Marie-Claire FREUNDLICH-LE THANH
Docteur en Droit et Economie du développement - Avocat

FONCTIONNEMENT DES ORGANISATIONS

Cours n° 5

5. SIGNATURE ELECTRONIQUE ET SECURITE

5.1 Introduction à la notion de signature électronique

Le paradigme de signature électronique (appelé aussi signature numérique) est un procédé permettant de garantir l'authenticité de l'expéditeur (fonction d'authentification), ainsi que de vérifier l'intégrité du message reçu.

La signature électronique assure également une fonction de non-répudiation, c'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message (autrement dit elle empêche l'expéditeur de nier d'avoir expédié le message).

5.2. Définition d'une PKI

On appelle PKI (Public Key Infrastucture, ou en français infrastructure de clé publique (ICP), parfois infrastructure de gestion de clé (IGC)) l'ensemble des solutions techniques basées sur la cryptographie à clés publiques
Les crypto systèmes à clés publiques permettent de s'affranchir de la nécessité d'avoir recours systématiquement à un canal sécurisé pour s'échanger les clés. En revanche, la publication de la clé publique à grande échelle doit se faire en toute confiance pour assurer que :
La clé publique est bien celle de son propriétaire
Le propriétaire de la clé est digne de confiance
La clé est toujours valide
Ainsi, il est nécessaire d'associer au bi-clé (ensemble clé publique/clé privée) un certificat délivré par un tiers de confiance: l'infrastructure de gestion de clés.

5.3. Le tiers de confiance

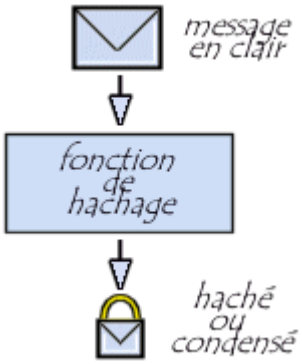
Le tiers de confiance est une entité (appelée communément autorité de certification, abréviation AC, ou en anglais Certification authority, en abrégé CA) chargée d'assurer la véracité des informations contenues dans le certificat de clé publique et de sa validité. Pour ce faire, l'autorité signe le certificat de clé publique avec sa propre clé.

Le rôle de l'infrastructure de clés publiques est de :

- *Enregistrer des demandes*
- *générer les paires de clés (clé privée / clé publique)*
- *garantir la confidentialité de la clé privée*
- *certifier la clé publique*
- *révoquer des clés (en cas de perte par son propriétaire ou de compromission de la clé*

5.4. La fonction de hachage

Une fonction de hachage (parfois appelée fonction de condensation) est une fonction permettant d'obtenir un condensé (appelé aussi haché) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense. La fonction de hachage doit être telle qu'elle associe un et un seul haché à un texte en clair (cela signifie que la moindre modification du document entraîne la modification de son haché). D'autre part, il doit s'agir d'une fonction à sens unique (one-way function) afin qu'il soit impossible de retrouver le message original à partir du condensé.



Ainsi, le haché représente en quelque sorte l'empreinte digitale (en anglais finger print) du document.
Les algorithmes de hachage les plus utilisés actuellement sont :

