existe un décalage dans les versions des listes utilisées. En effet, dans le cas de la validation off-line, l'ordinateur qui effectue cette validation utilise une liste qui se trouve dans sa cache. La version de cette liste peut différer de la version réelle, car une mise à jour n'est effectuée que quand la version présente sur la machine n'est plus valide. La révocation des certificats, pendant la validité de la version se trouvant sur la machine, ne sera donc prise en compte qu'après une mise à jour de la liste de révocation.

Un autre problème lié à la CRL concerne la taille de cette liste lorsqu'une autorité de certification certifie énormément de sujets. Comme le taux de révocation pour une population donnée n'est pas prévisible, la CRL d'une telle autorité peut devenir énorme et quand la taille devient trop importante, la CRL est difficile à prendre et des problèmes liés à une bande passante limitée pour accéder à l'autorité peuvent se produire. De plus, les CRL sont signées par l'autorité de certification, ce qui augmente le temps nécessaire à leur vérification avant leur utilisation. Afin de remédier à ce problème de taille, on peut envisager plusieurs approches :

- **Différentes CRL selon la raison de la révocation** : Ces raisons ont des importances très variables. Il peut y avoir une CRL pour les causes de révocations mineures, comme un changement d'information à l'intérieur du certificat, et une autre pour les causes majeures pouvant entraîner des problèmes de sécurité. Cette dernière est beaucoup plus importante et devra avoir une durée de validité plus courte pour que les programmes aient de fréquentes mises à jour.
- **Différentes CRL selon le sujet du certificat** : Il peut y avoir une CRL pour les autorités de certification qui ont été révoquées et une autre pour les utilisateurs normaux. La première est plus importante et devra également faire l'objet d'une publication plus fréquente.
- **Utilisation des « *Delta-CRLs* »** : Il s'agit de listes signées par l'autorité de certification qui reprennent seulement tous les changements apportés à la CRL depuis sa précédente émission complète. Elles permettent des publications plus fréquentes et réduisent la possibilité qu'un certificat révoqué puisse encore être utilisé. Un système

de révocation pourrait commencer par émettre une CRL complète et ensuite utiliser ces « Delta-CRLs » pour la mettre à jour.

2.1.3 L'authentification

L'authentification est le processus qui confirme une identité. Quand une autorité certifie un sujet et qu'un utilisateur valide cette certification, on dit que le sujet a été authentifié. Le degré de confiance que l'utilisateur accorde aux informations du certificat et à sa validité est une mesure de la force de l'authentification.

Dans le contexte d'interactions à l'intérieur d'un réseau, l'authentification implique une identification mutuelle des deux parties concernées. Ces interactions se déroulent généralement entre un client et un serveur. Cette authentification peut prendre différentes formes :

- **Client Authentication** : Identification du client par le serveur.
- **Server Authentication** : Identification du serveur par le client.
- **Signatures numériques pour un message électronique.**

L'identification du client par le serveur est un élément essentiel pour la sécurité dans des réseaux internes ou externes. Il en existe deux types : l'authentification avec mot de passe et avec certificat.

Authentification avec mot de passe

Un serveur peut exiger un nom d'utilisateur et un mot de passe pour accorder l'accès. Pour cela, le serveur garde une liste de noms et de mots de passe. Si un nom particulier se trouve dans cette liste et que l'utilisateur entre le mot de passe correspondant, l'accès lui sera accordé.

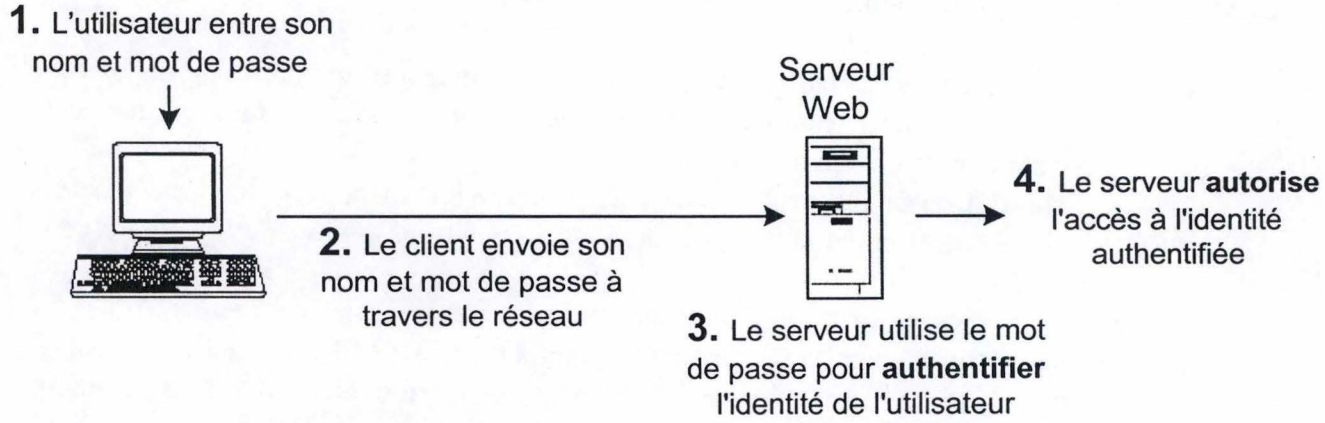

Figure 8 : Utilisation d'un mot de passe pour l'authentification d'un client sur un serveur

Si l'utilisateur a décidé d'avoir confiance dans le serveur à qui il a demandé une ressource, l'authentification se passe comme suit :

1. En réponse à la demande d'authentification du serveur, le client est invité à entrer un nom d'utilisateur et un mot de passe. Cet utilisateur devra faire de même pour tous les autres serveurs dont il aura besoin pendant sa session de travail.

2. Le client envoie son nom et mot de passe sur le réseau en clair ou bien via une connexion sécurisée (SSL).
3. Le serveur regarde dans sa liste s'il y a une correspondance avec ce qu'il vient de recevoir. Si c'est le cas, l'identité du client est confirmée.
4. Le serveur détermine si le client qui vient d'être identifié a bien la permission d'accéder à la ressource demandée et lui donne accès si c'est le cas.

Authentification avec certificat

Afin de s'authentifier auprès d'un serveur, le client signe numériquement des données générées aléatoirement et envoie son certificat ainsi que les données signées à travers le réseau.

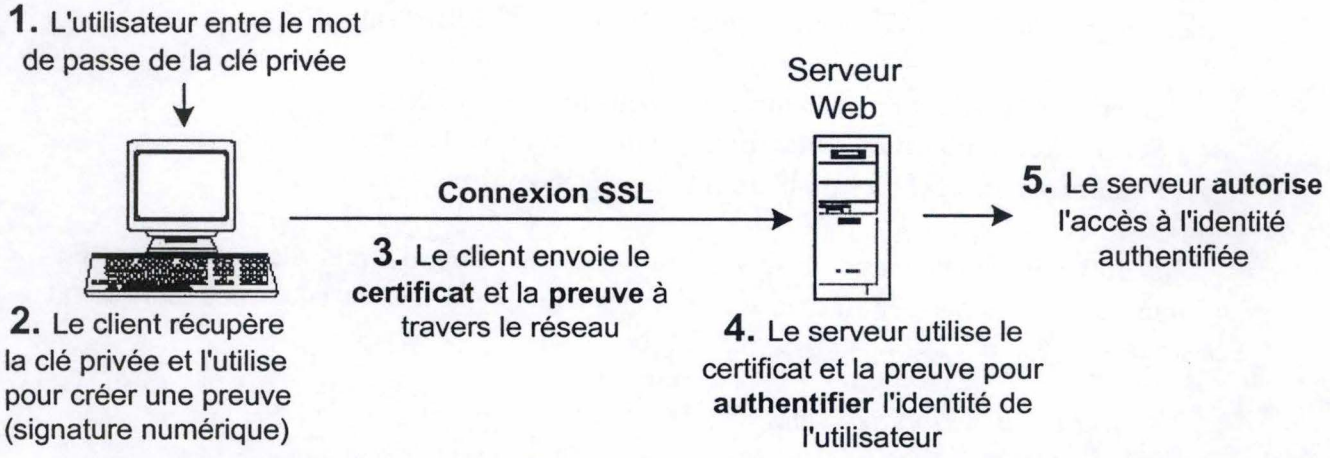

Figure 9 : Utilisation d'un certificat pour l'authentification d'un client sur un serveur

Comme pour l'authentification avec mot de passe, l'utilisateur doit avoir confiance dans le serveur auquel il s'adresse. De plus, son certificat doit bien entendu être valide. L'authentification se passe comme suit :

1. Le client accède à sa clé privée stockée sur sa machine ou bien sur un module hardware en entrant un mot de passe ou code PIN. Il ne devra le faire qu'une seule fois par session de travail.
2. Le client utilise sa clé privée pour signer numériquement des données générées aléatoirement. Les données et la signature constituent une preuve de la validité de la clé privée.
3. Le client envoie son certificat d'utilisateur et cette preuve à travers le réseau.
4. Le serveur utilise le certificat et la preuve pour authentifier l'identité de l'utilisateur.
5. Le serveur vérifie que l'utilisateur a bien la permission d'accéder à la ressource demandée et lui donne accès si c'est le cas.

Cette méthode d'authentification est préférable à la première. Au lieu de devoir **envoyer un mot de passe à travers le réseau** chaque fois qu'il doit s'authentifier auprès d'un serveur, l'utilisateur doit entrer une seule fois un mot de passe pour accéder à sa clé privée sur sa machine **sans l'envoyer sur le réseau**. Après, il lui suffit de présenter son certificat d'utilisateur pour s'authentifier auprès de chaque nouveau serveur qui le demande.

2.1.4 Gestion des certificats

Une infrastructure à clés publiques fournit les composants nécessaires pour gérer les certificats et les clés privées pendant la durée de validité d'un certificat. Le cycle de vie d'un certificat comporte les éléments suivants :

- Emission du certificat
- Révocation du certificat
- Renouvellement du certificat
- Expiration du certificat

Afin de gérer ce cycle de vie, l'infrastructure à clés publiques doit apporter des méthodes pour supporter les différentes activités de gestion suivantes :

- Enregistrement des certificats pour les utilisateurs et les ordinateurs
- Distribution des certificats pour un usage public
- Publication des listes de révocation (CRL)
- Renouvellement des certificats
- Tenue à jour d'un journal d'audit pour les certificats

Enregistrement des certificats

Le processus d'enregistrement des certificats comporte deux phases : d'abord l'identification du sujet et ensuite sa certification.

Dans un premier temps, le sujet doit prouver son identité, soit en étant déjà enregistré dans un annuaire officiel connu de l'autorité, soit en remplissant des formulaires fournis par celle-ci afin de s'enregistrer.

La certification consiste à lier l'identité d'un sujet à une clé publique. La génération de cette clé publique peut s'effectuer de deux manières : soit le sujet a généré lui-même la paire de clés (publique et privée) et présente sa clé publique, soit c'est l'autorité qui s'en occupe avant de renvoyer la paire de clés au sujet. Lorsque l'autorité a la confirmation de l'identité du sujet et qu'elle est en possession de la clé publique, elle génère un certificat reprenant toutes les informations (l'identité du sujet et sa clé publique) et le signe numériquement avec sa clé privée.

Distribution des certificats

Quand un certificat est émis, il doit être renvoyé au demandeur mais aussi être publié aux endroits où les autres utilisateurs peuvent y avoir accès. Cette publication s'effectue généralement dans des répertoires (directorys) qui sont souvent de type LDAP[7]. Dans le cas où l'autorité aurait généré elle-même la paire de clés, la clé privée doit être également renvoyée au demandeur, mais via un moyen sécurisé afin de ne pas la compromettre.

[7] Lightweight Directory Access Protocol

Listes de révocation (CRL)

Comme cela a été vu auparavant, l'autorité de certification publie des listes de révocation (CRL) reprenant tous les certificats qui ne sont plus valides pour des raisons diverses. L'autorité de certification signe numériquement cette liste pour en assurer l'intégrité.

Renouvellement des certificats

Quand le certificat arrive à sa date d'expiration, il devient invalide et ne peut plus être utilisé. Ce certificat pourra être réémis (avec les mêmes clés) ou renouvelé (avec de nouvelles clés) et se verra attribuer de nouvelles dates de validité.

Journal d'audit

Chaque autorité de certification doit tenir à jour un journal d'activités. Il reprend les certificats émis, les demandes qui ont échoué, les certificats révoqués (et la date de révocation). Ce journal est indispensable pour la sécurité de l'autorité et de l'organisation. Les opérateurs de l'autorité doivent être capables de détecter toutes les mauvaises utilisations de l'autorité ainsi que la cause de l'échec d'une demande.

2.1.5 Gestion des clés

La gestion des clés est une fonction très importante de l'infrastructure à clés publiques. Les clés privées doivent être générées, fournies à leur propriétaire et stockées en toute sécurité.

Protection de la clé privée

Les clés privées doivent être possédées et utilisées uniquement par leur propriétaire. C'est pourquoi l'infrastructure à clés publiques doit stocker les clés privées dans un endroit inaccessible aux autres et aucune autre copie de la clé ne devrait exister.

Une clé privée peut être protégée de deux manières :

- **Protection du lieu de stockage** : La clé privée peut être stockée sur le disque dur de la machine ou bien sur une carte à puce (Smart Card). Cette deuxième solution est la meilleure car elle assure une protection physique de la clé et celle-ci ne pourra jamais être exportée en dehors de cette carte. La première nécessite une protection plus importante de l'ordinateur contre les accès non autorisés.
- **Protection par mot de passe** : La génération de la clé privée requiert un mot de passe. A chaque utilisation ultérieure de la clé privée, ce mot de passe sera demandé.

Les conditions pour qu'une tierce personne puisse accéder à cette clé sont les suivantes : elle doit avoir accès au lieu de stockage de la clé (disque dur ou carte à puce) et connaître le mot de passe.

Historique des clés

Comme les clés sont renouvelées à des intervalles réguliers, il est toujours nécessaire de pouvoir accéder à des données chiffrées avec la génération précédente de clés d'un utilisateur donné. L'infrastructure à clés publiques doit fournir un moyen de maintenir un historique complet par utilisateur et d'accéder à la bonne version de la clé chaque fois qu'une demande de déchiffrement ou de validation d'une signature numérique sera effectuée.

Sauvegarde et restauration des clés

La sauvegarde et la restauration des clés assurent qu'une copie des clés de déchiffrement est gardée au niveau de l'autorité pour chaque utilisateur et que ces clés peuvent être restaurées à tout moment quand le besoin s'en fait sentir (si l'utilisateur a oublié son mot de passe, par exemple).

Cependant, les clés de signature ne peuvent en aucun cas être sauvegardées pour assurer la non-répudiation. Sinon, un utilisateur pourrait prétendre ne pas être responsable d'une transaction au motif qu'une tierce personne peut éventuellement accéder à sa clé privée et se faire passer pour lui. La paire de clés de chiffrement peut être sauvegardée et restaurée tandis que la paire de clés nécessaire pour signer ne peut être en possession que de son propriétaire.

2.2 Composants d'une infrastructure à clés publiques

2.2.1 Autorité de certification (CA)

L'autorité de certification est le composant le plus important d'une infrastructure à clés publiques. Tous les liens de confiance à l'intérieur de cette infrastructure dépendent de la signature de l'autorité. Cette autorité fonctionne selon ses propres politiques et est contrôlée par ses opérateurs (CAO : Certification Authority Operator). Son rôle et son fonctionnement sont les mêmes indépendamment du fait qu'elle se trouve dans un réseau interne ou sur Internet. Elle offre différents services de base durant la durée de vie des certificats :

- Effectuer des demandes de certificats pour vérifier l'identité du demandeur et ensuite émettre un certificat suivant les politiques de l'autorité.
- Gérer l'administration des certificats (journaux d'audit) de leur enregistrement à leur expiration ou à leur révocation, ainsi que leur publication.
- Renouveler des certificats avant qu'ils expirent.
- Révoquer les certificats si nécessaire.
- Mettre à jour et publier la liste de révocation (CRL).

Différents types d'autorités de certification

Il existe 3 types d'autorités de certification :

- **Autorité de certification « self-signed »** : La clé publique figurant dans le certificat et celle utilisée pour vérifier le certificat sont identiques. Certaines autorités « self-signed » sont des autorités racines (Root CA).

- **Autorité de certification subordonnée** : La clé publique figurant dans le certificat et celle utilisée pour vérifier les certificats sont différentes.
- **Autorité de certification racine** : Une classe spéciale d'autorité de certification qui est reconnue sans réserve par un client et qui se trouve au sommet d'une hiérarchie de certification. Toutes les chaînes de certification se terminent par une autorité racine. Celle-ci signe elle-même son propre certificat parce qu'il n'y a pas de plus haute autorité de certification dans la hiérarchie.
  Toutes les autorités « self-signed » sont des autorités racines car les chaînes de certification se terminent quand on arrive à une autorité « self-signed ».

Hiérarchie d'autorités de certification (CA)

Comme cela a été vu plus haut, une autorité de certification est indispensable pour établir une infrastructure à clés publiques. Mais sur des réseaux de plus en plus vastes, il est impensable d'avoir une seule autorité pour tout le monde. C'est pourquoi une autorité peut également émettre un certificat pour une autre autorité de certification.

