Sécurité des échanges sur les réseaux :

1) L'enjeu :

La sécurité des réseaux informatiques est un sujet essentiel pour favoriser le développement des échanges dans différents domaines.

Savoir sécuriser les données, c'est garantir :

- L'authentification réciproque des correspondants pour être sûr de son interlocuteur
- L'intégrité des données transmises pour être sûr qu'elles n'ont pas été modifiées accidentellement ou intentionnellement.
- La confidentialité pour éviter que les données soient lues par des systèmes ou des personnes non autorisées
- La non répudiation pour éviter la contestation par l'émetteur de l'envoi de données

2) L'Objectif :

Lorsque l'on cherche à sécuriser un réseau les objectifs attendus sont divers, voici ci-dessous les principaux objectifs recherchés ainsi que leur signification :

- La confidentialité : C'est le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé, dans le domaine de l'informatique, consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

- L'authentification : C'est l'action consistant à assurer que seules les personnes autorisées aient accès aux ressources. Dans n'importe quel domaine c'est la base même de la sécurité.

- La non répudiation : La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction. La non-

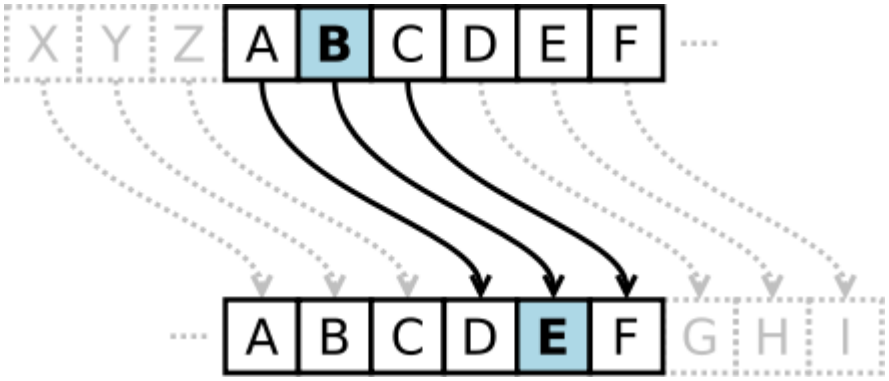
répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues

- Contrôle de l'intégrité : C'est garantir que les données sont bien celles que l'on croit être

3) Les Moyens

- Le Chiffrement :

Le chiffrement désigne la pratique consistant à coder et décoder des données. Des données chiffrées sont des données qui ont été codées à l'aide d'un algorithme de sorte qu'elles ne se présentent plus sous leur forme d'origine et ne soient donc plus lisibles.



Il existe de nombreuses méthodes de chiffrements, ici nous allons nous intéresser à l'algorithme du RSA.

Le chiffrement RSA (nommé par les initiales de ses trois inventeurs : Rivest, Shamir, Adleman) est un algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

La cryptographie asymétrique, ou cryptographie à clé publique, est une méthode de chiffrement qui s'oppose à la cryptographie symétrique. Elle repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le

décoder. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour coder un message que seul le destinataire (en possession de la clé privée) peut décoder, garantissant la confidentialité du contenu. Inversement, l'expéditeur peut utiliser sa propre clé privée pour coder un message que le destinataire peut décoder avec la clé publique ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message.

P.K.I

Une infrastructure à clés publiques (ICP) ou infrastructure de gestion de clés (IGC) ou encore Public Key Infrastructure (PKI), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériel type HSM ou encore des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) destiné à gérer le cycle de vie des certificats numériques ou certificats électroniques.

