Réseaux
L2 Info
INUC Albi

François POUIT,

Éléments de sécurité réseau

Plan :

Chiffrement symétrique et asymétrique

Chiffrement symétrique - asymétrique

Rappel : chiffrement symétrique et asymétrique

Dans les algorithmes symétriques (ou à clé secrète) :

clé de chiffrement = clé de déchiffrement.

valeur de cette clé = secret partagé entre l'émetteur et le destinataire uniquement. Ceci explique le qualificatif de « clé secrète ».

DES (Data Encryption Standard) et AES (Advanced Encryption Standard) sont les algorithmes symétriques les plus connus.

Chiffrement symétrique - asymétrique

Rappel : cryptographie symétrique et asymétrique

Les opérations de chiffrement symétriques font appel à des fonctions mathématiques simples.

→ avantage : les opérations de chiffrement et de déchiffrement sont rapides à exécuter sur des ordinateurs classiques.

Par contre, le problème est la gestion des clés :

chaque clé que l'on utilise avec un correspondant doit être secrète et unique

→ autant de clés que de correspondants

Chiffrement symétrique - asymétrique

Rappel : cryptographie symétrique et asymétrique

il faut aussi trouver un moyen d'échanger chaque clé secrète avec chaque correspondant de manière sûre.

Si ceci est possible entre un groupe restreint de personnes, c'est impossible à plus grande échelle, par exemple pour échanger des messages chiffrés avec tous nos correspondants sur internet.

Chiffrement symétrique - asymétrique

Rappel : cryptographie symétrique et asymétrique

Dans les algorithmes asymétriques (ou à clé publique) :

la clé de chiffrement est différente de la clé de déchiffrement (d'où le terme asymétrique).

les deux clés (une pour chiffrer, l'autre pour déchiffrer) sont créées ensemble avec une fonction mathématique. Elles forment un couple, l'une ne va pas sans l'autre, mais il est impossible avec une des clés de découvrir l'autre.

tout texte chiffré avec une des clés (de chiffrement ou de déchiffrement) peut être déchiffré avec l'autre clé (de déchiffrement ou de chiffrement) et uniquement avec celle-ci.

Chiffrement symétrique - asymétrique

Rappel : cryptographie symétrique et asymétrique

Il faut :

générer un couple de clés (l'une pour chiffrer, l'autre déchiffrer) pour chaque utilisateur.

clé de déchiffrement = clé secrète ou clé privée.

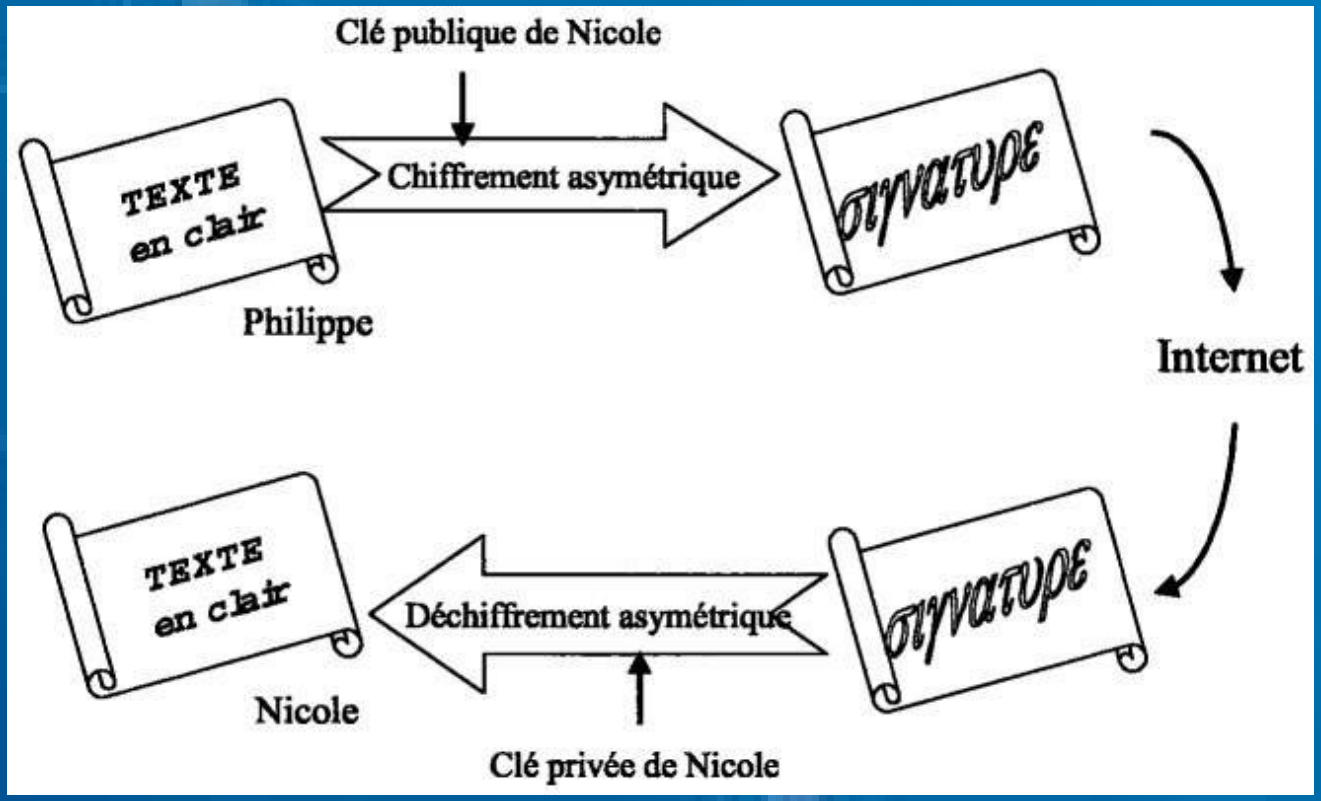
clé de chiffrement = clé publique donc diffusée (dans des annuaires électroniques, par exemple)