Dans une grande organisation, il est souvent approprié de déléguer la responsabilité d'émettre les certificats à plusieurs autorités, pour différentes raisons :

- Le nombre de certificats à émettre est trop important pour une seule autorité de certification.
- Les champs d'application des certificats peuvent être différents.
- L'organisation est divisée en plusieurs départements qui ont des politiques différentes pour les certificats.
- L'organisation est divisée géographiquement en plusieurs départements situés dans des régions éloignées.

Cette division en hiérarchie peut apporter des atouts administratifs non-négligeables :

- La sécurité liée à l'autorité peut être mieux adaptée : chaque autorité ne nécessite pas la même sécurité (longueur de clé, protection physique, protection contre les attaques via le réseau, etc.). Pour une autorité racine (Root CA), il est préférable d'utiliser des mesures spéciales vu que toute la confiance repose sur elle. Il est donc préférable de prévoir des modules matériels de sécurité (HSM) ainsi qu'une utilisation off-line. Les autorités qui vont émettre les certificats pour les utilisateurs ne peuvent évidemment pas fonctionner dans le même environnement.
- Il est possible de mettre à jour les clés ou certificats des autorités qui émettent des certificats, celles qui sont le plus exposées à être compromises, sans qu'il soit nécessaire de modifier les relations de confiance existantes.
- Il est possible d'arrêter une partie de la hiérarchie sans affecter les relations de confiance existantes. Une autorité d'une division d'une région différente peut être révoquée sans interférence avec les autres divisions.

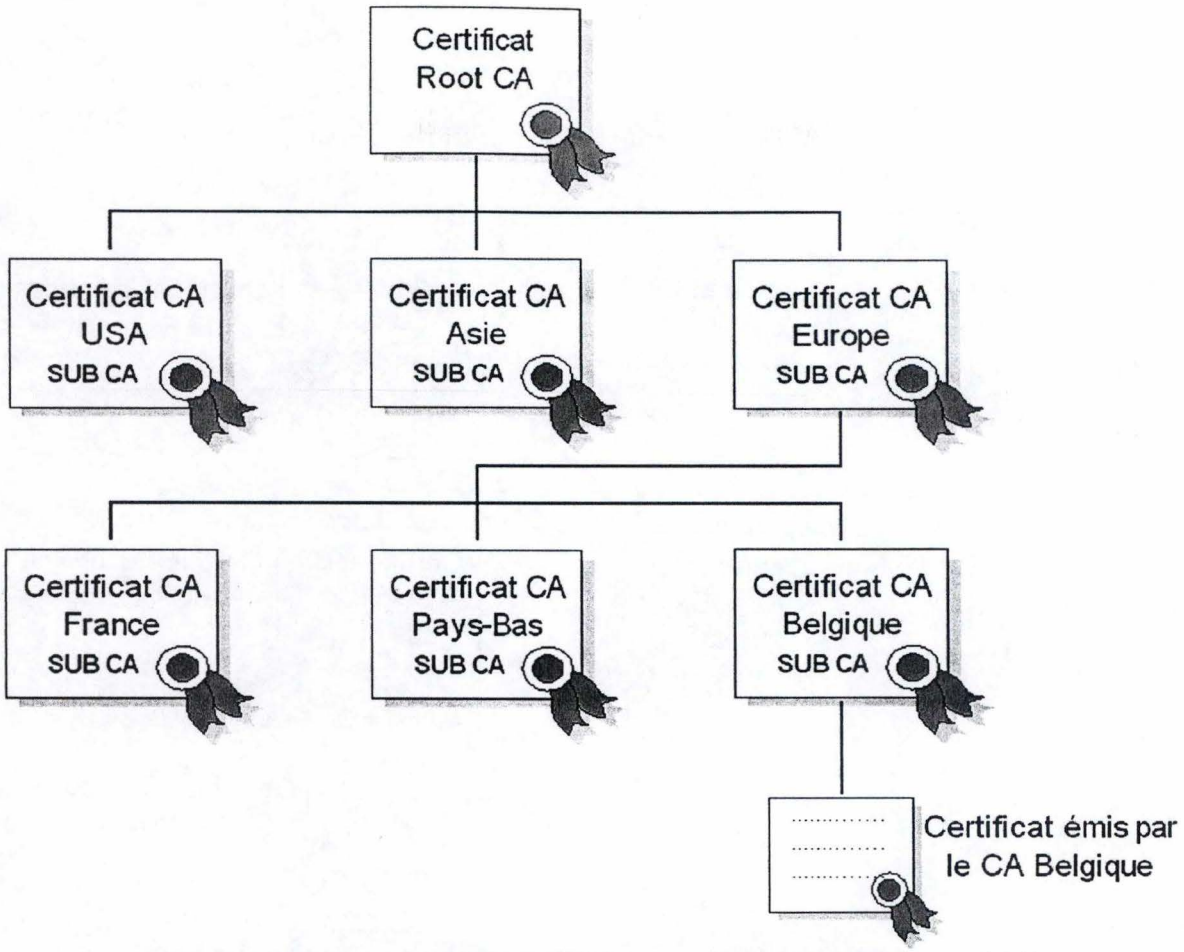

Figure 10 : Exemple de hiérarchie d'autorités de certification (CA)

Dans ce schéma, l'autorité de certification racine (Root CA) est au sommet de la hiérarchie. Son certificat est « self-signed », c'est-à-dire que ce certificat est signé par la même entité que celle que le certificat identifie. Les autorités de certification inférieures (Subordinate CAs) voient leur certificat signé par l'autorité racine. Les autres autorités situées plus bas dans la hiérarchie voient leur certificat signé par l'autorité du niveau juste au-dessus.

La hiérarchie d'autorités ressort dans les chaînes de certification. Une chaîne de certification est une série de certificats émis par plusieurs autorités successives. Dans le schéma qui suit, on peut voir la chaîne de certification pour un certificat donné.

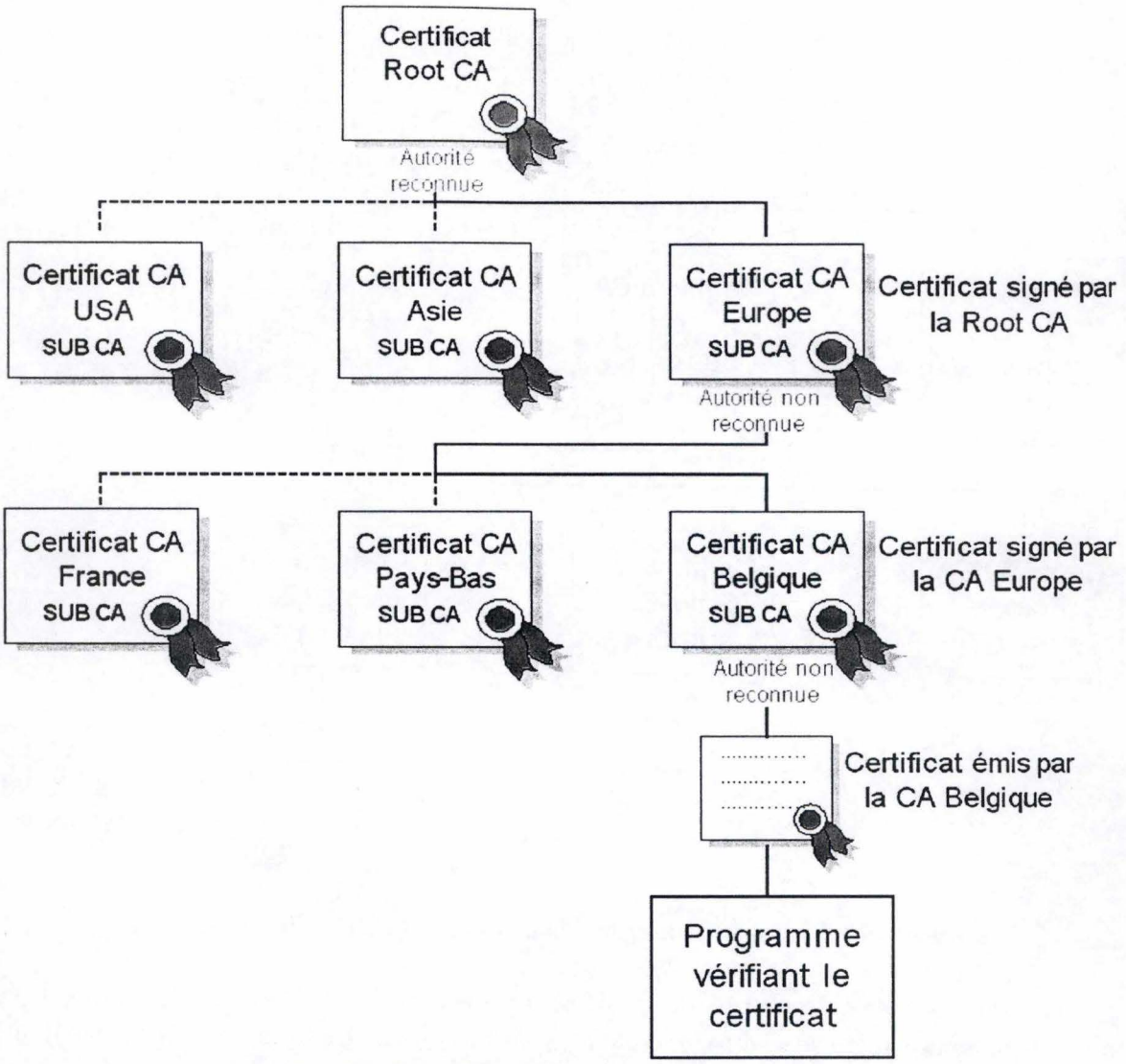

Figure 11 : Exemple d'une chaîne de certification

Sécurité des autorités de certification

Les autorités les plus vulnérables sont celles qui sont connectées directement à un réseau, qui ont une faible sécurité physique et qui signent un grand nombre de certificats. C'est pourquoi il faut trouver le juste milieu entre la sécurité et la disponibilité. La meilleure solution est une hiérarchie à trois niveaux qui comprend : une autorité de certification racine « off-line », une autorité de certification subordonnée « off-line » et une autre « on-line » pour émettre les certificats.

- **Autorité de certification racine « off-line »** : Cette autorité nécessite le niveau de sécurité le plus élevé. Elle doit se trouver dans un endroit protégé, rester déconnectée de tout réseau et signer seulement un très petit nombre de certificats. Il faudrait garder l'autorité et ses clés dans un coffre fort qui serait seulement accessible à deux opérateurs : un pour effectuer les actions obligatoires et un autre pour surveiller le déroulement de ces actions.
- **Autorité de certification intermédiaire « off-line »** : Cette autorité se situe juste en dessous de l'autorité racine. En la mettant « off-line », on accroît la sécurité.

- **Autorité de certification émettrice « on-line »** : la dernière autorité dans la chaîne doit être connectée à un réseau afin d'être accessible pour procéder à des demandes de certificats de la part d'un grand nombre de clients. Elle transmet des informations à jour concernant les certificats révoqués. Les opérateurs peuvent changer les clés de ce type d'autorité assez fréquemment vu que le coût de distribution des nouveaux certificats est très faible. Le gain que des pirates peuvent retirer d'une attaque est minime et ces autorités peuvent être rapidement et facilement bloquées au moyen de la révocation de leur certificat par une autorité supérieure.

2.2.2 Opérateurs d'une autorité de certification (CAO)

Ces opérateurs correspondent aux responsables de la sécurité dans l'infrastructure à clés publiques et s'occupent de toutes les tâches administratives. Il n'y a pas moyen de travailler directement avec l'autorité, il faut donc passer obligatoirement par ces opérateurs. Ceux-ci sont chargés :

- de définir les différents éléments de l'infrastructure à clés publiques et de générer les certificats pour ceux-ci,
- d'administrer tous les certificats,
- de communiquer les demandes d'émission et de révocation de certificats à l'autorité,
- de créer et d'assurer la maintenance des politiques pour l'émission des certificats,
- d'archiver toutes les données et tous les journaux d'audit dans la base de données de l'autorité. Toutes les informations archivées sont signées numériquement par celle-ci.

2.2.3 Autorité d'enregistrement (RA)

L'autorité d'enregistrement fait office d'interface entre l'utilisateur et l'autorité de certification. Elle saisit et authentifie l'identité des utilisateurs et soumet les demandes de certificats à l'autorité de certification. La qualité de ce processus d'authentification détermine le niveau de confiance qui peut être accordé aux certificats.

L'utilisation de ces autorités d'enregistrement apporte différents avantages :

- Les organisations peuvent mettre en place des centres d'enrôlement à des endroits éloignés géographiquement (compagnies internationales). Les certificats électroniques des employés sont émis par l'autorité de certification de la compagnie qui peut se trouver à l'autre bout du monde.
- L'utilisation d'une autorité d'enregistrement permet de séparer le processus de demande de certificats du processus d'émission de certificats.
- Les demandes de certificats sont envoyées à l'autorité d'enregistrement plutôt qu'à l'autorité de certification. Les opérateurs de l'autorité de certification sont soulagés de la lourde tâche de vérification des identités. Cette opération de vérification est souvent celle qui demande le plus de travail dans une infrastructure à clés publiques, spécialement si les politiques exigent un examen en profondeur de chaque demande de certificat.

2.2.4 Opérateurs d'une autorité d'enregistrement (RAO)

La fonction première de ces opérateurs est d'approuver les demandes de certificats qui seront émis par l'autorité de certification. Chaque opérateur a le droit d'émettre des certificats qui respectent les politiques formulées par l'opérateur de l'autorité de certification.

2.2.5 Politiques de sécurité d'une infrastructure à clés publiques[8]

Les politiques de sécurité définissent les contraintes dans lesquelles l'infrastructure à clés publiques va fonctionner.

Certificate Policy

Lorsqu'une autorité de certification émet un certificat, elle fournit à l'utilisateur d'un certificat la preuve qu'une clé publique particulière est bien liée à une entité particulière. Les différents certificats émis par cette autorité peuvent suivre des pratiques et des procédures différentes et être applicables à des applications ou à des sujets différents. Le standard X.509 définit une politique de certificat comme suit :

Définition 2.2 : « *C'est un ensemble de règles donné qui indique l'applicabilité d'un certificat pour une communauté particulière et/ou une classe d'applications ayant des exigences communes point de vue sécurité.* »

Les politiques de certificats constituent également la base de l'accréditation des autorités de certification. Chaque autorité est accréditée pour une ou plusieurs politiques de certificats, ce qui lui permet de les implémenter.

A partir du standard X.509 v3, la politique de certificat est incluse ou référencée dans le certificat électronique. Dans une politique, on retrouve entre autres les informations suivantes :

- les procédures d'authentification des utilisateurs par l'autorité de certification,
- les problèmes légaux (responsabilité) qui peuvent se poser si l'autorité de certification devient compromise ou est utilisée avec de mauvaises intentions,
- à quelles fins le certificat pourra être utilisé,
- les exigences de la gestion de la clé privée, comme le stockage sur carte à puce ou autre dispositif matériel,
- si la clé privée peut être exportée,
- les exigences des utilisateurs du certificat (ce qu'ils doivent faire si leur clé privée est perdue ou compromise…),
- les exigences pour l'enrôlement et le renouvellement d'un certificat,
- la période de validité d'un certificat,
- les algorithmes cryptographiques à utiliser,
- la longueur minimale de la paire de clés publique et privée.

---

[8] Source bibliographique : *[IETF2527]*

CPS : « Certificate Practice Statement »

Un « Certificate Practice Statement » peut être défini comme une déclaration des pratiques utilisées par une autorité de certification pour émettre des certificats.

Ce document peut prendre la forme d'une déclaration émanant d'une autorité de certification et reprenant les détails de son système de confiance ainsi que des pratiques utilisées pour les opérations d'émission de certificats. Il doit également apparaître dans le contrat qui lie l'autorité de certification au demandeur de certificat. Le « Certificate Practice Statement » peut comprendre plusieurs documents parmi lesquels des lois publiques existantes et des contrats privés. Les personnes et les organisations utilisent le CPS d'une autorité pour déterminer le niveau de confiance qu'ils accordent à l'autorité de certification. Il peut contenir les informations suivantes :

- une identification positive de l'autorité de certification (nom de l'autorité de certification, nom du serveur et adresse DNS[9]),
- les politiques de certificats implémentées par l'autorité ainsi que les types de certificats pouvant être émis,
- les politiques, procédures et procédés d'émission et de renouvellement des certificats,
- les algorithmes cryptographiques, CSP[10] et longueur de clé utilisés pour le certificat de l'autorité,
- la période de validité du certificat de l'autorité de certification,
- la sécurité physique de l'autorité, du réseau ainsi que les procédures de sécurité,
- la période de validité de chaque certificat émis par l'autorité de certification,
- les politiques de révocation des certificats (conditions pour révoquer, par exemple fin de carrière d'un employé, mauvaise utilisation de privilèges de sécurité...),
- les politiques pour les listes de révocation (CRL) : point de distribution de ces listes[11] et intervalles de publication,
- la politique de renouvellement du certificat de l'autorité de certification avant son expiration.

Relation entre « Certificate Policy » et « Certificate Practice Statement »

Les concepts de politique de certificat et de « Certificate Practice Statement » proviennent de sources différentes et ont été développés pour des raisons différentes. Malgré cela, leur corrélation est importante.