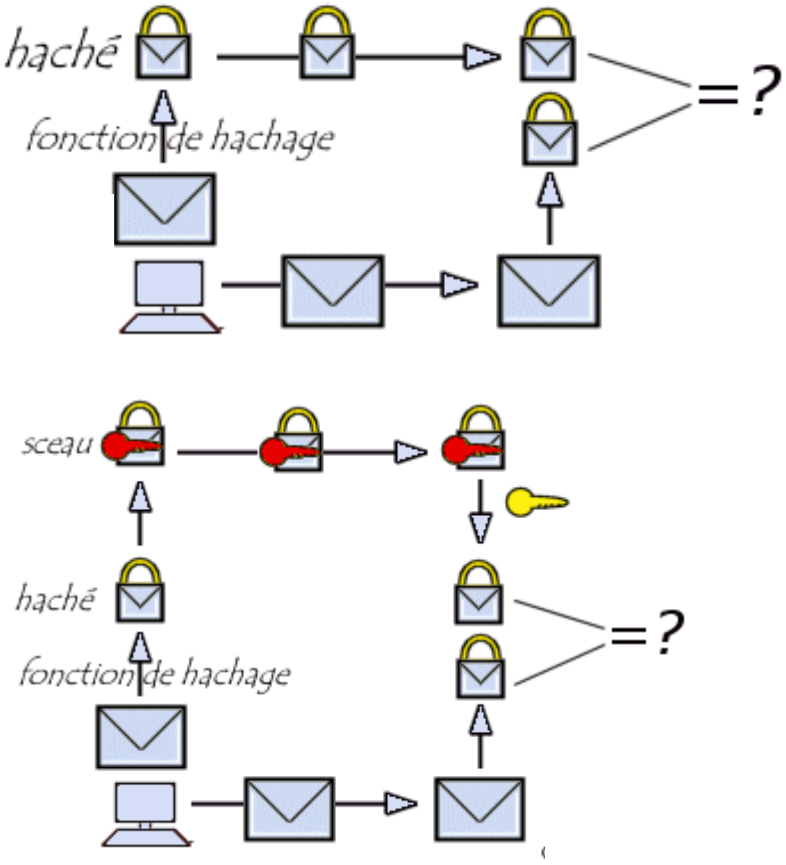
***MD5** (MD signifiant Message Digest), créant une empreinte digitale de 128 bits. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du condensé du document permettant de vérifier l'intégrité de ce dernier)*
***SHA** (pour Secure Hash Algorithm, pouvant être traduit par Algorithme de hachage sécurisé) créant des empreintes d'une longueur de 160 bits*

Utilité d'une fonction de hachage

En expédiant un message accompagné de son haché, il est possible de garantir l'intégrité d'un message, c'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré (intentionnellement ou de manière fortuite) durant la communication.

Lors de la réception du message, il suffit au destinataire de calculer le haché du message reçu et de le comparer avec le haché accompagnant le document. Si le message (ou le haché) a été falsifié durant la communication, les deux empreintes ne correspondront pas.

Ainsi, pour garantir l'authentification du message, il suffit à l'expéditeur de chiffrer (on dit généralement signer) le condensé à l'aide de sa clé privée (le haché signé est appelé sceau) et d'envoyer le sceau au destinataire.



A réception du message, il suffit au destinataire de déchiffrer le sceau avec la clé publique de l'expéditeur, puis de comparer le haché obtenu avec la fonction de hachage au haché reçu en pièce jointe. Ce mécanisme de création de sceau est appelé scellement.

5.5. La notion de certificat

Les algorithmes de chiffrement asymétrique sont basés sur le partage entre les différents utilisateurs d'une clé publique. Généralement le partage de cette clé se fait au travers d'un annuaire électronique (généralement au format LDAP) ou bien d'un site web.

Ainsi un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé ***autorité de certification*** *(souvent notée* ***CA*** *pour Certification Authority). L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).*

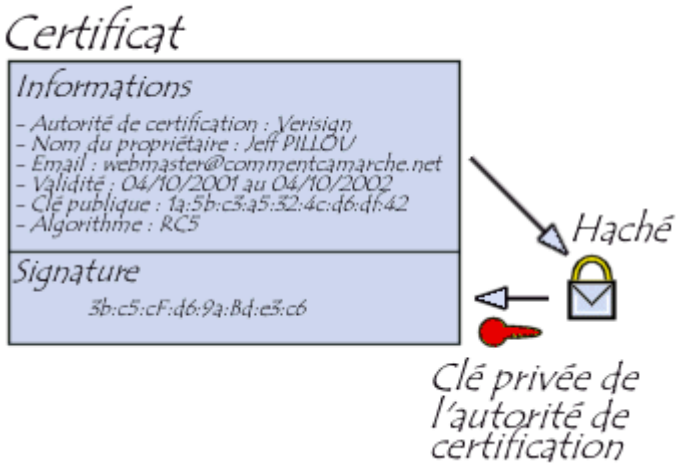
Qu'est-ce qu'un certificat ?