couple de clés = (clé privée pour déchiffrer, clé publique pour chiffrer)

Chiffrement symétrique - asymétrique

Rappel : cryptographie symétrique et asymétrique

Envoi de message :



RSA, du nom des trois inventeurs Rivest, Shamir, Adleman, est l'algorithme de chiffrement asymétrique le plus répandu.

Chiffrement symétrique - asymétrique

Rappel : cryptographie symétrique et asymétrique

Ce découplage entre clé publique et clé privée est très utile pour une utilisation « planétaire » du chiffrement :

les algorithmes symétriques obligent à échanger un secret, la clé secrète, avec chaque interlocuteur.

Avec les algorithmes asymétriques il suffit d'avoir des annuaires qui permettent de trouver la clé publique de chaque internaute et ce système peut fonctionner entre tous les internautes.

Quand un utilisateur voudra envoyer un message chiffré à un correspondant, il consultera un annuaire qui lui indiquera la clé publique de son correspondant. Avec cette clé, il chiffrera le message.

Chiffrement symétrique - asymétrique

Rappel : cryptographie symétrique et asymétrique

Celui-ci ne pourra être déchiffré qu'avec la clé privée du correspondant, donc que par le correspondant.

Ainsi les propriétés des algorithmes asymétriques permettent de s'affranchir du problème de la gestion des clés et ainsi d'envisager de déployer l'utilisation du chiffrement à très grande échelle.

Signature électronique

La signature électronique

La signature électronique est un mécanisme qui permet d'assurer les fonctions d'authentification et d'intégrité.
Elle est utilisée en particulier dans la messagerie électronique.

Génération d' une signature électronique :

- utilisation d' une fonction de hachage sur le texte.
résultat = une suite de bits de taille fixe<< à la taille du texte initial.
= condensé ou empreinte.
La fonction de hachage est telle que si un bit du texte d'origine est modifié, le résultat de la fonction sera, avec de très fortes probabilités, différent.

MD5 (Message Digest) et SHA (Secure Hash Algorithm) sont parmi les plus connues.