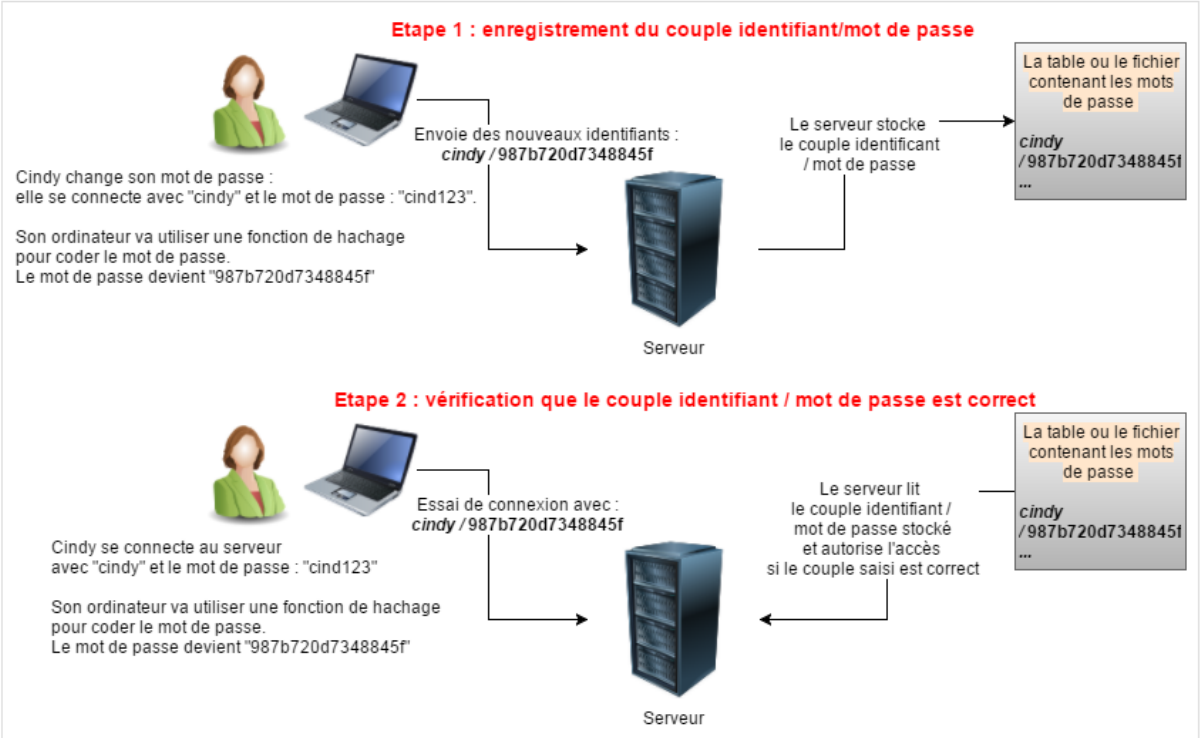
Une infrastructure à clés publiques fournit des garanties permettant de faire a priori confiance à un certificat signé par une autorité de certification grâce à un ensemble de services. Ces services sont les suivants :

- Enregistrement des utilisateurs (ou équipement informatique) ;
- Génération de certificats ;
- Renouvellement de certificats ;
- Révocation de certificats ;
- Publication de certificats ;
- Publication des listes de révocation (comprenant la liste des certificats révoqués) ;
- Identification et authentification des utilisateurs (administrateurs ou utilisateurs qui accèdent à l'ICP) ;
- Archivage, séquestre et recouvrement des certificats (option).

Le Hachage

Une fonction de hachage est une fonction qui va calculer une empreinte (ou signature) unique à partir des données fournies.

Cette fonction va prendre le texte du mot de passe et le « mouliner » pour obtenir une signature (cette signature est aussi appelée « empreinte »). L'ordinateur ne va pas envoyer le mot de passe au serveur, mais une signature du mot de passe. Le serveur ne va enregistrer le mot de passe mais enregistrera cette signature. Lorsque l'utilisateur se connectera, le serveur ne va pas vérifier si le mot de passe est identique, mais il va vérifier que la signature du mot de passe saisi est bien la même que la signature du mot de passe enregistré.

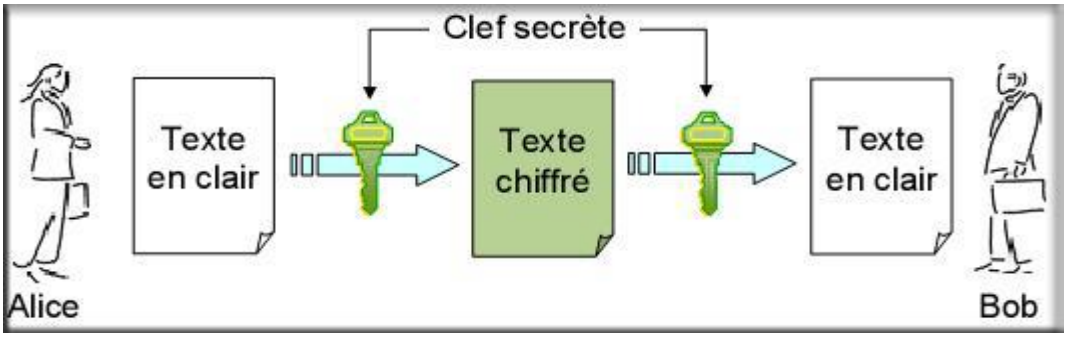


La différence du Chiffrement Symétrique et Asymétrique

Cryptage Symétrique :

- On parle de cryptographie symétrique lorsqu'un texte, document, etc. est chiffré et déchiffré avec la même clé, qui est la clé secrète. Ce procédé est à la fois simple et sûr.