Comme cela a été vu précédemment, un CPS est une déclaration détaillée qui reprend les pratiques d'une autorité de certification et qui doit être consultée et comprise par les demandeurs et les utilisateurs des certificats. Le niveau de détail de cette déclaration peut varier mais il est toujours plus élevé que la définition des politiques de certificats. De plus, une autorité de certification ayant un CPS unique peut supporter plusieurs politiques de certificats (utilisées à

[9] Domain Name System

[10] Cryptographic Service Provider : accomplit toutes les opérations cryptographiques et gère les clés privées

[11] CDP = CRL Distribution Point

des fins différentes), et plusieurs autorités différentes, ayant des CPS différents, peuvent supporter la même politique de certificat.

Enfin, la différence principale se situe dans le fait que le « Certificate Practice Statement » est un document sur mesure pour les pratiques de chaque organisation tandis que les différences entre les politiques de certification pour un même usage doivent être aussi réduites que possible afin que le certificat puisse être reconnu par le plus grand nombre possible de systèmes.

2.3 Applications[12] utilisant l'infrastructure à clés publiques[13]

2.3.1 Smart Card Logon

Une Smart Card[14] est une carte de crédit de taille classique mais avec une puce électronique intégrée. Les données et/ou programmes y sont stockés en toute sécurité. Cependant, certaines cartes ne sont pas protégées et ce qui y est stocké est accessible à n'importe qui. Normalement, seul le propriétaire de la carte peut accéder à l'information en prouvant son identité avec un code PIN[15]. Cette carte à puce est inviolable car il est très difficile de reproduire l'information qu'elle contient sans avoir les droits d'accès nécessaires (code PIN). Elles peuvent donc être utilisées pour stocker les certificats d'un utilisateur et ses clés privées. Les Smart Cards peuvent effectuer des opérations de cryptographie à clés publiques très sophistiquées comme la signature numérique et l'échange de clés.

L'utilisation de cartes à puce permet une plus grande authentification et la non-répudiation de l'utilisateur pour une large gamme de solutions sécurisées comme l'ouverture d'une session à travers un réseau, les communications Web sécurisés et le courrier électronique sécurisé.

Avantages des Smart Cards

Les avantages de l'utilisation des cartes à puce sont les suivants :

- **Les clés privées sont stockées dans une carte à puce « inviolable »** plutôt que sur un média moins sécurisé comme le disque dur d'un utilisateur. Les Smart Cards fournissent une sécurité plus importante pour l'authentification et la non-répudiation de l'utilisateur. Le stockage des clés dans la carte à puce s'effectue au moyen d'un petit système d'exploitation interne permettant la génération des clés. La clé privée n'étant pas exportable, elle est ainsi protégée des menaces extérieures. De plus, si un individu essaye de s'introduire dans la carte pour découvrir les clés, le contenu est automatiquement effacé.
- **Les opérations cryptographiques sont isolées du système d'exploitation**, les Smart Cards ne sont pas susceptibles d'être attaquées via le système d'exploitation (comme par les « Buffer Overflow Attacks » et « Memory Dump Attacks » qui peuvent révéler les clés privées ou autres secrets cryptographiques).

---

[12] Dans le contexte du système d'exploitation Microsoft Windows 2000

[13] Source bibliographique : *[MSRKit00a]*

[14] Carte à puce

[15] Personal Identification Number

- **Cette méthode autorise la portabilité des données personnelles et autres informations privées** entre les ordinateurs sur le lieu de travail, à la maison ou sur la route…

L'ouverture de session avec une Smart Card apporte une sécurité accrue par rapport aux autres procédés traditionnels qui dépendent de mots de passe. De plus, l'administration liée à ces méthodes est très élevée et l'emploi de cartes la diminuera significativement.

La Smart Card ne pourra être utilisée que par une personne **possédant cette carte** et **connaissant le code PIN**.

Comparaison PINs et mots de passe

Les « Personal Identification Numbers » apportent une protection plus significative que les mots de passe réseaux standard.

Les **mots de passe** (ou des dérivés comme les condensés[16]) voyagent sur les réseaux et sont sujets à des « Brute Force Attacks » (« Key Search Attacks ») dans lesquelles le pirate essaye toutes les combinaisons possibles jusqu'à ce qu'il trouve le mot de passe. Les mots de passe sont aussi la cible des « Dictionary Attacks » dans lesquelles un pirate essaye des mots se trouvant dans des dictionnaires ainsi que de nombreux mots de passe fréquents pour connaître le véritable mot de passe. Comme la plupart des utilisateurs préfèrent des mots de passe faciles à retenir, les « Dictionary Attacks » représentent souvent un raccourci par rapport aux « Brute Force Attacks ».

La force d'un mot de passe dépend de plusieurs facteurs : sa longueur, la manière dont son propriétaire le protège, la manière dont il est protégé sur le réseau et la difficulté de le deviner. Mais même les mots de passe qui sont chiffrés lors des transmissions et qui ne sont pas susceptibles de subir des « Dictionary Attacks » peuvent être cassés par des « Brute Force Attacks » en quelques semaines ou mois par un pirate qui intercepte le mot de passe sur un réseau.

Par contre, les **PINs** ne voyagent jamais sur des réseaux et ne peuvent donc jamais être captés. De plus, les « Dictionary Attacks » et « Brute Force Attacks » ne peuvent être tentées que par une personne en possession physique de la carte. Même si cette personne possède celle-ci, la Smart Card se bloque après un nombre limité de tentatives infructueuses. C'est ce qui rend les attaques sur des Smart Card infaisables.

Un autre avantage des cartes à puce vient du fait que les politiques liées aux PINs peuvent être moins restrictives que les politiques applicables aux mots de passe. En général, un bon mot de passe réseau doit être changé assez souvent, en plus d'être long et complexe. Vu que les utilisateurs ont tendance à écrire leurs longs mots de passe difficiles à retenir, la sécurité des réseaux est amoindrie. Par contre, un bon PIN peut être changé plus rarement et être relativement court. Dans ce cas, les utilisateurs pourront plus facilement s'en souvenir et la sécurité des réseaux risquera moins d'être compromise à cause d'un PIN malencontreusement écrit quelque part.

---

[16] Traduction du mot anglais "Hash"

Processus d'ouverture de session

L'authentification de l'utilisateur lors du processus d'ouverture de session sous Microsoft Windows 2000 s'effectue au moyen du protocole Kerberos. Ce protocole est expliqué en détail dans le chapitre 3 au point 3.4.

Le processus d'ouverture d'une session de travail avec une carte à puce se déroule de la manière suivante : l'utilisateur insère sa carte à puce dans le lecteur prévu à cet effet, il introduit son code PIN et, si ce code et les données de la carte sont valides, la session de l'utilisateur est ouverte et le lien avec son compte utilisateur est créé avec les permissions qui lui ont été accordées. Les données de la carte sont valides si le certificat qui s'y trouve est valide et s'il a été émis par une autorité de certification reconnue par l'organisation.

Si certaines personnes ont encore la possibilité de se connecter au réseau avec un mot de passe traditionnel, la sécurité du réseau sera du niveau du mot de passe le plus faible du système. Pour un maximum de sécurité lors de l'ouverture de sessions de travail, l'utilisation de cartes à puce doit être généralisée à tous les utilisateurs et ceux-ci doivent être obligés d'y avoir recours pour se connecter à n'importe quel poste de travail. Mais cette obligation ne peut pas s'appliquer directement lors de l'installation du processus car les utilisateurs doivent avoir la possibilité de s'habituer à manipuler ces cartes.

Un autre avantage de l'utilisation des cartes à puce est la possibilité de demander au système de bloquer la session de l'utilisateur si celui-ci retire sa carte. Quand un utilisateur quitte son ordinateur pendant une session active et qu'il oublie de le sécuriser en le bloquant ou en quittant la session, un intrus peut utiliser l'ordinateur avec des intentions malveillantes. Avec les cartes à puce, cette situation ne sera plus possible si le système a bien été configuré.

2.3.2 E-mail signés et chiffrés : S/MIME[17]

Le courrier Internet standard est envoyé sur les réseaux en clair sans aucune sécurité. Des intrus pourraient surveiller les serveurs de courrier et le trafic sur le réseau pour obtenir des informations personnelles ou sensibles. De plus, il existe un risque pour les informations confidentielles de l'organisation lors d'envoi de mails sur Internet. En effet, les messages envoyés sur Internet peuvent être interceptés et lus par des espions qui écoutent le trafic Internet ou bien par les administrateurs des serveurs de courrier et des réseaux se trouvant sur la route du message. Une autre forme d'intrusion est l'usurpation d'identité, qui consiste à falsifier l'adresse IP des expéditeurs et l'en-tête du mail. C'est pourquoi l'utilisation d'un courrier sécurisé est nécessaire : il garantit la confidentialité des communications, l'intégrité des données et la non-répudiation.

Le standard S/MIME autorise la signature numérique et le chiffrement du courrier confidentiel. Le courrier électronique sécurisé peut être échangé entre des clients S/MIME qui tournent sur n'importe quelle plate-forme ou n'importe quel système d'exploitation. Ces clients peuvent envoyer des messages sur Internet sans tenir compte du type de serveur mail qui traite

[17] Secure/Multipurpose Internet Mail Extension

les messages entre leur origine et leur destination finale car c'est au niveau du client que toutes les opérations cryptographiques sont effectuées, et non au niveau du serveur.

Afin de garantir l'authentification des messages, l'intégrité des données et la non-répudiation, les personnes peuvent signer les messages avec leur clé privée avant de les envoyer. Le destinataire utilise la clé publique de l'expéditeur pour vérifier la signature numérique du message. L'expéditeur doit détenir un certificat valide pour courrier sécurisé et le destinataire doit être en possession d'une copie de ce certificat avant de pouvoir vérifier la signature (car la clé publique est incluse dans le certificat).

Les personnes peuvent également envoyer et recevoir du courrier confidentiel. Les applications clientes génèrent aléatoirement des clés symétriques de chiffrement et utilisent cette clé secrète pour chiffrer les messages afin de garantir la confidentialité. Elles protègent ensuite cette clé secrète en la chiffrant avec la clé publique du destinataire (s'il y en a plusieurs, les applications procèdent à des chiffrements séparés pour chaque destinataire avec leur certificat respectif) et envoient au destinataire cette clé chiffrée attachée au message, celui-ci étant également chiffré. Le destinataire utilise sa clé privée pour déchiffrer la clé secrète de chiffrement et utilise cette clé pour déchiffrer le message.

Donc, grâce à l'utilisation de clients sécurisés, l'expéditeur est assuré que l'intégrité de ses messages est préservée et que seuls les réels destinataires pourront lire les messages chiffrés. Le destinataire est certain que le message est authentique et qu'il provient bien de l'expéditeur indiqué.

2.3.3 Web sécurisé : SSL[18]

Les communications par Internet basées sur le protocole TPC/IP[19], comme les protocoles HTTP[20], Telnet et FTP[21], ne sont pas sécurisées car toutes les communications se déroulent en clair. Les informations confidentielles et sensibles qui sont transmises via ces protocoles peuvent facilement être interceptées et lues à moins que l'information ne soit protégée par une technologie de chiffrement.

Les serveurs Web qui n'utilisent que le standard HTTP pour communiquer avec leurs clients sont des proies faciles pour des attaques parce que n'importe quel client peut envoyer des requêtes HTTP à un serveur Web et exploiter les faiblesses du protocole HTTP ou de son implémentation. De plus, les clients qui communiquent en utilisant le protocole HTTP sont également des cibles faciles pour des serveurs Web non-autorisés, qui peuvent usurper l'identité de sites légaux et porter préjudice aux clients (par exemple envoyer des virus à ceux-ci).

Les protocoles de communication Web sécurisée fournissent un moyen d'authentifier les clients et les serveurs sur Internet et de protéger la confidentialité des communications entre clients et serveurs. Plusieurs standards de communication sécurisée utilisant la technologie à

---

[18] Secure Socket Layer

[19] Transfer Control Protocol/Internet Protocol

[20] Hypertext Transfer Protocol

[21] File Transfer Protocol

clés publiques ont été développés, comme S-HTTP[22], IPSec[23] et SSL 3.0 qui est le plus utilisé actuellement sur Internet. Un désavantage de SSL est que la force du chiffrement utilisé sur les canaux sécurisés est soumise à des restrictions gouvernementales d'import-export : la force du chiffrement à clé symétrique utilisé pour une technologie non-exportable est plus importante (128 bits) que celle admise pour les technologies exportables (40 bits ou 56 bits). Le client et le serveur doivent utiliser la même force cryptographique et le même algorithme de chiffrement quand ils communiquent sur un canal sécurisé. Au début d'une session SSL, le serveur choisit la cryptographie la plus importante disponible à la fois chez le client et le serveur. La sécurité pour des communications sécurisées SSL n'est maximale que si le client et le serveur supportent la cryptographie non-exportable la plus élevée.

Avantages des communications Web sécurisées

SSL apporte les protections suivantes pour les communications sur Internet :

- **Authentification du serveur** : Elle est basée sur le certificat d'authentification du serveur. Les clients peuvent identifier le serveur au moyen de son certificat et choisissent de communiquer avec les serveurs authentifiés. Les clients sont capables de détecter si une personne non-autorisée essaye d'usurper l'identité d'un serveur Web légitime.
- **Authentification mutuelle entre serveurs et clients** : Elle est basée sur des clients et des serveurs ayant des certificats valides et de confiance. Les serveurs et les clients choisissent de faire confiance uniquement à des certificats émis par des autorités de certification spécifiques. Les clients qui ne sont pas en possession d'un certificat d'authentification valide sont empêchés de communiquer avec les serveurs Web, ce qui réduit le risque d'attaques du type « Denial of Service ».
- **Communications Web confidentielles par l'utilisation d'un canal chiffré et sécurisé** : Le serveur et le client négocient l'algorithme cryptographique qui sera utilisé. Ils négocient également la clé de session secrète et partagée qui sera utilisée dans les communications sécurisées. Les communications Web sécurisées utilisent par défaut la plus longue clé de session supportée à la fois par le client et par le serveur.
- **Intégrité des données** : Elle est basée sur les HMACs[24]. Un intrus ne peut altérer les données car l'information transmise est accompagnée d'un résumé du message qui doit être vérifié avant que l'information ne soit acceptée par le client ou le serveur.

2.3.4 IPSec et Virtual Private Network : VPN

IPSec opère au niveau de la couche réseau IP et de la couche transport TCP/UDP et est transparent pour le système d'exploitation et les applications. IPSec comporte une série de directives pour la protection des communications IP. Il spécifie les moyens de protéger les informations privées transmises via un réseau public. Les services supportés par IPSec sont les suivants :

---

[22] Secure Hypertext Transfer Protocol

[23] IP Security

[24] Hash Message Authentication Codes

- Authentifie l'expéditeur de paquets de données IP sur la base d'une authentification Kerberos, des certificats électroniques ou bien d'une clé secrète partagée (ou d'un mot de passe).
- Assure l'intégrité des paquets de données IP qui sont transmis à travers le réseau.
- Chiffre toute donnée qui est envoyée sur le réseau pour une confidentialité totale.
- Cache les adresses IP d'origine pendant que les paquets voyagent.

Virtual Private Network

Un réseau privé virtuel (VPN) est l'extension d'un réseau privé qui contient des liens à travers un réseau partagé ou public comme Internet. Un VPN permet d'envoyer des données entre deux ordinateurs à travers un réseau public en émulant les propriétés d'un lien privé point à point.

Pour l'émulation d'un lien point à point, les données sont encapsulées ou bien compactées, avec un en-tête qui spécifie le cheminement de l'information en lui permettant de traverser un réseau public pour atteindre sa destination. De plus, les données envoyées sont chiffrées pour garantir la confidentialité. Les paquets qui sont interceptés sur le réseau public sont alors indéchiffrables sans les clés de chiffrement. Ce lien dans lequel les données sont encapsulées et chiffrées est connu sous le nom de connexion VPN.