Signature électronique

La signature électronique

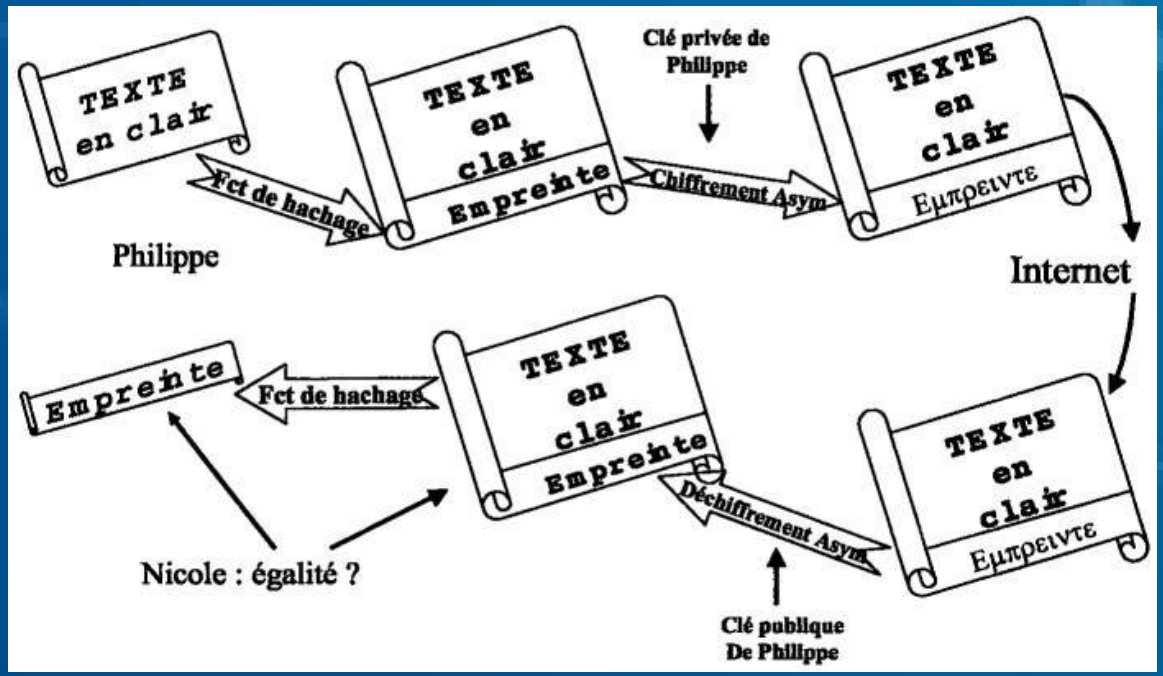
- chiffrage ensuite de cette empreinte par un algorithme asymétrique avec la clé privée de l'utilisateur.
C'est la signature électronique.

Avant l'envoi, cette signature est ajoutée au message, qui devient un message signé.

Signature électronique

La signature électronique

Le récepteur déchiffre cette empreinte chiffrée avec la clé publique de l'émetteur. Puis il recalcule la fonction de hachage sur le message reçu et compare le résultat avec l'empreinte déchiffrée. Si les deux sont égaux, cela veut dire que le message n'a pas été modifié durant le transfert et que l'émetteur est authentifié



Signature électronique

La signature électronique

En effet, si le message a été modifié durant le transfert, les 2 empreintes seront différentes. De plus, être capable de déchiffrer, avec la clé publique d'une personne, une empreinte chiffrée, prouve que cette empreinte a obligatoirement été chiffrée avec la clé privée de la personne, clé que seul possède l'émetteur. Cela authentifie donc l'émetteur. On peut rappeler qu'une des propriétés du couple clé privée-clé publique est que tout ce qui est chiffré avec une des clés peut être déchiffré avec l'autre clé et uniquement avec celle-ci.

certificat électronique

Les logiciels combinent à la fois le chiffrement du message et sa signature.

Mais il y a un oubli dans les raisonnements précédents : on a considéré qu'un utilisateur prenait connaissance de la clé publique d'une personne simplement en consultant un annuaire (ou un serveur web).

Qu'est-ce qui garantit que la clé publique de Philippe qu'un utilisateur a ainsi récupérée est la bonne ?

certificat électronique

Un pirate, François

a pu modifier l'annuaire ou le serveur web qui contient cette clé.
Il a pu par exemple remplacer la clé publique de Philippe par la sienne.

Une fois cette mascarade commise, François pourra lire les courriers confidentiels destinés à Philippe et signer des messages en se faisant passer pour Philippe.

Il a donc fallu créer un mécanisme supplémentaire pour pouvoir vérifier la validité d'une clé publique : le **certificat électronique**.

certificat électronique

Un certificat électronique de personne est l'équivalent électronique d'une carte d'identité ou d'un passeport.