Les certificats sont des petits fichiers divisés en deux parties :
La partie contenant les informations
La partie contenant la signature de l'autorité de certification
La structure des certificats est normalisée par le standard X.509 de l'UIT (ITU : International Telecommunication Union), qui définit les informations contenues dans le certificat:

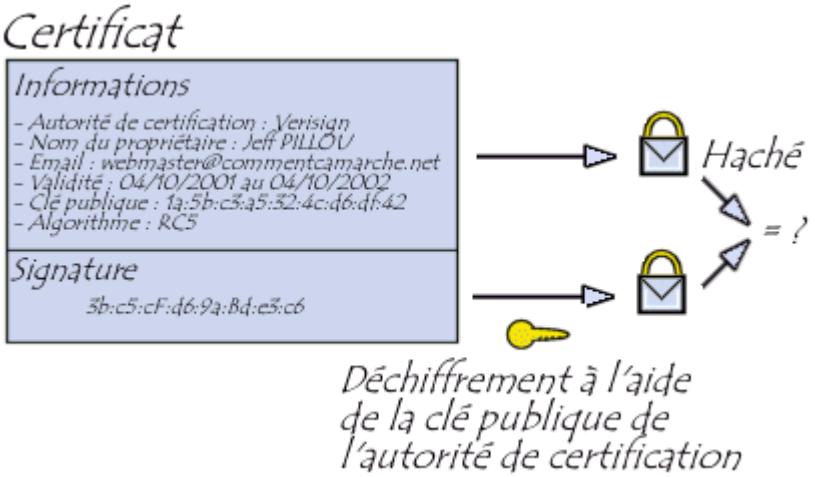
- *Le nom de l'autorité de certification*
- *Le nom du propriétaire du certificat*
- *La date de validité du certificat*
- *L'algorithme de chiffrement utilisé*
- *La clé publique du propriétaire*

5.6. Le scellement des données

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, ***puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification****; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification.*



Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire. Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats.



Utilité d'un tiers de confiance :

Exemple de tiers de confiance :

www.certinomis.com

www.Chambersign.tm.fr

Certificat de classe 2 : délivré par visualisation de document papier

Les certificats Societis sont des certificats de classe 2 garantissant le lien entre l'organisation (personne morale), vous (personne physique), les données nominatives et les données de signature. Ils sont délivrés après vérification de ces éléments selon une procédure de Classe 2.

Chaque certificat fourni est valable pour une utilisation illimitée, et est renouvelable ***tous les deux ans A partir de 120 € HT***

Usage
Quelle que soit la forme juridique de votre organisation (société, association, collectivité,...), le certificat permet de sécuriser et signer électroniquement les échanges dématérialisés en interne, au sein des entreprises, des administrations ou des communautés d'intérêts (groupement, associations, fédérations, etc.).

Fonctions
Signature et chiffrement de messages électroniques, documents et fichiers.
Authentification de l'utilisateur auprès des serveurs Web (SSL/TLS).
Signature et chiffrement des transactions en ligne.

Services
Enregistrement
Programme de garantie
Service de révocation en cas de perte, vol,
Assistance en ligne (messagerie et F.A.Q)
Assistance téléphonique

Certificat de classe 3: délivré uniquement par présentation face à face

Qu'est-ce qu'un certificat X509 ? Sans entrer dans du détail technique, les échanges https sont cryptés et décryptés à l'aide d'un couple de 'clés informatiques' qui sont propres à un serveur W3 :

La clé privée, qui n'est connue que de ce serveur
La clé publique qui est connue du monde entier

Le navigateur qui accède à un serveur à l'aide du protocole W3 doit récupérer la clé publique de ce serveur ; celle-ci lui est transmise par le serveur W3, encapsulée dans un certificat X509 (c'est un fichier informatique).

Ce certificat contient donc la clé publique du serveur, validée ("signée") par un organisme reconnu, appelé Autorité de Certification (AC).