- Principal inconvénient : étant donné que l'on n'a qu'une clé, si vous la donnez à X pour qu'il puisse vous envoyer des messages chiffrés avec celle-ci, il pourra aussi bien déchiffrer tous les documents que vous avez chiffrés avec cette dernière. La clé est donc connue uniquement par le destinataire et l'émetteur et il est plus sûr de faire une clé pour un échange entre X et Y, pour éviter qu'avec une clé on puisse tout déchiffrer.



Cryptage Asymétrique :

- Contrairement à la cryptographie symétrique, ici avec l'asymétrique, on a 2 clés.

- Il y a dans un premier temps la clé publique, tout le monde peut la posséder, il n'y a aucun risque, vous pouvez la transmettre à n'importe qui. Elle sert à chiffrer le message.

- Puis il y a la clé privée que seul le récepteur possède, en l'occurrence vous. Elle servira à déchiffrer le message chiffré avec la clé publique.

4) Certificat

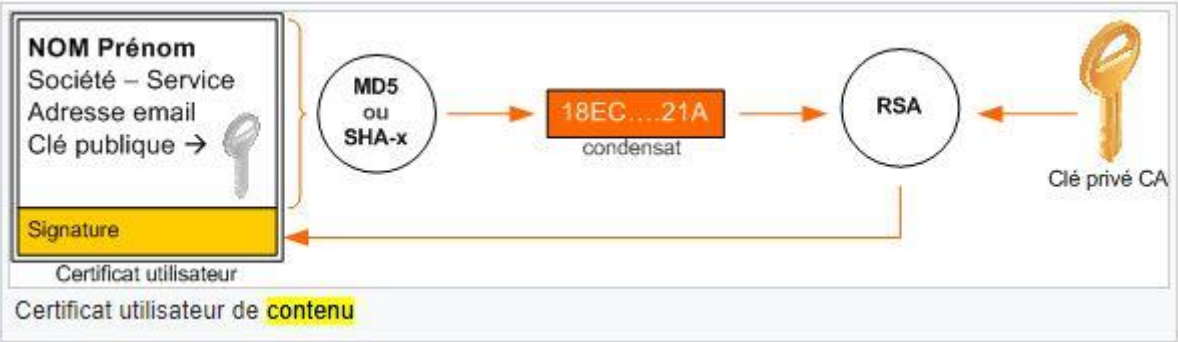
Un Certificat peut être considéré comme une carte d'identité numérique. Il est utilisé principalement pour identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges.

Contenus :

Un certificat électronique est un ensemble de données contenant :

- Une clé publique (au moins)
- Des informations d'identification, par exemple : nom, localisation, adresse électronique.
- Au moins une signature (clé privée) ; de fait quand il n'y en a qu'une, l'entité signataire est la seule autorité permettant de prêter confiance (ou non) à l'exactitude des informations du certificat.

Les certificats électroniques et leur cycle de vie peuvent être gérés au sein d'infrastructures à clés publiques.



Utilisation :

Les certificats électroniques sont utilisés dans différentes applications informatiques dans le cadre de la sécurité des systèmes d'information pour garantir :

- la non-répudiation et l'intégrité des données avec la signature numérique ;
- la confidentialité des données grâce au chiffrement des données ;
- l'authentification ou l'authentification forte d'un individu ou d'une identité numérique.

Exemples d'utilisation :

- Serveur web (TLS, X.509) ;
- Courrier électronique (OpenPGP) ;
- Poste de travail (IEEE 802.1X) ;
- Réseau privé virtuel (VPN)
- Secure Shell (SSH), TLS
- Documents électroniques
- Site Web

Signature :

Comme je l'ai expliqué dans la rubrique « contenus », la signature dans un certificat est représentée par une clé privée, quand il n'y en a qu'une, l'entité signataire est la seule autorité permettant de prêter confiance (ou non) à l'exactitude des informations du certificat.

Les certificats résolvent le problème du canal sécurisé grâce à la signature de tiers de confiance.

Autorité de Certification :

Le terme Autorité de Certification désigne les organismes enregistrés et certifiés auprès d'autorités publiques et/ou de gouvernance de l'Internet qui établissent leur viabilité comme intermédiaire fiable.

Ces organismes diffusent leurs propres clés publiques. Étant certifiées fiables ces autorités sont en contact direct avec les principaux producteurs de systèmes d'exploitation et de navigateurs web qui incluent nativement les listes de clés des autorités de certification.

C'est cette relation qui est à la base de la chaîne de confiance. Ces clés sont appelées clés publiques racines ou certificats racines et sont utilisées pour identifier les clés publiques d'autres organismes.

Les certificats peuvent être stockés par des serveurs de clés, qui peuvent aussi faire office d'autorité d'enregistrement et de certification. Ils recensent et contrôlent les certificats. Ils possèdent souvent une liste.