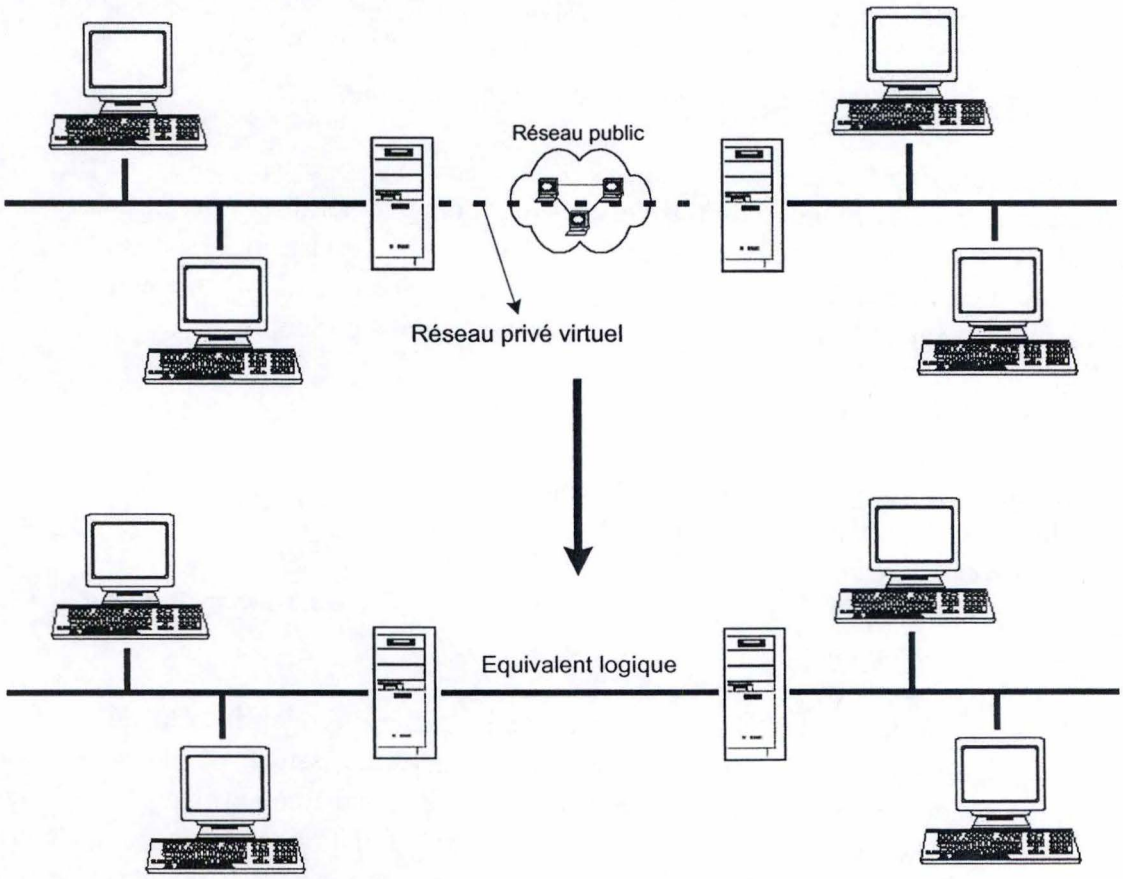

Figure 12 : Concept de réseau privé virtuel

Les connexions VPN permettent aux utilisateurs travaillant chez eux ou sur la route d'obtenir une connexion d'accès à distance avec le serveur de leur organisation en utilisant l'infrastructure de réseaux publics comme Internet. L'infrastructure exacte du réseau public importe peu car, d'un point de vue logique, les données sont envoyées via un lien privé spécialement prévu à cet effet. Les connexions VPN permettent aux organisations d'avoir des connexions avec des bureaux géographiquement éloignés ou avec des organisations sur Internet tout en maintenant des communications sécurisées.

2.3.5 Chiffrement de données : EFS[25]

La technologie de sécurité EFS autorise un utilisateur individuel à chiffrer des fichiers de telle sorte qu'ils ne soient pas lisibles par les autres utilisateurs. EFS utilise un attribut de chiffrement par fichier pour désigner quels sont les fichiers protégés. Quand cet attribut est sélectionné, le fichier est stocké comme donnée chiffrée. Quand un utilisateur autorisé veut accéder à un fichier protégé à l'intérieur d'une application, EFS déchiffre le fichier en arrière-plan et fournit à cette application une copie en clair. Cet utilisateur peut voir et modifier ce fichier et EFS sauvegarde de manière transparente chaque changement comme donnée chiffrée. Les autres utilisateurs n'ont pas d'accès en lecture ou en écriture à ce fichier.

Un des usages les plus fréquents est le chiffrement des données sur les ordinateurs portables pour protéger les fichiers en cas de vol des ordinateurs.

Chiffrement de fichiers et technologie à clés publiques

Pour que EFS fonctionne, l'utilisateur doit être en possession d'un certificat valide d'utilisateur EFS et au moins un « recovery agent » doit être défini et être en possession d'un certificat valide de « EFS recovery ». EFS ne demande pas obligatoirement une autorité de certification pour émettre les certificats parce qu'il génère automatiquement ses propres certificats utilisateurs et le certificat pour le « recovery agent » par défaut.

EFS chiffre des fichiers de la manière suivante :

- Il génère une clé symétrique de chiffrement,
- chiffre les fichiers en utilisant cette clé,
- chiffre cette clé en utilisant la clé publique de l'utilisateur EFS,
- stocke la clé chiffrée dans un champ spécial (appelé « Data Decryption Field » (DDF)) attaché au fichier EFS.

EFS peut ensuite utiliser la clé privée de l'utilisateur pour déchiffrer la clé symétrique de chiffrement de même que le fichier si nécessaire. Comme l'utilisateur est le seul à posséder la clé privée, les autres personnes ne peuvent trouver la clé de chiffrement. De plus, EFS autorise un « recovery agent » désigné à déchiffrer et à récupérer le fichier dans le cas où la clé privée de l'utilisateur serait endommagée ou perdue. Pour chaque compte de « recovery agent », EFS procède comme suit :

---

[25] Encrypting File System

- Il chiffre la clé symétrique de chiffrement en utilisant la clé publique provenant des certificats de « recovery agent »,
- stocke la clé chiffrée dans un autre champ spécial (appelé « Data Recovery Field » (DRF)) attaché au fichier EFS.

2.3.6 Logiciels signés : Code Signing

Les logiciels qui sont téléchargés d'Internet sur les ordinateurs des utilisateurs peuvent contenir des programmes comme des virus ou des chevaux de Troie qui ont été développés pour causer des dommages ou bien pour fournir un accès clandestin à un réseau. Comme les réseaux sont de plus en plus interconnectés, les logiciels délictueux et virus deviennent aussi un danger pour les réseaux internes. Pour aider à contrer cette menace croissante, une société peut recourir à la signature numérique des logiciels qu'elle distribue sur son réseau interne ou sur Internet, et cela afin d'assurer leur intégrité. Les logiciels signés permettent aux utilisateurs de vérifier leur origine et de s'assurer qu'aucune personne n'a eu l'occasion de les altérer, car n'importe quelle modification du logiciel, après sa signature, invalide la signature numérique.

Chapitre 3 : Environnement Windows 2000

Source bibliographique : [W2kmag00]

Le système d'exploitation Microsoft Windows 2000 a été conçu pour atteindre certains objectifs afin de favoriser le commerce électronique :

Améliorer la sécurité

- L'authentification NT LAN Manager (NTLM) a été remplacée par Kerberos pour corriger les faiblesses de NTLM.
  En effet, cette authentification NTLM est utilisée par les services Telnet pour la connexion des clients. Quand cette connexion s'établit entre un système Microsoft et un autre système comme UNIX, le nom d'utilisateur et le mot de passe sont envoyés en clair sur le réseau. Un espion peut donc facilement s'approprier ceux-ci pour s'en servir à mauvais escient.
- Le support de l'infrastructure à clés publiques réduit les risques causés par les mots de passe et le support des cartes à puce améliore la sécurité des clés privées.
- L'accès physique aux disques durs est protégé avec l'apparition de la technologie d' « Encrypting File System ».

Supporter les standards et protocoles du marché

Microsoft Windows 2000 utilise des standards (comme LDAP[26], Kerberos, PC/SC[27], PKCS[28], IPSec[29], etc.) au lieu de technologies propriétaires (qui sont toujours supportées). L'utilisation de standards augmente l'interopérabilité du système et permet de remplacer certaines fonctionnalités par des solutions plus appropriées.

Réduire les coûts de développement des applications

Les API[30] de Windows 2000 favorisent la réutilisation de services (par exemple le service de chiffrement) assurés par le système d'exploitation. L'abstraction des applications du fournisseur les protège de l'obsolescence. Il est possible de mettre à jour et d'améliorer les composants au fur et à mesure du progrès de la technologie sans affecter l'application.

De plus, le support de l'infrastructure à clés publiques dans tout le système d'exploitation inclut le support des cartes à puces, l'accès Web basé sur l'infrastructure à clés publiques, le réseau privé virtuel (VPN), l'Encrypting File System (EFS), le courrier sécurisé et les logiciels signés. Windows 2000 supporte ces composants à travers ses services de sécurité distribués comme les services de l'Active Directory, les services cryptographiques, les services de certificats, les services d'authentification, les protocoles de transport sécurisés et les cartes à puce.

---

[26] Lightweight Directory Access Protocol

[27] Intégration du PC et de la carte à puce

[28] Public Key Cryptographic Standards

[29] IP Security

[30] Application Programming Interface

3.1 Active Directory (AD)

Un service d'annuaire consiste à la fois en un système de stockage du répertoire (appelé le « Directory Store ») et en un mécanisme qui est utilisé pour localiser et récupérer les informations du système. L'Active Directory, le service d'annuaire qui est inclus dans Microsoft Windows 2000, stocke les objets qui apportent de l'information à propos des choses réelles existant dans le réseau de l'organisation et qui sont associés à un ou plusieurs domaines, comme des utilisateurs, des groupes spécifiques d'utilisateurs, des ordinateurs, des applications, des services, des fichiers, etc. Cette information est disponible pour tous les utilisateurs et applications partout dans l'organisation.

L'Active Directory permet de résoudre les problèmes dont souffraient les précédents systèmes d'exploitation en termes de capacité de montée en charge, d'extensibilité, d'administration et d'ouverture de cet annuaire. En effet, avec l'Active Directory, les domaines peuvent comporter jusqu'à un million d'objets, contre à peine 20.000 auparavant. Les changements effectués sur un contrôleur de domaine se dupliquent pour le reste de l'environnement et cette duplication est paramétrable afin d'optimiser les performances et de protéger la bande passante.

De plus, l'administration est beaucoup plus puissante avec l'Active Directory. Il est possible d'organiser les utilisateurs et les ordinateurs à l'intérieur d'une hiérarchie représentant la structure réelle de l'organisation. Les domaines peuvent avoir des domaines parents et fils (sauf le domaine racine qui n'a pas de parent). A l'intérieur d'un domaine, les « Organizational Units » (OU) font apparaître la structure et des privilèges administratifs individuels peuvent être définis à tous les niveaux. L'Active Directory permet également de publier les ressources, comme les répertoires partagés, de telle sorte que les utilisateurs n'aient pas besoin de connaître la localisation physique du serveur. Une application peut être déplacée d'un serveur à un autre sans que l'utilisateur s'en rende compte.

Les méthodes d'accès à l'Active Directory (LDAP[31] et ADSI[32]) et sa structure basée sur X.500 donnent une architecture ouverte et lui permettent de s'intégrer à d'autres systèmes d'exploitation et aux applications prenant en charge les annuaires.

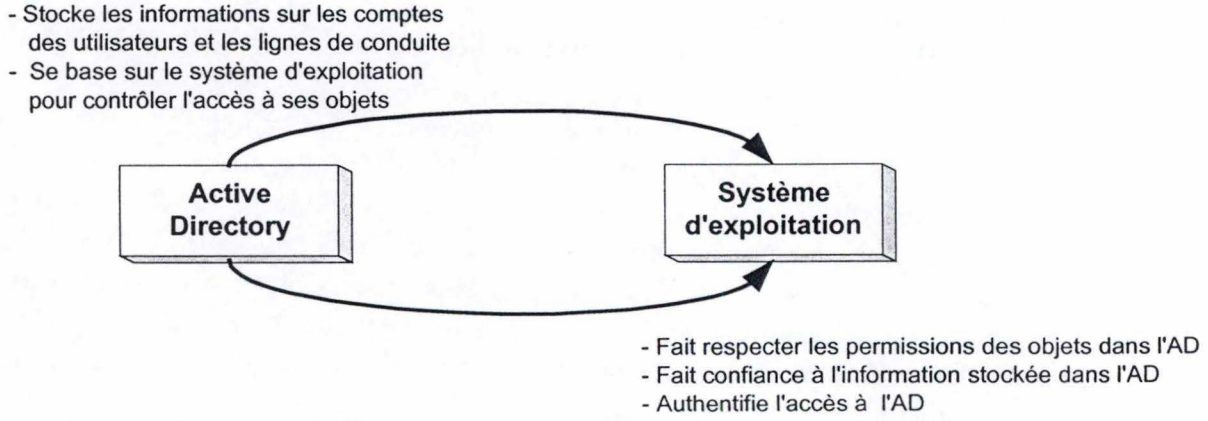

Figure 13 : Relation entre l'Active Directory et le système d'exploitation

[31] Lightweight Directory Access Protocol

[32] Active Directory Service Interface

L'Active Directory a une relation symbiotique avec le reste du système d'exploitation. Windows 2000 utilise l'Active Directory comme stock de données pour les informations sur les comptes des utilisateurs et les lignes de conduite et utilise la hiérarchie pour contrôler le flux de l'héritage de ces politiques. De son côté, l'Active Directory compte sur le système d'exploitation pour authentifier et contrôler l'accès aux objets de l'Active Directory.

Les avantages de l'Active Directory sont les suivants :

- **Sécurité** : L'Active Directory fournit une infrastructure pour une variété de nouvelles capacités dans le domaine de la sécurité. En utilisant l'authentification mutuelle, les clients sont capables de vérifier l'identité d'un serveur avant de transmettre des données sensibles et en supportant la sécurité à clés publiques, les utilisateurs peuvent se connecter en utilisant des cartes à puce au lieu des mots de passe.
- **Administration flexible et simplifiée** : Les objets dans l'Active Directory ont un contrôle d'accès par attribut qui permet une délégation de l'administration très fine. La délégation de l'administration autorise à distribuer plus efficacement les responsabilités administratives dans l'organisation et réduit le nombre d'utilisateurs qui ont un contrôle sur tout le domaine.
- **Modularité** : L'Active Directory utilise le « Domain Name System » (DNS) comme mécanisme de localisation. Le DNS est un système utilisé sur les réseaux, dont Internet, pour faire correspondre les adresses IP[33] à des noms plus conviviaux. L'annuaire stocke les informations en utilisant des domaines, qui sont des partitions permettant de distribuer cet annuaire à travers un large réseau de vitesse et fiabilité variables. La combinaison de localisation et de répartition assure que le répertoire s'adapte parfaitement à la croissance d'une organisation.
- **Grande disponibilité** : Les annuaires traditionnels avec une réplication « single master » offrent une grande disponibilité pour les requêtes mais pas pour les opérations de mise à jour. Avec la réplication « multimaster », l'Active Directory offre une grande disponibilité à la fois pour les opérations de requête et celles de mise à jour.
- **Extensibilité** : Le schéma, qui contient une définition de chaque classe d'objet qui peut exister dans le service d'annuaire, est extensible. Les administrateurs et les développeurs de logiciels ont alors la possibilité d'adapter l'annuaire à leurs besoins.
- **Support des standards ouverts** : L'Active Directory est construit avec des protocoles basés sur des standards comme :
  - DNS : pour la localisation des serveurs où se trouve l'Active Directory
  - LDAP[34] : comme protocole de requête et de mise à jour
  - Kerberos : pour l'ouverture d'une session et l'authentification

  Le support de standards ouverts rend possible l'utilisation d'une large variété de logiciels avec l'Active Directory, comme les carnets d'adresses de clients basés sur LDAP.
- **Programmation de l'accès simplifiée** : Les ADSI[35] sont accessibles à partir d'une variété de plates-formes de programmation. Quand les administrateurs et les développeurs de logiciels utilisent les ADSI, ils peuvent créer rapidement des applications puissantes tirant parti de l'annuaire.

---

[33] Internet Protocol

[34] Lightweight Directory Access Protocol

[35] Active Directory Service Interfaces

3.2 CryptoAPI

La CryptoAPI est un composant de l'architecture de sécurité de Windows 2000 aussi fondamental que l'Active Directory. Le but de la CryptoAPI est d'être une source unique de services de chiffrement de base pour toutes les applications et autres composants du système d'exploitation utilisant des services de chiffrement (CSP[36]) installables. Ces services de chiffrement prennent en charge la génération des clés, les signatures, le chiffrement, le hashing et les services de certificats grâce à des interfaces standard.

Chaque service de chiffrement apporte une implémentation différente de la CryptoAPI. Certains fournissent des algorithmes cryptographiques plus puissants pendant que d'autres contiennent des composants matériels comme des cartes à puce.