Un passeport contient des informations concernant son propriétaire (nom, prénom, adresse…), la signature manuscrite, la date de validité, ainsi qu'un tampon et une présentation (forme, couleur, papier) qui permettent de reconnaître que ce passeport n'est pas un faux, qu'il a été délivré par une autorité bien connue.

Un certificat électronique est un petit fichier qui contient des informations similaires. Le format standard actuellement est le format X509v3.

certificat électronique

On peut par exemple trouver dans un certificat électronique les informations suivantes :

le nom de l'autorité (de certification) qui a créé le certificat,
le nom et le prénom de la personne,
le nom de l'institution de la personne,
son adresse électronique,
sa clé publique,
les dates de validité du certificat,
la signature électronique de ce certificat.

certificat électronique

La signature électronique du certificat :

Cette signature électronique, le dernier élément du certificat listé ci-dessus, est calculée sur les informations contenues dans le certificat (nom, clé publique…) comme dans le cas d'un message électronique.

Cette signature est l'empreinte de ces informations, chiffrée avec la clé privée de l'autorité de certification qui a délivré ce certificat.

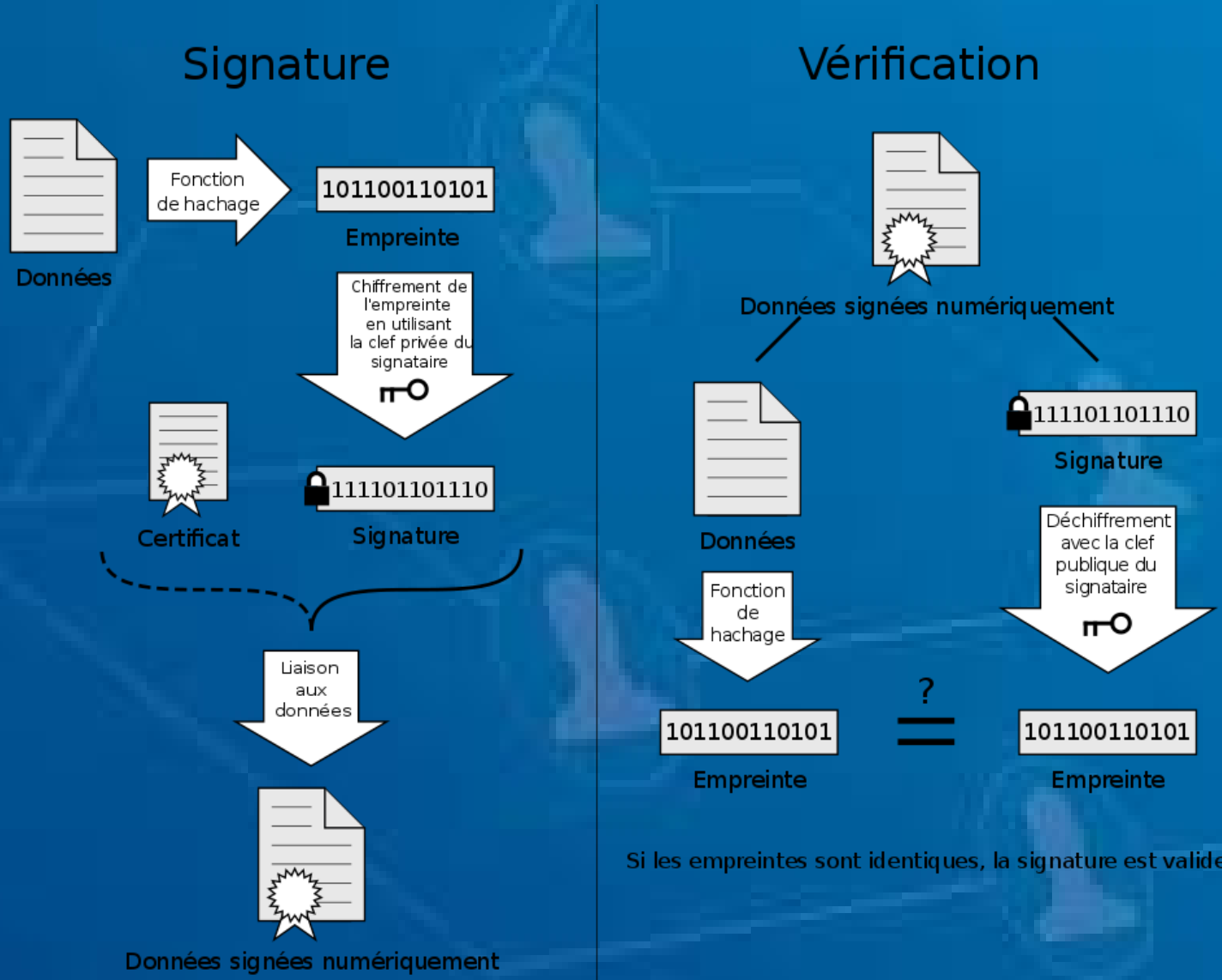
certificat électronique

L’autorité de certification

Une entité qui délivre des certificats pour une communauté d’utilisateurs au sommet d’une infrastructure de gestion de clés : IGC.
C’est l’équivalent de la préfecture pour un passeport.

Cette autorité, préalablement à toute action, a généré un couple de clés publique-privée pour elle-même. Ensuite elle a très largement diffusé la valeur de sa clé publique, sous la forme d’un certificat d’autorité de certification. Les utilisateurs qui veulent utiliser et faire confiance aux certificats émis par cette autorité, insèrent ce certificat dans leurs outils (navigateur, client de messagerie).

Signature & certificat électronique



Signature & certificat électronique

La démarche ci-dessus est celle de la messagerie électronique.
Des mécanismes légèrement différents sont très répandus pour utiliser ces mêmes éléments dans d'autres applications.

Quelques exemples :

Un serveur web peut posséder un couple de clés et un certificat. Ils seront mis en œuvre pour prouver à chaque client qu'il est bien sur le bon serveur avec la bonne application, assurance obligatoire quand le serveur permet des transactions financières, par exemple.