LES FAMILLES DE CERTIFICATS REFERENCEES EN FRANCE

Autorité de certification	Famille de certificats
ATOS ORIGIN	MédiaCert TéléPro Entreprise
BNP PARIBAS-AUTHORITY ENTREPRISE	NET-IDENTITY
CERTEUROPE	CERTEUROPE CLASSE 3PLUS
CERTIGREFFE	CERTIGREFFE
CERTINOMIS	SOCIEPOSTE
CERTPLUS	DECLARACERT ENTREPRISE
CHAMBERSIGN (CHAMBRES DE COMMERCE ET D'INDUSTRIE)	CHAMBERSIGN FRANCE INITIO FIDUCIO
CLICK AND TRUST Groupe Banque Populaire	ADMINEO MERCANTEO
CREDIT AGRICOLE	CA CERTIFICAT
CREDIT COMMERCIAL DE FRANCE	CCF ELYS CERTIFICATION
CREDIT LYONNAIS	CREDIT LYONNAIS ENTREPRISE
GREFFE-TC-PARIS	GREFFE-TC-PARIS-OR-S
OUVERTURE	LE CHAINON MANQUANT CLASSE3PLUS
NATEXIS BANQUES POPULAIRES	NXBP RELATIONS FISCALES
SG TRUST SERVICES (SOCIETE GENERALE ET GROUPE CREDIT DU NORD)	SG TRUST SERVICES AUTHENTIFICATION ET CHIFFREMENT DE CLEF

5.7 Introduction à HTTPS

HyperText Transfer Protocol Secure - Protocole de transmission issu de Netscape lié à une connexion par socket sécurisée, autrement dit HTTP et SSL . Les accès à des pages web se font à l'aide du protocole http, en empruntant le réseau Internet.

Aucune garantie de confidentialité n'est assurée lors de ces accès ; il est relativement simple à un pirate d'intercepter vos requêtes et les réponses faites par le serveur. En outre, vous n'avez pas une certitude absolue d'être en cours de consultation du site que vous croyez.

Internet est maintenant utilisé pour des applications de commerce électronique, ou parfois pour accéder à des données confidentielles soumises à authentification (échange de login - mot de passe).

Il faut savoir que, dans ce cas, il n'est pas très difficile à un pirate d'intercepter ces informations confidentielles, y compris votre mot de passe, et ainsi d'usurper votre identité, voire récupérer votre code de carte bleue.

Afin de palier à ces inconvénients, le protocole https peut être mis en oeuvre. D'une manière très schématique, il permet d'encapsuler et de crypter le trafic http; ainsi, il sera quasiment impossible à un pirate qui intercepterait des accès à des pages chargée via le protocole https de décrypter cet échange, et donc de récupérer des informations confidentielles.

En outre, https permet de s'assurer que le serveur W3 auquel on accède est bien celui que l'on croit.

TRAVAUX DIRIGES N° 5

SIGNATURE ELECTRONIQUE

Exemple de chiffrement : Le chiffrement de Vigenère

Le chiffrement de Vigenère est un cryptosystème symétrique, ce qui signifie qu'il utilise ***la même clé pour le chiffrement et le déchiffrement.*** *Le chiffrement de Vigenère ressemble beaucoup au chiffrement de César, à la différence près qu'il utilise une clef plus longue afin de pallier le principal problème du chiffrement de César: le fait qu'une lettre puisse être codée d'une seule façon. Pour cela on utilise un mot clef au lieu d'un simple caractère.*

*Il consiste à coder un texte avec un mot en ajoutant à chacune de ses lettres la lettre d'un autre mot appelé clé. La clé est ajoutée indéfiniment en vis-à-vis avec le texte à chiffrer, puis le code ASCII de chacune des lettres de la clé est ajouté au texte à crypter. Par exemple le texte "****rendezvousamidi****" avec la clé* ***bonjour*** *sera codé de la manière suivante:*

212	212	220	206	212	239	232	209	228	225	203	220	222	214	203

Clé:

b	o	n	j	o	u	r
98	111	110	106	111	117	114

Texte crypté

r+b	e+o	n+n	d+j	e+o	z+u	v+r	o+b	u+o	s+n	a+j	m+o	i+u	d+r	i+b
114 + 98	101 + 111	110 + 110	100 + 106	101 + 111	122 + 117	118 + 114	111 + 98	117 + 111	115 + 110	97 + 106	109 + 111	105 + 117	100 + 114	105 + 98

212 -98	212 -111	220 -110	206 -106	212 -111	239 -117	232 -114	209 -98	228 -111	225 -110	203 -106	220 -111	222 -117	214 -114	203 -98

114	101	110	100	101	122	118	111	117	115	97	109	105	100	105

Texte original:

r	e	n	d	e	z	v	o	u	s	a	m	i	d	i
114	101	110	100	101	122	118	111	117	115	97	109	105	100	105

Pour déchiffrer ce message il suffit d'avoir la clé secrète et faire le déchiffrement inverse, ***à l'aide d'une soustraction.***