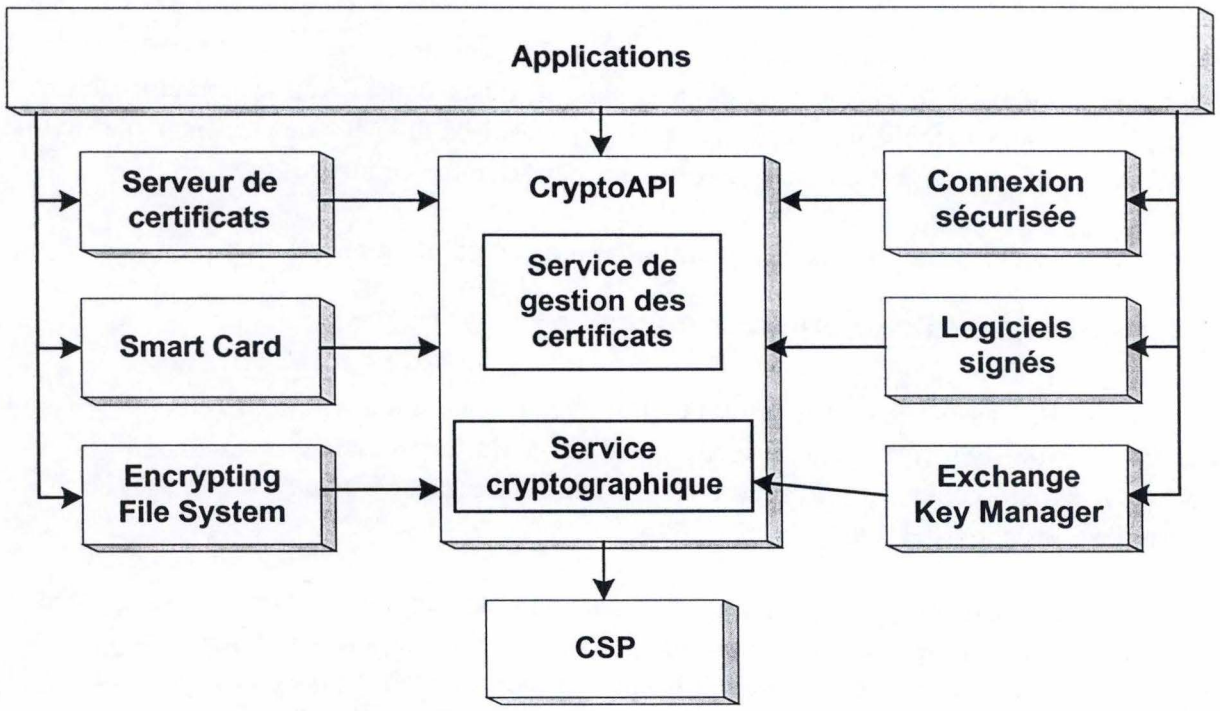

Figure 14 : CryptoAPI

La CryptoAPI confirme l'objectif de Microsoft Windows 2000 de réduire le coût de développement des applications de trois manières :

- Les développeurs ne doivent pas implémenter du code cryptographique.
- Ils peuvent développer une application une fois pour toutes en utilisant différents standards et protocoles cryptographiques.
- Les applications ne devront pas être modifiées lorsque les techniques de chiffrement évolueront.

De plus, la CryptoAPI possède des fonctions importantes pour l'infrastructure à clés publiques. En effet, les développeurs peuvent demander et publier des certificats et des listes de révocation (CRL) et construire des chaînes de certification lorsqu'une application de serveur

[36] Cryptographic Service Provider

doit contrôler la validité d'un certificat. Du fait que la CryptoAPI utilise les standards X.509 v3 et PKCS, les développeurs peuvent y avoir recours pour gérer les certificats dans le magasin de certificats natif de Windows 2000, dans l'Active Directory et dans d'autres autorités de certification tierces.

3.3 Certificate Services

Microsoft Windows 2000 intègre un service de certificat puissant et intégré au système d'exploitation. Il assure les fonctions de base d'une autorité de certification, à savoir la demande, l'émission, la publication et la gestion des certificats. De plus, les services de certificats utilisent l'Active Directory pour stocker et publier les certificats. L'Active Directory permet d'associer facilement des certificats aux utilisateurs et de tirer parti des fonctions de gestion du GPE[37] pour contrôler à qui, par qui et pourquoi les certificats ont été émis.

Par rapport à avant, Microsoft a ajouté les fonctions de gestion de certificats à la CryptoAPI et déplacé le magasin de données de certificats dans l'Active Directory ;en outre comme les services de certificats accèdent à leur magasin de données de certificats par le biais de la CryptoAPI, ils peuvent publier les certificats dans d'autres annuaires tiers.

Ces services de certificats seront vus plus en détail au point 5.2 du chapitre 5.

3.4 Services d'authentification

La SSPI[38] assure les services d'authentification grâce à une autre API. Les applications client/serveur ont besoin d'authentifier le client vis-à-vis du serveur et de temps en temps le serveur vis-à-vis du client. SSPI procure un avantage d'abstraction analogue aux interfaces CSP des applications client/serveur.

La SSPI est une API utilisée par beaucoup de services systèmes pour isoler les protocoles du niveau application des protocoles de sécurité servant à l'authentification sur un réseau. Les fournisseurs de sécurité utilisent des données différentes pour authentifier les utilisateurs : au moyen d'un secret partagé ou bien avec des certificats à clés publiques. Ces protocoles de sécurité interagissent avec différents services d'authentification et des magasins d'informations sur les comptes.

Needham et Schroeder

Le protocole de Needham et Schroeder permet à deux utilisateurs (ou bien à un utilisateur et à un serveur proposant un service) de se convaincre mutuellement de leur identité respective. Voici les conventions de représentations qui seront utilisées dans l'illustration suivante :

---

[37] Group Policy Editor

[38] Security Support Provider Interface

K_X^{Pub} : la clé publique de X

K_X^{Priv} : la clé privée de X

Nb_X : un nombre aléatoire généré par X

$C.T.$: le composant tiers

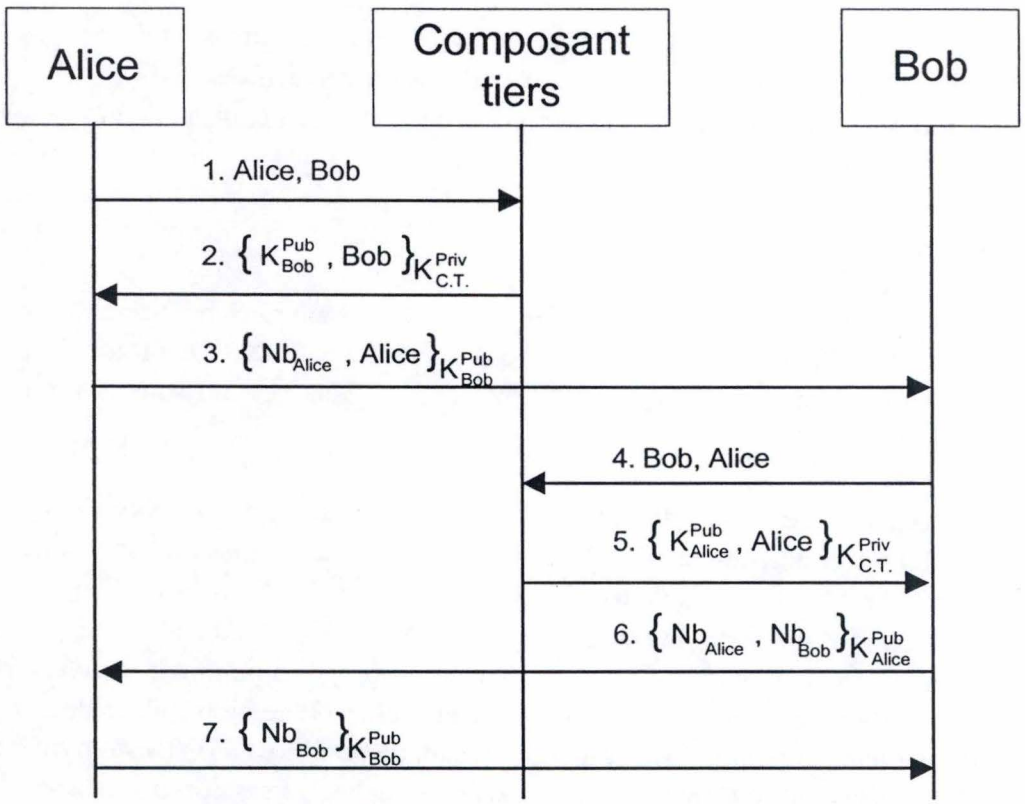

Figure 15 : Protocole de Needham et Schroeder

Dans la figure 15, le but d'Alice est de s'authentifier auprès de Bob au moyen d'un système à clés publiques. Le composant tiers représente un répertoire contenant toutes les clés publiques existant dans le système. Ce répertoire possède également une paire de clés dont la clé publique est connue de tous. Le protocole se déroule comme suit :

1. Alice indique au composant tiers son intention d'entrer en communication avec Bob en lui envoyant son identité ainsi que celle de Bob.
2. Le composant tiers renvoie à Alice un couple reprenant l'identité de Bob et sa clé publique. Ce couple est chiffré avec la clé privée du composant tiers.
3. Alice possède la clé publique du composant et peut donc déchiffrer le message reçu et vérifier l'identité du composant tiers. A ce moment, Alice envoie un couple comprenant un nombre aléatoire qu'elle vient de générer et son identité. Ce couple est chiffré avec la clé publique de Bob qu'elle vient de recevoir.
4. Bob déchiffre le message et découvre qu'Alice veut communiquer avec lui. Il annonce donc au composant tiers qu'il désire communiquer avec Alice (en envoyant son identité accompagnée de celle d'Alice).
5. Le composant tiers renvoie à Bob un couple reprenant l'identité d'Alice et sa clé publique. Ce couple est chiffré avec la clé privée du composant tiers.

6. Bob peut déchiffrer le message reçu et vérifier l'identité du composant tiers. A ce moment, Bob envoie à Alice le nombre aléatoire d'Alice reçu au point 4 avec un nombre aléatoire qu'il vient de générer. Le tout est chiffré avec la clé publique d'Alice.
7. Alice déchiffre le message reçu et vérifie si le premier nombre correspond bien au nombre aléatoire qu'elle avait généré. Si c'est le cas, **Bob est authentifié**. Afin de terminer cette procédure d'authentification, elle renvoie le deuxième nombre reçu au point 6, chiffré avec la clé publique de Bob.
8. Bob déchiffre le message reçu et vérifie si le nombre correspond bien au nombre aléatoire qu'il avait généré. Si c'est le cas, **Alice est authentifiée**.
9. A ce moment, les deux parties impliquées dans la communication sont donc authentifiées.

Kerberos[39]

Le protocole Kerberos s'inspire du protocole de Needham et Schroeder. Kerberos est le protocole d'authentification par défaut de Microsoft Windows 2000. Ce protocole définit les interactions entre un client et un service d'authentification réseau connu sous le nom de « Key Distribution Center » (KDC).

Le protocole Kerberos définit une série d'échanges entre les clients, le KDC et les serveurs pour obtenir et utiliser un ticket Kerberos. Quand un utilisateur se connecte à une station Windows, le SSP[40] de Kerberos acquiert un ticket Kerberos (TGT[41]) basé sur un condensé chiffré du mot de passe de l'utilisateur. Windows 2000 place ce TGT dans une cache pour les tickets sur la machine de l'utilisateur. Quand un programme client essaye d'accéder à un service réseau, l'application Kerberos vérifie si un ticket de session valide pour le serveur concerné se trouve dans la cache. S'il n'y a pas de ticket disponible, le TGT est envoyé dans une requête au « Key Distribution Center » pour recevoir un ticket de session qui permet d'accéder au serveur. Ce ticket de session est ajouté à la cache et pourra être réutilisé dans des connexions futures avec le même serveur jusqu'à son expiration. La période d'expiration du ticket peut être définie dans une politique de sécurité du domaine mais est de huit heures par défaut. Si le ticket de session expire durant une session active, le fournisseur de sécurité de Kerberos renvoie une valeur d'erreur qui autorise le client et le serveur à renouveler le ticket, générer une nouvelle clé de session et reprendre la connexion.

[39] Source bibliographique : *[MsSN00]*

[40] Security Support Provider

[41] Ticket-Granting Ticket

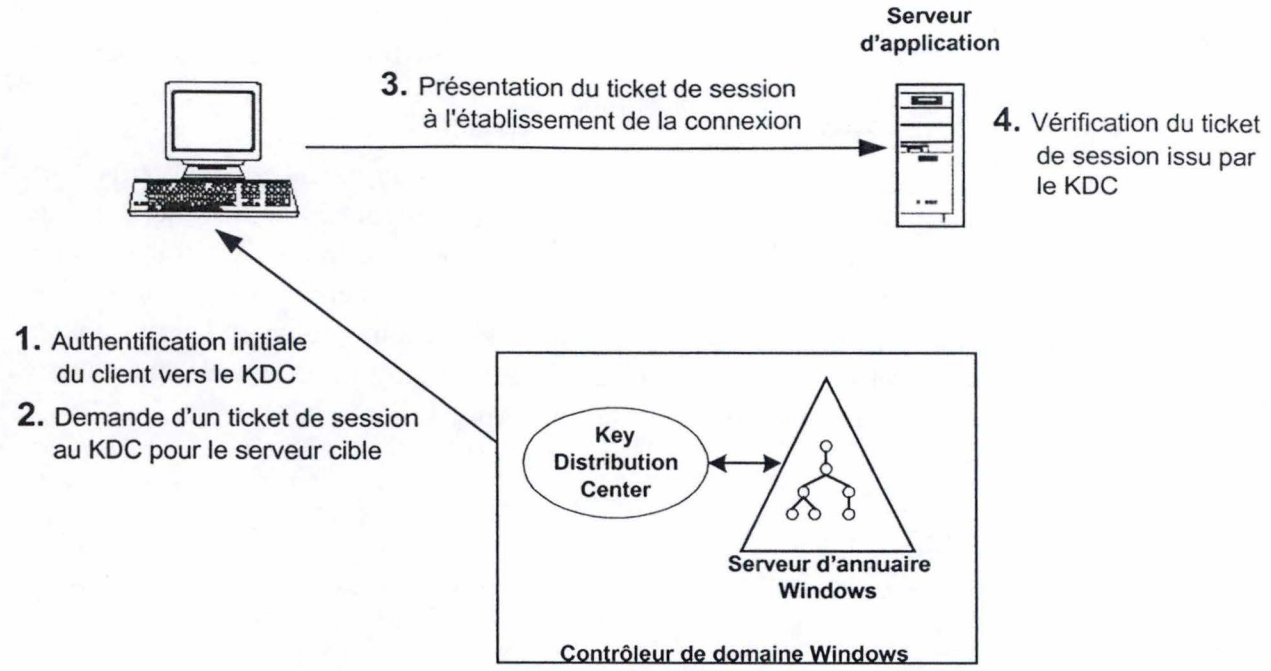

Figure 16 : Protocole d'authentification Kerberos

Le ticket de session Kerberos est présenté au service distant durant le message de connexion initial. Certaines parties du ticket de session sont chiffrées grâce à la clé secrète partagée entre le service et le KDC. Le serveur peut rapidement authentifier le client en vérifiant le ticket de session sans aller jusqu'au service d'authentification parce que l'application Kerberos pour le serveur garde une copie de la clé secrète du serveur en cache. Les tickets de session Kerberos contiennent une clé de session unique créée par le KDC à utiliser pour le chiffrement symétrique des informations d'authentification et des données transférées entre le client et le serveur. Dans le modèle Kerberos, le KDC est utilisé comme une tierce partie de confiance en ligne pour générer les clés de session.

Microsoft Windows 2000 implémente également des extensions du protocole Kerberos pour supporter l'authentification basée sur les paires de clés privées et publiques en plus des clés secrètes partagées. Les extensions de l'authentification à clés publiques autorisent le client à demander le TGT initial, en utilisant une clé privée, pendant que le KDC vérifie cette demande avec la clé publique retirée du certificat se situant dans l'objet utilisateur de l'Active Directory. Après l'authentification initiale de la clé privée, les protocoles standard Kerberos sont utilisés pour obtenir un ticket de session en vue de se connecter à des services réseau.

3.5 Chiffrement

Les deux endroits où il est possible de protéger des données critiques uniquement avec le chiffrement sont les disques et les réseaux.

L' « Encrypting File System » (EFS) de Windows 2000 chiffre les fichiers au niveau du système de fichier en cochant une simple case. EFS effectue le chiffrement et le déchiffrement en totale transparence pour l'utilisateur et les programmes. EFS est intégré à l'infrastructure à clés publiques de Windows 2000 et supporte la récupération des données chiffrées dans le cas où la clé privée de l'utilisateur serait perdue ou indisponible. C'est une amélioration pour les

utilisateurs d'ordinateurs portables qui sont très vulnérables vis-à-vis des vols. Malheureusement, il n'est pas encore possible de placer les clés privées pour l'EFS sur des cartes à puce pour augmenter encore plus leur sécurité.

Pour protéger les données à travers les réseaux, en totale transparence pour l'utilisateur et les applications, Windows 2000 utilise IPSec[42]. IPSec apporte l'authentification, la confidentialité, l'intégrité des données et le filtrage du trafic TCP/IP. L'implémentation d'IPSec est en dessous de la couche des protocoles d'applications et permet de sécuriser les communications pour toute application sans modification. IPSec est un protocole Internet solide qui bénéficie d'une large adhésion du marché. C'est l'Active Directory qui garde la stratégie IPSec et le contrôle de celle-ci se fait à travers le « Group Policy Editor ».

[42] IP Security

Chapitre 4 : Critères d'évaluation d'une infrastructure à clés publiques

Le choix du fournisseur d'un système d'infrastructure à clés publiques s'avère très difficile vu le nombre croissant de solutions différentes, chacune ayant ses avantages et ses inconvénients. Il est donc indispensable d'établir certains critères objectifs d'évaluation de tels systèmes afin d'implanter le système le plus proche des exigences. Les sources bibliographiques utilisées sont : *[BTInt00]* et *[MIEL99]*.

4.1 Facilité d'utilisation

Les principes de fonctionnement d'une infrastructure à clés publiques peuvent être très complexes mais la gestion de celle-ci doit pouvoir s'effectuer facilement. En effet, cette gestion sera le plus souvent effectuée par un personnel non-spécialisé dans une technologie qui doit fonctionner en toute confiance. Ces opérateurs ne doivent pas être confrontés aux manipulations complexes d'algorithmes cryptographiques, de clés et de signatures. C'est donc les logiciels d'infrastructure à clés publiques qui doivent prendre en charge ces opérations tout en offrant une interface intuitive aux opérateurs afin de faciliter leur tâche de gestion.