Les mêmes éléments sur ce serveur pourront aussi être utilisés pour chiffrer tous ses échanges avec ses clients en utilisant les protocoles HTTPS (Hypertext Transfer Protocol Secure) et SSL (Secure Socket Layer).

Signature & certificat électronique

Plus généralement toute application qui utilise le réseau :

- transfert de fichiers
- accès interactif
- accès à des bases de données
- calcul distribué)

et tous les objets (postes nomades, équipements de réseau) peuvent avoir un couple de clés et un certificat pour mettre en œuvre ces fonctions de sécurité.

Signature & certificat électronique

En simplifiant, il existe trois standards principaux à la base des applications qui utilisent les certificats électroniques :

- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- SSL/TLS (Secure Socket Layer et Transport Layer Security)
- IPSec (IP Security Protocol).

S/MIME, standard de messagerie permet, avec un mécanisme de signature, l'authentification de l'émetteur et l'intégrité du message, ainsi que la confidentialité du contenu avec un mécanisme de chiffrement, dans l'échange de messages électroniques. Il est supporté de base par Netscape-Mozilla et Outlook.

Signature & certificat électronique

SSL/TLS permet un transport sécurisé des informations sur l'internet avec les fonctions d'authentification du serveur et du client, d'intégrité et de confidentialité des échanges. Il peut être utilisé pour tous les accès web avec le protocole HTTPS, pour accéder aux boîtes aux lettres à distance avec les protocoles IMAPS (Internet Message Access Protocol) et POPS (Post Office Protocol), et éventuellement dans d'autres applications (transfert de fichiers, telnet). Netscape-Mozilla et Internet Explorer intègrent HTTPS et IMAPS.

IPSec est destiné à sécuriser le contenu des datagrammes IP dans les communications entre équipements de réseau et/ou les stations. Il permet par exemple de construire des réseaux virtuels privés (VPN) entre routeurs et des connexions sécurisées de postes nomades vers un site central. Il est intégré maintenant dans la majorité des systèmes d'exploitation des équipements de réseau et des postes de travail.

Signature & certificat électronique

D’autre part, les versions récentes de SSH, très répandu, ensemble de logiciels utilisés pour l’accès interactif principalement, supportent maintenant les certificats comme méthode d’authentification.

Il existe ainsi tout le nécessaire pour construire un ensemble d’applications dont les fonctions de sécurité sont basées sur les certificats électroniques.