Ce critère de facilité d'utilisation est primordial car il détermine le coût et la durée de formation nécessaire pour être apte à gérer et à configurer correctement cette infrastructure, ainsi que l'efficacité et le degré de confiance associés à celle-ci.

4.2 Flexibilité

La flexibilité est indispensable dans un système d'infrastructure à clés publiques afin de permettre l'adaptation de toutes les procédures et pratiques aux besoins et aux exigences de l'organisation qui met en place cette infrastructure. Cette flexibilité doit se retrouver principalement dans les méthodes d'enregistrement, de distribution et de révocation des certificats.

Pour le support de cartes à puce et de modules matériels de sécurité (HSM[43]), l'emploi d'interfaces ouvertes et standard, telles que PKCS#11 (Cryptoki[44]), offre à l'infrastructure à clés publiques la flexibilité indispensable pour accepter de multiples systèmes de sécurité. Pour atteindre un niveau de confiance maximal, l'enregistrement des certificats devrait se faire en présence de l'intéressé mais ce n'est pas toujours possible dans les organisations très vastes. Dans ce cas, l'enregistrement devra se faire à distance. C'est pourquoi l'infrastructure doit autoriser les utilisateurs à demander des certificats par courrier électronique, à l'aide d'un navigateur Web standard ou bien automatiquement au moyen de périphériques de communication réseau pour VPN[45].

---

[43] Hardware Security Module

[44] Cryptographic Token Interface Standard

[45] Virtual Private Network

Au même titre que la facilité d'utilisation, la flexibilité aura une influence considérable sur la rentabilité d'un système d'infrastructure à clés publiques. Ensemble, elles affectent des facteurs tels que la formation, la maintenance, la configuration des systèmes, l'intégration ainsi que l'augmentation future du nombre d'utilisateurs. Tous ces éléments peuvent rendre le coût d'exploitation d'une infrastructure à clés publiques bien plus élevé que celui du déploiement initial.

4.3 Modularité

Au fur et à mesure qu'augmentent l'emploi d'un système d'infrastructure à clés publiques dans une organisation et la confiance qui lui est accordée, il devient essentiel que le système puisse évoluer en même temps que cette augmentation. Il se peut qu'à ses débuts, un système d'infrastructure à clés publiques ne prenne en charge qu'un nombre restreint d'applications. Ce système doit toutefois être suffisamment polyvalent pour prendre en charge d'autres applications lorsqu'elles seront utilisées.

Les organisations doivent aussi avoir la possibilité d'étendre leur infrastructure à clés publiques en ajoutant de nouveaux composants (autorité de certification et autorité d'enregistrement) pour accepter un nombre croissant de certificats en fonction de l'évolution du système. En outre, divers types de certificats et mécanismes d'enregistrement peuvent s'avérer nécessaires si le système d'infrastructure à clés publiques s'accroît et inclut de nouveaux services.

4.4 Interopérabilité

Tous les composants d'une infrastructure à clés publiques se doivent d'être interopérables car il y a très peu de chances qu'ils proviennent tous d'un même et unique fournisseur. L'infrastructure à clés publiques doit utiliser des interfaces ouvertes et standard, comme LDAP[46] et X.500, pour garantir son interopérabilité avec tous les serveurs d'annuaires conformes à ces normes.

De plus, la technologie d'infrastructure à clés publiques n'en est toujours qu'à ses débuts et il est difficile de prédire avec une quelconque certitude quelles seront les utilisations et les exigences futures de ces systèmes. Les normes dans ce domaine sont toujours en cours d'évolution, voire parfois inexistantes.

Il est donc indispensable de disposer d'un système d'infrastructure à clés publiques totalement ouvert et conçu en conformité avec les normes commerciales les plus répandues et les plus avancées afin d'évoluer en même temps que ces normes.

4.5 Sécurité des autorités de certification et d'enregistrement

Les autorités de certification et d'enregistrement constituent le cœur de tout système d'infrastructure à clés publiques. Leur sécurité a une importance primordiale, car la violation de celle-ci pourrait mettre en péril l'ensemble de l'infrastructure.

---

[46] Lightweight Directory Access Protocol

L'infrastructure à clés publiques doit notamment offrir les garanties suivantes :

- La clé privée de l'autorité de certification doit être conservée dans un module de sécurité résistant à toute tentative d'intrusion. Des dispositions doivent également être prises pour prévoir des copies de sauvegarde en cas d'incident grave.

- L'accès à l'autorité de certification et à l'autorité d'enregistrement doit faire l'objet d'un contrôle très strict, par exemple à l'aide de cartes à puce permettant d'identifier les utilisateurs de manière très fiable.

- Il doit être possible de configurer le processus de gestion des certificats de manière à ce que plusieurs opérateurs soient requis pour autoriser les demandes de certification.

- Toutes les demandes de certificats doivent être signées numériquement par une authentification cryptographique forte, afin de détecter et prévenir toute tentative de piratage visant à générer de faux certificats. Tous les évènements importants sur les systèmes des autorités de certification et d'enregistrement doivent être mentionnés dans un journal d'audit sûr aux entrées horodatées et signées pour en interdire la falsification.

- L'autorité de certification doit être agréée et vérifiée par un organisme indépendant. Elle doit par exemple, au minimum, être conforme aux normes ITSEC[47] de niveau E2, mais de préférence de niveau E3. Les normes ITSEC sont reconnues mondialement dans le domaine de la mesure de produits de sécurité. L'évaluation E3 représente le niveau le plus élevé de sécurité commerciale demandé à l'heure actuelle.

4.6 Support des politiques de sécurité d'une organisation

Le système d'infrastructure à clés publiques devient un élément central des infrastructures de sécurité des organisations, et n'importe quelle autorité de certification doit être à même de refléter et de mettre en œuvre la politique de sécurité de l'organisation.

Un système d'infrastructure à clés publiques basé sur des politiques est donc primordial pour garantir que le processus de gestion des certificats traduit fidèlement les rôles des opérateurs des autorités de certification et d'enregistrement et des utilisateurs de certificats. Par exemple, l'opérateur de l'autorité de certification peut décider de déléguer la tâche de révocation des certificats utilisateurs finaux aux opérateurs de l'autorité d'enregistrement tout en se réservant les droits de révocation des certificats de ces derniers.

[47] Information Technology Security Evaluation Criteria

Chapitre 5 : Application de ces critères à des vendeurs de PKI

Pour illustrer les différents critères d'évaluation abordés au chapitre précédent, ceux-ci vont être appliqués à deux fournisseurs d'infrastructure à clés publiques : Baltimore UniCERT 3.5 et Microsoft Windows 2000 PKI. La source bibliographique utilisée est : *[ZDNet00]*.

5.1 Baltimore : UniCERT 3.5[48]

Baltimore Technologies est spécialisé dans le développement et la commercialisation d'une famille complète de produits et services servant à sécuriser les activités s'effectuant via des réseaux d'ordinateurs, que ce soit des réseaux internes ou externes comme Internet. La gamme de produits comprend un système complet d'infrastructure à clés publiques, des kits d'outils de développement cryptographiques, des applications sécurisées et des composants matériels de cryptographie.

Site Internet : http://www.baltimore.com

5.1.1 Description du produit

UniCERT est l'un des principaux systèmes d'autorité de certification. Il est utilisé dans les systèmes d'infrastructure à clés publiques pour fournir une sécurité performante à une large variété de systèmes de sécurité d'entreprises et de commerce électronique. En utilisant des certificats électroniques, il rend possibles des services tels que le courrier électronique sécurisé, les achats sur Internet, les services bancaires via le Web, le commerce en ligne et les réseaux privés virtuels.

UniCERT est un système fondé sur des politiques. Son « Security Policy Editor » et son contrôle centralisé permettent à toute organisation de définir des politiques de sécurité pour son infrastructure à clés publiques. Il consiste en un système d'autorité de certification hautement sécurisé qui emploie un matériel interdisant toute manipulation non autorisée, des modules d'autorité d'enregistrement et des passerelles assurant une intégration transparente avec d'autres systèmes de sécurité. La plate-forme UniCERT comprend des composants additionnels distincts qui peuvent être déployés et mis à jour séparément.

UniCERT est composé de différents éléments complémentaires :

- *« PKI Editor »* : permet aux gestionnaires de la sécurité de dessiner les composants[49] de l'infrastructure à clés publiques au moyen d'une interface graphique très intuitive. Il permet également d'avoir une vue d'ensemble de l'infrastructure mise en place.
- *« Certification Authority (CA) »*
- *« Certification Authority Operator (CAO) »* : définit les différentes politiques de sécurité pour l'autorité de certification. A l'aide du « Security Policy Editor », ces opérateurs

[48] Sources bibliographiques : *[BtInt00], [BtUn01], [BtUPO00], [MIEL99]*

[49] Autorités de certification, autorités d'enregistrement, opérateurs, serveurs d'archivage des clés…

peuvent contrôler le processus d'enregistrement de certificats en définissant des politiques appropriées à leurs usages ultérieurs.

- *« Registration Authority (RA) »*
- *« Registration Authority Operator (RAO) »* : met en application les politiques définies au niveau du CAO pour l'enregistrement des certificats. Le RAO peut être configuré pour effectuer seulement des requêtes et des opérations spécifiques (gérer la base de données des certificats, suspendre ou révoquer des certificats ...).
- *« Advanced Registration Module (ARM) »* : permet de générer automatiquement des certificats pour une quantité importante de sujets en prenant les informations nécessaires dans des bases de données ou dans des répertoires disponibles (ex : certificats pour tous les employés d'une société).
- *« Archive Server »* : archive de manière sécurisée les clés privées de chiffrement des utilisateurs afin de permettre de retrouver la clé privée, par exemple, en cas d'oubli du mot de passe associé à celle-ci.

Ces composants communiquent entre eux à l'aide d'un système de transactions de bases de données Oracle et utilisent des connexions TCP/IP (PKIX[50]) sécurisées. Chaque composant peut être installé sur une plate-forme matérielle distincte, ce qui permet de réduire les goulots d'étranglement tout en assurant la distribution sûre, dans toute l'organisation, de la charge qu'impose l'infrastructure à clés publiques. UniCERT est protégé au moyen d'un contrôle des accès par carte à mémoire, d'un système de messagerie authentifiée et de modules matériels de sécurité.

5.1.2 Critères

1. Facilité d'utilisation

UniCERT est contrôlé au moyen d'interfaces intuitives et communes à toute l'application. Des messages d'information ou d'indication d'une certaine marche à suivre peuvent également être inclus pour informer et guider les opérateurs. La période de formation de ceux-ci sera donc très réduite.

La configuration de l'infrastructure s'effectue au moyen des interfaces graphiques du « PKI Editor » (pour son design) et du « Security Policy Editor » (pour les politiques des certificats). Il est donc possible de configurer facilement le système ainsi que de vérifier rapidement tous les détails de la configuration. Les politiques créées avec le « Security Policy Editor » peuvent être publiées uniquement où elles seront utilisées. Cela élimine donc la charge associée à la gestion de politiques non usitées ainsi que le risque d'erreur dans le processus complexe de configuration de l'infrastructure.

La gestion et le contrôle de l'infrastructure sont grandement facilités par les outils fournis. En effet, des rapports et des journaux d'évènements sont disponibles pour vérifier le bon fonctionnement. Ces rapports reprennent la gestion de tous les jours des certificats (création, suspension et révocation) grâce aux informations stockées dans une base de données. De leur côté, les journaux d'évènements reprennent les détails de toutes les actions effectuées par l'autorité de certification et d'enregistrement. Chaque entrée dans ces journaux est signée

[50] Public Key Infrastructure X.509

numériquement par l'entité qui est à l'origine de l'information et cette signature est vérifiable au moyen d'interfaces graphiques. La gestion de la base de données de l'infrastructure s'effectue par l'intermédiaire d'outils fournis par Oracle, parmi lesquels on retrouve un outil de sauvegarde de la base de données, un outil indispensable pour un élément si précieux et si critique.

2. Flexibilité

UniCERT est un système d'infrastructure à clés publiques très flexible, que ce soit du point de vue de l'enregistrement, de la distribution ou de la révocation des certificats.

En ce qui concerne l'enregistrement des certificats, UniCERT permet d'adapter le processus d'enregistrement et l'usage du certificat selon les besoins grâce au « Security Policy Editor ». Les paramètres suivants peuvent y être définis :

- La manière dont le processus d'enregistrement doit être fait, soit face à face (le sujet doit se présenter en personne chez le responsable de la sécurité), soit à distance (via un navigateur Internet, un courrier électronique ou un réseau privé virtuel (VPN)).
- Les informations devant être vérifiées ou enregistrées.
- Le nombre de clés qui doivent être générées ainsi que l'endroit où elles doivent l'être.
- Le format utilisé pour le certificat.
- Le nombre de responsables nécessaires pour l'émission du certificat.
- L'algorithme cryptographique utilisé ainsi que la longueur minimale de la paire de clés.

La fonction principale que doit remplir une infrastructure à clés publiques de manière flexible, c'est la distribution de certificats. Il en existe 3 types :

- **La distribution du certificat émis vers le demandeur** : le format du certificat et la méthode de distribution doivent correspondre aux attentes du demandeur. C'est pourquoi UniCERT propose une large variété de formats ainsi que des mécanismes de distribution appropriés. Si la demande se déroule face à face, le certificat peut être émis en software ou bien sur un matériel cryptographique. Par contre, si le demandeur est à distance, le certificat est acheminé de la même façon que l'introduction de la demande.
- **La publication du certificat de l'autorité de certification** : ce certificat doit être accessible par tous ceux qui utilisent l'infrastructure car il est à la base de la confiance dans tout le système. UniCERT propose également une large variété de formats différents dont les formats PKCS#7 et PKCS#12[51]. De plus, il peut être publié dans un répertoire s'il y en a un qui est accessible.
- **La publication des certificats dans un répertoire** : la publication de tous les certificats dans un répertoire est indispensable. UniCERT permet de publier les certificats ainsi que les listes des certificats révoqués dans des répertoires compatibles DAP[52], LDAP[53] ou X.500. Le principal avantage d'un répertoire, c'est la disponibilité des certificats émis pour le chiffrement des messages ainsi que pour la vérification des signatures numériques.

---

[51] Public Key Cryptographic Standards

[52] Directory Access Protocol

[53] Lightweight Directory Access Protocol

La révocation des certificats doit également être flexible. C'est pour cette raison que UniCERT peut adapter les méthodes selon les besoins :

- Le nombre d'autorisations nécessaires.
- La publication de la liste de révocation dans un répertoire et/ou chez un répondeur OCSP[54].
- La division de cette liste en plusieurs parties si nécessaire.
- La suspension du certificat au lieu de la révocation.
- La possibilité d'exporter la liste de révocation.

3. Modularité

UniCERT a été conçu pour répondre aux besoins de toutes les organisations, des petites configurations limitées à un ordinateur jusqu'aux infrastructures répandues dans toute l'organisation. Les caractéristiques principales sont les suivantes :

- Une conception modulaire où chaque élément peut être placé sur un système différent, diminuant ainsi la surcharge de travail du système ainsi que les goulots d'étranglement.
- Des communications sécurisées entre ces différents éléments. Ils peuvent donc utiliser les réseaux publics pour véhiculer l'information.
- Le nombre d'opérateurs pour les autorités d'enregistrement (RAO), qui est limité par le nombre maximal de clients pouvant être connectés à la base de données Oracle.
- La possibilité de créer une hiérarchie d'autorités de certification.
- Un nombre quasi illimité de politiques pour les certificats.

Vu le nombre important de composants possibles, il n'y a pas de limite théorique pour le nombre de certificats pouvant être gérés. Ce nombre dépend uniquement du design de l'infrastructure à clés publiques ainsi que des matériaux cryptographiques utilisés.

De ce fait, l'infrastructure peut continuer à s'étendre au même rythme que la croissance de l'organisation.

4. Interopérabilité

UniCERT apporte une grande ouverture en ce qui concerne les applications utilisant la technologie à clés publiques, les répertoires ainsi que les médias cryptographiques. Baltimore Technologies a adopté une approche en quatre points dans le domaine de l'ouverture commerciale :

- L'implémentation de tous les standards industriels pertinents.
- L'implémentation de tous les protocoles spécifiques de certaines compagnies (ex : le protocole SCEP[55] de Cisco).
- Le support d'applications commerciales dominantes.
- La mise à disposition d'une interface ouverte et étendue aux produits d'une tierce partie.

---

[54] Online Certificate Status Protocol

[55] Simple Certificate Enrollment Protocol

Parmi les standards supportés, on retrouve :

- Les algorithmes cryptographiques : RSA, DSA, SHA-1, MD5 ...
- L'intégration avec différents répertoires X.500 et LDAP.
- Les certificats électroniques X.509 v3.
- Les standards PKCS (1, 7, 10, 11, 12).

Grâce à la compatibilité avec tous ces standards, les applications tirant parti de l'infrastructure à clés publiques pourront évoluer avec la technologie sans subir de modification.

5. Sécurité des autorités de certification et d'enregistrement

L'exigence principale d'une infrastructure à clés publiques est la sécurité de l'autorité de certification. En effet, si cette autorité est compromise, c'est l'infrastructure dans son ensemble qui est compromise. On comprend dès lors aisément l'importance accordée à ce sujet. Les préoccupations principales pour une autorité de certification sont les suivantes :

- La sécurité des clés privées de l'autorité de certification.
- La prévention des attaques de personnes extérieures visant à générer de faux certificats.
- La tolérance aux pannes (manque d'électricité, coupure de communications, mauvais comportement d'un certain module ...).
- La crédibilité des opérateurs des autorités de certification et d'enregistrement.

Pour satisfaire toutes ces exigences, UniCERT propose :

- La compatibilité avec une large variété de modules matériels de sécurité (HSM).
- La possibilité d'utiliser des cartes à puce à tous les endroits de l'infrastructure pour le contrôle d'accès et l'authentification des messages.
- L'utilisation de PKIX pour la communication entre les différents modules.
- Le chiffrement des clés privées des autorités et des opérateurs.
- Une base de données Oracle avec les outils de sauvegarde et de rétablissement. Cette base de données est utilisée pour stocker les informations suivantes :
  - Les demandes et émissions de certificats et de listes de révocation.
  - Les messages entre les différentes autorités.
  - Les journaux d'évènements.
  - Les détails des politiques d'enregistrement de certificats.
  - Les informations sur le sujet qui ne sont pas incluses dans le certificat.

  Chaque entrée est signée avec la clé privée de l'opérateur à l'origine de celle-ci, ce qui permet son authentification. De plus, chaque demande et chaque message possèdent un numéro d'identification, éliminant ainsi toute confusion entre les messages.
- Une méthode de sauvegarde des clés privées de chiffrement dans le module « Archive Server ».
- La certification ITSEC[56] E3 qui a été délivrée à UniCERT.

[56] Information Technology Security Evaluation Criteria

6. Support des politiques

Une politique définit les procédures à suivre pour permettre l'accès aux ressources et aux informations de l'organisation tout en empêchant les utilisateurs non autorisés d'accéder à ces mêmes ressources. Dans UniCERT, les politiques de sécurité définissent les contraintes et les profils utilisés pour les certificats ainsi que pour leurs demandes. Ces politiques sont définies au niveau des opérateurs de l'autorité de certification (CAO) et autorisent l'émission de certificats pour différents usages.

La création d'une politique est une tâche complexe qui est grandement simplifiée avec l'interface graphique du « Security Policy Editor ». La démarche de création de politiques d'émission de certificats personnalisées comporte quatre étapes :

1. La définition des éléments repris dans le « distinguished name », qui identifie de manière unique un sujet, et qui apparaîtra dans les certificats émis en suivant cette politique.
2. La définition des extensions du certificat ; celles-ci déterminent l'usage que le sujet pourra faire de son certificat.
3. Le choix des informations complémentaires qui devront être apportées pour l'émission du certificat. Celles-ci ne seront pas publiées dans le certificat.
4. Le choix des contraintes additionnelles qui devront être satisfaites pour permettre l'émission du certificat. Parmi ces contraintes, on retrouve :
    - la longueur acceptable pour la paire de clés,
    - les algorithmes à clés publiques acceptables,
    - les algorithmes de hashing acceptables,
    - la période de validité des certificats,
    - le nombre d'opérateurs requis pour l'émission du certificat.

Afin d'aider les opérateurs à créer et à gérer les différentes politiques de certificats, la documentation du produit relative au module des opérateurs de l'autorité de certification fournit des explications détaillées sur les différents attributs possibles d'une politique.

5.1.3 Avantages et inconvénients de UniCERT

Avantages

- La configuration de l'autorité de certification, qui est simple et très pointue car beaucoup d'options différentes peuvent être choisies.
- La maturité du produit, qui a été amélioré et fiabilisé grâce à l'expérience acquise au cours des années (ce produit existe depuis pratiquement 5 ans).
- L'interface graphique, qui offre une vision globale de l'infrastructure à clés publiques et permet ainsi une meilleure gestion de celle-ci.
- L'ouverture vers les plates-formes non-Microsoft ainsi que vers beaucoup d'applications grâce à la compatibilité avec de nombreux standards.
- L'adaptation des politiques d'émission de certificats pour des besoins spécifiques.
- La sécurité de l'autorité de certification, qui est garantie avec le chiffrement des clés privées et l'utilisation de modules matériels de sécurité (HSM). Chaque module ne peut

être démarré qu'après la fourniture d'un mot de passe pour l'accès aux informations du module et d'un autre mot de passe pour la connexion à la base de données Oracle.

- Les nombreux outils offrant des fonctions avancées de sécurité et de gestion, comme les journaux reprenant tous les évènements du système.
- L'indépendance de la base de données par rapport au produit. De plus, UniCERT peut retirer des avantages de l'utilisation d'Oracle vu la sécurité, la robustesse et la fiabilité de ses bases de données.

Inconvénients

- La nécessité d'envisager les coûts supplémentaires liés à l'acquisition de licences.
- L'intégration avec le système d'exploitation Microsoft Windows 2000 qui n'est pas encore totale vu l'adaptation récente de UniCERT à cet environnement, entre autres les éléments suivants :
  - La publication des certificats dans l'Active Directory de Microsoft Windows 2000 lorsque l'architecture comprend plusieurs domaines distincts.
  - L'indisponibilité de certaines fonctionnalités comme l'enregistrement et le renouvellement automatique de certains certificats (par exemple : les certificats pour le chiffrement des données EFS et pour les contrôleurs de domaines).
  - L'indisponibilité de certaines fonctionnalités à moins qu'une autorité de certification de Microsoft soit présente dans le système.

5.2 Microsoft Windows 2000 PKI[57]

Microsoft a été créée au milieu des années 70. Cette société est spécialisée dans la création de systèmes d'exploitation ainsi que dans les applications bureautiques. L'implantation d'une infrastructure à l'intérieur de ces systèmes est assez récente. En effet, c'est à partir du système d'exploitation Windows NT4 que cette technologie est apparue sous une forme très simplifiée. Son successeur, Microsoft Windows 2000, intègre une version plus récente et plus développée des infrastructures à clés publiques.

Site Internet : http://www.microsoft.com

5.2.1 Description du produit

Dans la version serveur de son système d'exploitation Windows 2000, Microsoft a intégré la technologie d'infrastructure à clés publiques. Les principaux outils nécessaires à l'implantation et à la gestion de cette infrastructure s'y retrouvent. L'avantage indéniable de ce système est que le coût de cette technologie est compris dans la licence d'utilisation du système d'exploitation alors que les systèmes d'autres revendeurs se vendent à des prix non-négligeables. L'infrastructure à clés publiques de Windows 2000 est principalement basée sur les standards existants, compte tenu toutefois des interprétations habituelles de ces standards qui constituent l'une des caractéristiques des produits Microsoft.

[57] Sources bibliographiques : *[MsSDG00], [MsCry&Pki], [MsW2kCs], [NetM00]*

Cette infrastructure est construite sur les bases de l'architecture du système d'exploitation Windows 2000. Parmi celles-ci, on retrouve :

- L'API cryptographique de Microsoft « *CryptoAPI 2.0* », qui apporte les services cryptographiques requis tout en supportant la majorité des algorithmes connus. De plus, des services de chiffrement (CSP[58]) installables peuvent être ajoutés afin de supporter d'autres algorithmes.
- Le « Certificate Server » de Microsoft qui constitue l'autorité de certification de l'infrastructure. Il était déjà présent dans la version précédente du système d'exploitation mais est implémenté ici dans une nouvelle version.
- Le répertoire compatible LDAP « *Active Directory* », qui est utilisé pour le stockage des clés, des certificats et des listes de révocation. Il est donc inutile de disposer d'une base de données et d'un répertoire supplémentaires.

La gestion de l'infrastructure à clés publiques s'effectue au moyen de la console de Microsoft « *MMC*[59] » où plusieurs écrans sont disponibles. Premièrement, un écran « *Certificate Manager* » qui propose une interface aux sujets pour la gestion locale des certificats personnels et pour la demande de certificats supplémentaires. Deuxièmement, l'écran « *Certificate Services* » représentant l'autorité de certification et permettant aux opérateurs d'administrer les certificats (émission et révocation de ceux-ci). Enfin, l'écran « *Group Policy* » qui sert à définir les différentes politiques de sécurité et les droit d'accès relatifs à l'autorité de certification.

Il existe également une autre méthode pour envoyer une requête d'émission d'un certificat via un navigateur Internet à l'adresse http://adresseAutoritédeCertification/certsrv. La version la plus récente de la liste de révocation ainsi que le certificat de l'autorité de certification sont aussi disponibles à la même adresse.

On constate donc que la plupart des éléments nécessaires à l'implantation d'une infrastructure à clés publiques sont présents dans le système proposé par Microsoft. Malgré cela, il s'agit toujours d'une solution très récente et pas encore vraiment testée, et il y a peu de documentation disponible sur la manière dont elle doit être implémentée, mis à part sur le site Internet de Microsoft.

5.2.2 Critères

1. Facilité d'utilisation

L'autorité de certification est contrôlée via l'interface graphique intuitive de la console Microsoft « *MMC* ».

La configuration principale de l'autorité s'effectue lors de l'installation du logiciel Microsoft Windows 2000 Serveur. Elle est aisée vu le nombre restreint d'options sélectionnables. Une configuration plus poussée pourra toutefois s'effectuer ultérieurement via la console Microsoft (quels certificats pourront être émis, qui pourra les demander, l'intervalle de temps entre les différentes listes de révocation, etc.).

---

[58] Cryptographic Service Provider

[59] Microsoft Management Console

La gestion de l'autorité de certification s'effectue facilement via la même console. Cependant, les outils sont assez limités et pratiquement aucun journal d'évènements n 'est disponible, mis à part l'outil « *Event Viewer* » propre au système d'exploitation. Le contrôle des différentes opérations effectuées au niveau de l'autorité sera donc assez difficile.

Pour les sauvegardes de la base de données de certificats, un outil existe dans l'écran « Certificate Services » de la console, mais cette base de données étant dans un format propriétaire, la sauvegarde l'est également. De plus, ce système étant relativement nouveau, sa fiabilité devra encore être prouvée.

2. Flexibilité

Le système d'infrastructure à clés publiques de Microsoft est flexible mais comporte tout de même quelques limitations.

En ce qui concerne l'enregistrement des certificats, il existe deux méthodes : soit via la console Microsoft, soit via un navigateur Internet à l'adresse de l'autorité de certification. Cet enregistrement peut être effectué par le sujet ou bien plus probablement par un responsable disposant des droits nécessaires pour faire une requête. Ce responsable est appelé « *Enrollment Agent* ».

Pour chaque autorité de certification, il est possible de définir quels types de certificats pourront être émis mais le choix est limité à une liste prédéfinie reprenant 16 types de certificats différents. Ceux-ci seront définis plus en détail au point 6 « Support des politiques ». Il est également possible de définir les utilisateurs qui disposeront des droits nécessaires pour demander chaque certificat via des politiques de sécurité internes à Microsoft Windows 2000 (dans l'écran « *Group Policy* » de la console Microsoft).

Comme cela a été vu pour UniCERT, la distribution des certificats doit également pouvoir se dérouler de manière flexible pour les 3 types de distribution :

- **La distribution du certificat émis vers le demandeur** : le format du certificat peut être choisi en fonction du service de chiffrement (CSP) sélectionné dans la demande du certificat. Ce dernier est ensuite renvoyé au demandeur de la même façon que l'introduction de la demande (la console Microsoft « *MMC* » ou le navigateur Internet).
- **La publication du certificat de l'autorité de certification** : il est possible de télécharger ce certificat de n'importe où, en allant au moyen d'un navigateur sur la page de l'autorité de certification. Ce certificat est également publié automatiquement dans l'Active Directory. De ce fait, les utilisateurs travaillant sous Windows 2000 y ont directement accès sans devoir aller le chercher.
- **La publication des certificats dans un répertoire** : les certificats et les listes de révocation sont publiés dans l'Active Directory. Les applications devant vérifier une signature ou devant chiffrer un message pourront donc facilement retrouver le certificat dont ils ont besoin. Cependant, il est à regretter que l'autorité de certification ne puisse publier les certificats dans un autre répertoire compatible LDAP.

La fonction de révocation des certificats est très limitée. En effet, le seul moyen de révoquer un certificat, c'est de se trouver au niveau de l'autorité de certification. De plus, il est impossible de suspendre un certificat, de diviser la liste de révocation en plus petits morceaux ou bien de communiquer cette liste à un répondeur OCSP[60]. Malgré cela, les fonctions essentielles sont remplies avec la publication automatique de la liste dans l'Active Directory, la distribution automatique de cette liste sur tous les ordinateurs des sujets et son exportation possible dans un fichier.

3. Modularité

Les autorités de certification peuvent s'adapter aux besoins de l'organisation car la création d'une hiérarchie d'autorités est possible mais une autorité ne peut pas être répartie sur plusieurs machines. Seul l'Active Directory peut se trouver sur une machine distincte (généralement sur le contrôleur du domaine contenant cette autorité).

Pour répartir la charge, des autorités d'enregistrement peuvent être réparties dans le domaine. En fait, il n'existe pas d'autorité d'enregistrement proprement dite. Il s'agit seulement d'une autorité de certification dont certaines fonctionnalités ont été supprimées, comme la possibilité de signer des certificats.

L'infrastructure pourra donc évoluer en même temps que l'organisation pour autant que l'ensemble du système conserve le système d'exploitation Microsoft Windows 2000.

4. Interopérabilité

L'ouverture de ce système est assez limitée. En effet, elle est restreinte aux applications Microsoft tournant dans un environnement Microsoft Windows 2000. Deux causes principales sont à l'origine de cette faiblesse :

- On a adopté des standards propres au système d'exploitation Windows 2000 et non des standards commerciaux répandus dans de nombreuses applications.
- Si des standards généraux sont adoptés, ils sont étendus ou modifiés de telle sorte qu'ils ne pourront être utilisés que par des applications provenant de Microsoft.

Dans Windows 2000, la certification est basée sur le standard PKCS#10 (la demande de certificat arrive et une réponse PKCS#7 est renvoyée au demandeur). Pour les requêtes provenant des applications non-Microsoft, il n'est pas indiqué très clairement quelle procédure il faut suivre pour importer cette requête et, de plus, il n'est pas certain que ce certificat pourra être inclus dans l'Active Directory.

Certains problèmes d'ouverture peuvent également se poser dans le stockage et l'accès aux clés. En effet, les standards généraux pour l'interopérabilité sont les standards PKCS. Or, Windows 2000 utilise la CryptoAPI pour la gestion matérielle des clés et emploie le standard PC/SC au lieu du standard PKCS#11 pour l'interface avec les cartes à puce. Les certificats émis par Windows 2000 fonctionneront dès lors uniquement pour des applications tournant avec

[60] Online Certificate Status Protocol

implémentation Microsoft de PC/SC et non pour celles qui tournent avec le standard reconnu PKCS#11.

Finalement, quelques problèmes se posent avec l'Active Directory qui est utilisé pour le stockage des clés. Les autres plates-formes ou applications voulant utiliser l'infrastructure à clés publiques de Microsoft devront obligatoirement avoir accès à l'Active Directory pour tirer profit de cette technologie. Celle-ci étant complètement compatible LDAP, cela devrait être possible. Mais ce produit Microsoft contient des éléments propriétaires qui ont été ajoutés, ainsi que d'autres éléments standard qui ont été changés. L'accès risque donc d'être difficile pour les applications non-Microsoft.

5. Sécurité des autorités de certification et d'enregistrement

La sécurité de l'autorité de certification est l'exigence la plus importante dans toute l'infrastructure pour éviter qu'elle soit compromise. Dans le système de Microsoft, la sécurité n'est pas optimale. En effet, certaines lacunes apparaissent :

- La compatibilité avec des modules matériels de sécurité (HSM) n'est pas assurée pour la protection de la clé privée de l'autorité de certification.
- L'autorité de certification démarre en même temps que le système d'exploitation sans qu'on doive introduire de mot de passe ou prouver son identité.
- Les journaux d'évènements sont très rares et incomplets, ce qui empêche un contrôle pointu des opérations effectuées avec l'autorité.
- Les fonctions d'opérateurs de l'autorité de certification sont difficilement dissociables des fonctions d'administrateurs systèmes. L'accès est donc possible à des personnes n'ayant rien à voir avec l'autorité de certification.

Afin de permettre une restauration du système après une panne, un outil de sauvegarde des clés de l'autorité de certification et de la base de données des certificats est disponible. De plus, il existe un mécanisme d'archivage des clés privées des utilisateurs mais ce mécanisme n'est pas très satisfaisant, chaque utilisateur devant exporter lui-même sa clé privée dans un format PKCS#12. Cette procédure manuelle est assez lourde et même parfois impossible car certains services de chiffrement (CSP) n'autorisent pas l'exportation des clés privées en dehors du matériel (exemple : une carte à puce).

6. Support des politiques

Les politiques d'émission de certificats sont limitées à 16 possibilités prédéfinies et aucune adaptation de celles-ci n'est possible. Malgré cela, les utilisations les plus fréquentes s'y retrouvent :

- Domain controller : authentification des clients et des serveurs
- Encrypting File System : chiffrement des données sur un disque
- Enrollment Agent : agent traitant les demandes de certificats
- SmartCard Logon : authentification de l'utilisateur
- SmartCard User : authentification de l'utilisateur, signature et chiffrement du courrier électronique

- User : authentification de l'utilisateur, signature et chiffrement du courrier électronique et chiffrement des données sur disque

Pour plus de détails sur ces politiques, reportez-vous au document *[MsCh12]* dans le tableau 12.2.

5.2.3 Avantages et inconvénients de Microsoft Windows 2000 PKI

Avantages

- Une parfaire intégration avec le système d'exploitation Windows 2000.
- La publication des certificats et des listes de révocation, qui s'effectue sans aucun problème dans l'Active Directory.
- Le coût dérisoire de l'infrastructure à clés publiques, qui est compris dans la licence d'utilisation du système d'exploitation dans sa version serveur.
- L'enregistrement et le renouvellement automatiques de certains certificats (le certificat pour le contrôleur de domaine, les communications sécurisées IPSEC et le chiffrement des données EFS).

Inconvénients

- L'ouverture inexistante vers les applications non-Microsoft et les autres systèmes d'exploitation.
- L'absence de journaux d'évènements et d'outils de gestion, qui diminue le contrôle possible sur l'autorité de certification.
- L'adaptation impossible pour les politiques d'émission de certificats.
- Les composants propriétaires (base de données et répertoire), qui réduisent l'interopérabilité avec les autres applications.
- La sécurité de l'autorité de certification, qui n'est pas totale (incompatibilité avec les modules matériels de sécurité (HSM)).
- La durée de validité des certificats émis par l'autorité de certification, qui est identique à la durée de vie de l'autorité de certification. Cette option ne peut être changée qu'après le changement de la valeur d'une clé dans la base de registre de Microsoft Windows 2000.
- La jeunesse du produit : celui-ci évoluera dans le futur avec les nouvelles versions des systèmes d'exploitation (dont Windows XP).

Chapitre 6 : Comment tester réellement une infrastructure à clés publiques ?

Lors de l'implantation d'une infrastructure à clés publiques, comme pour tout système important, il est indispensable de définir en détail des tests d'acceptation qui devront être effectués sur le système pour vérifier la satisfaction des exigences requises. C'est encore plus primordial dans les systèmes traitant de la sécurité. Plusieurs méthodes existent pour définir des plans de tests, dont la méthode « *Test Requirement Hierarchy* »

6.1 Méthode « *Test Requirement Hierarchy* »

Cette méthode consiste en un arbre hiérarchique de besoins dont la racine représente le besoin principal du système, c'est-à-dire l'objectif à atteindre. Ce besoin principal se décompose en plusieurs besoins inférieurs devant être satisfaits pour que le besoin principal soit également satisfait. Cette décomposition s'effectue jusqu'à la découverte des besoins élémentaires. Le but des tests sera donc de satisfaire tous les besoins élémentaires afin de valider le besoin supérieur. Lorsque la racine est atteinte et que tous les besoins inférieurs sont satisfaits, l'objectif principal du système est vérifié.

Lorsque l'arbre hiérarchique des besoins est défini, les tests élémentaires doivent être classés selon leur priorité car la période disponible pour effectuer ces tests est souvent trop courte pour permettre de tout tester. Les responsables du projet procèdent alors à une classification en donnant un certain poids à chacun des tests pour la complexité du test et pour la priorité de la fonctionnalité. La graduation s'échelonne de l'indispensable au pas très important, et dépendra fortement du système à tester et de l'organisation concernée. Les tests ayant reçu les notes les plus élevées pour les deux catégories seront effectués en premier lieu.

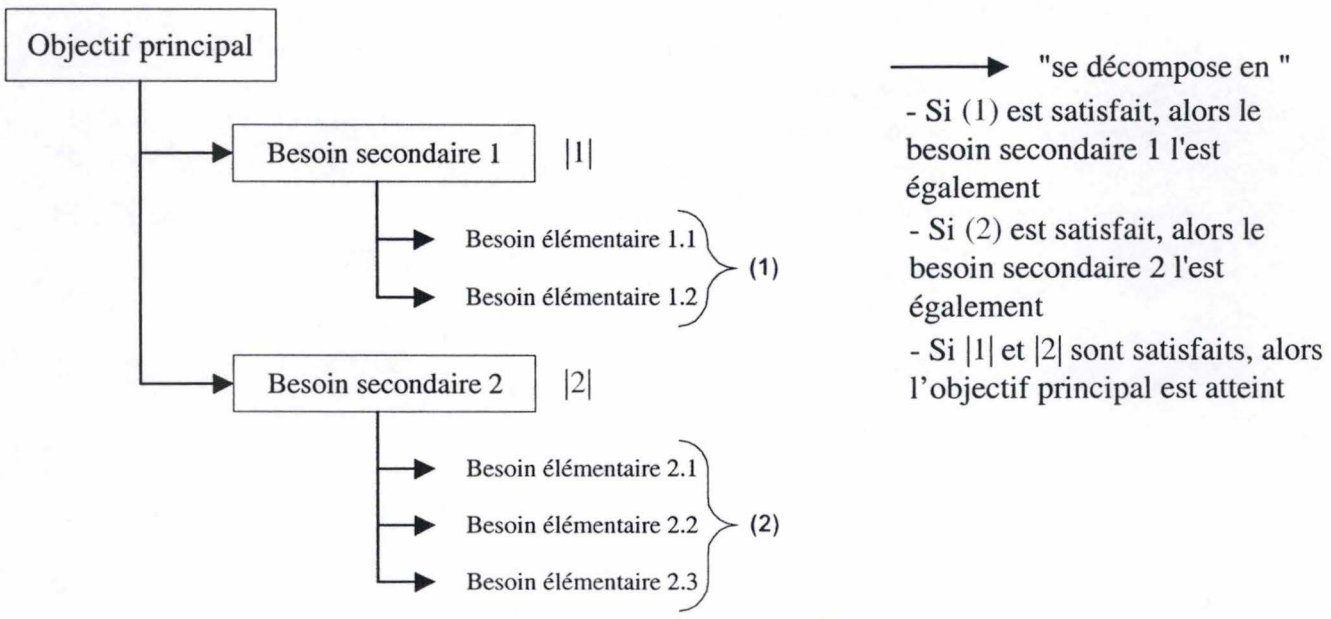

Figure 17 : Test Requirement Hierarchy

6.2 Application de la méthode aux infrastructures à clés publiques

Pour illustrer cette méthode, voici l'arbre hiérarchique des besoins applicables aux tests pour une infrastructure à clés publiques. Les détails exacts de ces tests et leur classement par ordre de priorité ont été omis car ils dépendent du contexte et de l'organisation dans laquelle le système doit s'implanter.

Objectif principal : une meilleure protection des informations et des transactions.

1. L'infrastructure à clés publiques (PKI) doit gérer les certificats électroniques
   - 1.1. La PKI doit être capable d'enregistrer une demande de certificat électronique de chiffrement
     - 1.1.1. Le sujet doit préparer les informations d'enregistrement (identification, autorisation, authentification)
       - 1.1.1.1. Les données d'enregistrement doivent être collectées auprès des organismes responsables
       - 1.1.1.2. Les données doivent être transmises à la PKI
     - 1.1.2. La PKI doit enregistrer l'identification du sujet demandant un certificat
       - 1.1.2.1. La PKI doit obtenir l'identité du sujet
       - 1.1.2.2. La PKI doit contrôler l'identité du sujet
       - 1.1.2.3. La PKI doit stocker l'identité du sujet dans le certificat
     - 1.1.3. La PKI doit être capable d'enregistrer l'autorisation du sujet demandant le certificat
       - 1.1.3.1. La PKI doit obtenir l'autorisation du sujet
       - 1.1.3.2. La PKI doit contrôler l'autorisation du sujet
       - 1.1.3.3. La PKI doit stocker l'autorisation du sujet
     - 1.1.4. La PKI doit être capable d'enregistrer l'authentification du sujet demandant le certificat
       - 1.1.4.1. La PKI doit obtenir l'authentification du sujet
       - 1.1.4.2. La PKI doit contrôler l'authentification du sujet
       - 1.1.4.3. La PKI doit stocker l'authentification du sujet
   - 1.2. La PKI doit être capable de générer des paires de clés pour la signature et le chiffrement
   - 1.3. La PKI doit être capable de sauvegarder les clés de chiffrement
   - 1.4. La PKI doit être capable de créer un certificat électronique
   - 1.5. La PKI doit être capable de publier le certificat électronique du sujet
2. Un sujet doit être capable d'utiliser son certificat électronique pour protéger ses informations et ses transactions
   - 2.1. Un sujet doit être capable d'utiliser son certificat électronique pour **effectuer un contrôle d'accès**
     - 2.1.1. Un sujet doit être capable de générer une signature numérique
     - 2.1.2. Un sujet doit être capable de transférer la signature numérique
     - 2.1.3. Un sujet doit être capable de contrôler une signature numérique
       - 2.1.3.1. Un sujet doit pouvoir contrôler la signature avec le certificat électronique associé
       - 2.1.3.2. Un sujet doit pouvoir contrôler le certificat et la chaîne de certification
     - 2.1.4. Un sujet doit être capable de traiter le résultat de la vérification de la signature numérique
       - 2.1.4.1. En cas de succès
       - 2.1.4.2. En cas d'échec à chaque étape de la vérification
   - 2.2. Un sujet doit être capable d'utiliser son certificat électronique pour **garantir la confidentialité des informations et des transactions**
     - 2.2.1. Un sujet doit être capable de chiffrer des informations confidentielles dans un format déchiffrable par toutes les personnes autorisées
       - 2.2.1.1. Un sujet doit pouvoir obtenir tous les certificats des personnes autorisées
       - 2.2.1.2. Un sujet doit pouvoir contrôler la validité des certificats des personnes autorisées
       - 2.2.1.3. Un sujet doit pouvoir chiffrer les informations confidentielles avec chaque clé publique des certificats des personnes autorisées
     - 2.2.2. Les personnes autorisées doivent pouvoir déchiffrer les informations chiffrées par d'autres personnes autorisées
     - 2.2.3. Le système doit être capable de récupérer des messages chiffrés en cas d'urgence
       - 2.2.3.1. La clé de chiffrement avec laquelle l'information a été chiffrée doit être récupérée
       - 2.2.3.2. L'information doit être déchiffrée

2.3. Un sujet doit être capable d'utiliser son certificat électronique pour **garantir l'authenticité des informations** (intégrité et non-répudiation)

2.3.1. Un sujet doit être capable d'utiliser son certificat électronique pour **garantir l'intégrité des informations**

2.3.1.1. Un sujet doit être capable de générer une signature numérique

2.3.1.2. Un sujet doit être capable de transférer la signature numérique

2.3.1.3. Un sujet doit être capable de contrôler une signature numérique

2.3.2. Un sujet doit être capable d'utiliser son certificat électronique pour **garantir la non-répudiation des informations**

2.3.2.1. Un sujet doit être capable de générer une signature numérique

2.3.2.2. Un sujet doit être capable de transférer la signature numérique

2.3.2.3. Un sujet doit être capable de contrôler une signature numérique

2.4. Un sujet doit être capable de révoquer l'utilisation d'un certificat électronique

Conclusion

La technologie des infrastructures à clés publiques n'en est qu'à ses débuts, mais son utilisation devient indispensable pour sécuriser les échanges de plus en plus nombreux sur les réseaux ouverts. Du fait de leur jeunesse, les systèmes d'infrastructure à clés publiques, qui remplissent déjà en grande partie leur rôle, présentent encore certaines lacunes. Cette constatation a été mise en évidence par l'application des critères d'évaluation définis à deux systèmes d'infrastructure à clés publiques existants. Ces derniers se sont révélés bien différents l'un de l'autre, chacun présentant ses avantages et ses inconvénients. Il faudra donc choisir le système le plus approprié après une analyse approfondie des différentes possibilités afin de retirer la solution la mieux adaptée aux besoins des parties concernées.

La confiance que les personnes accordent à une infrastructure à clés publiques repose principalement sur les autorités de certification ainsi que sur leur fonctionnement. Il est donc primordial de consacrer une grande attention à la définition de l'architecture de l'infrastructure et à la rédaction des procédures régissant les opérations qui pourront être effectuées à l'intérieur de cette infrastructure. De plus, des méthodes d'élaboration de plans de test vont permettre aux responsables du système de s'assurer du bon déroulement des différents scénarios possibles.

Enfin, la jeunesse du système d'exploitation Microsoft Windows 2000 ne facilite en rien l'adaptation des systèmes d'infrastructure à clés publiques existants à une telle plate-forme. Néanmoins, du fait de l'expansion constante du domaine de la sécurité des échanges sur les réseaux, les fournisseurs d'infrastructures à clés publiques vont être incités à faire évoluer leurs produits afin de répondre aux exigences prévisibles.

De ce fait les systèmes d'infrastructure à clés publiques sont assurés d'avoir un avenir prometteur.

Bibliographie

[APC95] Bruce Schneier, *Applied Cryptography*, John Wiley and Sons Ltd, 2ème édition, novembre 1995, 758 pages

[BtInt00] Baltimore Technologies, « An Introduction to PKI Based e-security », 2000, http://www.baltimore.com

[BtUPO00] Baltimore Technologies, « Baltimore Unicert – Product Overview », 2000, http://www.baltimore.com

[BtUn01] Baltimore Technologies, « Baltimore UniCERT », janvier 2001, http://www.baltimore.com/unicert/unicert/index.html

[CertPCN] Certplus, « Mieux comprendre la certification numérique », http://www.certplus.com

[CertPCrypt] Certplus, « Mieux comprendre la cryptographie », http://www.certplus.com

[HAC96] Alfred J. Menezes, Paul C. van Oorschot et Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, ISBN 0-8493-8523-7, octobre 1996, 816 pages, 4ème impression (juillet 1999), http://www.carc.math.uwaterloo.ca/hac.

[IETF2527] Network Working Group, « Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework », RFC 2527, mars 1999, http://www.ietf.org

[iPlan00] iPlanet e-commerce solutions, « Introduction to Public Key Infrastructure », 2000, http://www.iplanet.com/developer/docs/articles/security/pki.html

[MIEL99] MIEL e-Security Pvt. Ltd, « Public Key Infrastructure », 1999, http://www.mielesecurity.com/pki/pkimain.htm

[MsCry&Pki] Microsoft, « Cryptography and PKI Basics », *Microsoft White Paper*, Microsoft Press, 2000, http://www.microsoft.com/TechNet/prodtechnol/windows2000serv/deploy/cryptpki.asp

[MsSDG00] Microsoft, « Chapter 12 : Planning your Public Key Infrastructure », *Windows 2000 Server Deployment Guide*, Microsoft Press, janvier 2000, http://www.microsoft.com/TechNet/win2000/dguide/chapt-12.asp

[MsRKit00a] Microsoft, « Chapter 13 : Choosing Security Solutions That Use Public Key Technology », *Windows 2000 Server Ressource Kit*, Microsoft Press, 2000, http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/distsys/part2/dsgch13.asp

[MsRKit00b] Microsoft, « Chapter 14 : Cryptography for Network and Information Security », *Windows 2000 Server Ressource Kit*, Microsoft Press, 2000, http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/distsys/part2/dsgch14.asp

[MsPkiInt] Microsoft, « Public Key Interoperability », *Microsoft White Paper*, Microsoft Press, 2000, http://www.microsoft.com/WINDOWS2000/library/howitworks/security/w2kpkint.asp

[MsSN00] Microsoft, « Secure Networking Using Windows 2000 Distributed Security Services », *Microsoft White Paper*, Microsoft Press, 2000

[MsW2kCs] Microsoft, « Windows 2000 Certificate Services », *Microsoft White Paper*, Microsoft Press, 2000, http://www.microsoft.com/WINDOWS2000/library/technologies/security/windows2000csoverview.asp

[MsW2kPki] Microsoft, « Microsoft Windows 2000 Public Key Infrastructure », *Microsoft White Paper*, Microsoft Press, 2000, http://www.microsoft.com/WINDOWS2000/library/planning/security/pki.asp

[NetM00] Curtis E. Dalton, « Windows 2000 PKI : Contender or Pretender ? », *Network Magazine*, octobre 2000, http://www.networkmagazine.com/article/NMG20001004S0016/3

[RSA00] RSA Laboratories, *Frequently Asked Questions about Today's Cryptography*, RSA Security Inc, mai 2000, 269 pages, version 4.1, http://www.rsa.com.

[SCM0899] « Cover Story : PKI Evolution to Application », *Info Security Magazine*, août 1999, http://www.scmagazine.com

[SCM0800] Illena Armstrong, « Cover Story : PKI : Has It Truly Arrived Yet ? », *Info Security Magazine*, août 2000, http://www.scmagazine.com

[W2kMag00] R. Franklin Smith , « Windows 2000 Security Gains », *Windows 2000 Magazine*, 2000, http://www.windowsntmag.presse.fr/themes/securite/articles/sec0013.htm

[Xcert99] Xcert International Inc., « A practical Guide to Public Key Infrastructure », 1999, http://www.xcert.com

[ZDNet00] Alan Stevens, « PKI Shoot-Out » , *Network Edition of PC Magazine*, novembre 2000, http://www.zdnet.co.uk/pcmag/ne/2000/11/06.html.