Une introduction sur les PKI

On désigne sous l'appellation PKI (Public Key Infrastructure) l'ensemble des moyens matériels, logiciels, composants cryptographiques, mis en oeuvre par des personnes, combinés par des politiques, des pratiques et des procédures requises, qui permettent de créer, gérer, conserver, distribuer et révoquer des certificats basés sur la cryptographie asymétrique.

La PKI a pour but d'établir la confiance dans les échanges entre plusieurs personnes.

Avant l'échange, elle garantit :

- l'authentification des partenaires
  C'est à dire permettre aux partenaires de s'assurer de leur identité mutuelle.

Pendant l'échange, elle garantit :

- la confidentialité, grâce au chiffrement
  Le chiffrement consiste à rendre un document incompréhensible pour certaines personnes.

- l'intégrité des messages
  Cela signifie qu'un message émis est identique au message reçu.

Après l'échange, elle garantit :

- la non-répudiation des messages.
  Cela signifie qu'une personne ayant émis un message ne peut nier l'avoir fait.

Ces services ne seraient pas possibles sans la cryptographie et l'utilisation de certificats numériques.

Les principes essentiels de la cryptographie

On distingue deux grands domaines dans la cryptographie, la cryptographie symétrique et la cryptographie asymétrique ou cryptographie à clef publique.

La cryptographie symétrique

Dans la cryptographie symétrique deux partenaires souhaitant échanger des informations confidentiellement se mettent d'accord sur une clef secrète commune, appelée clef de session, qui leur

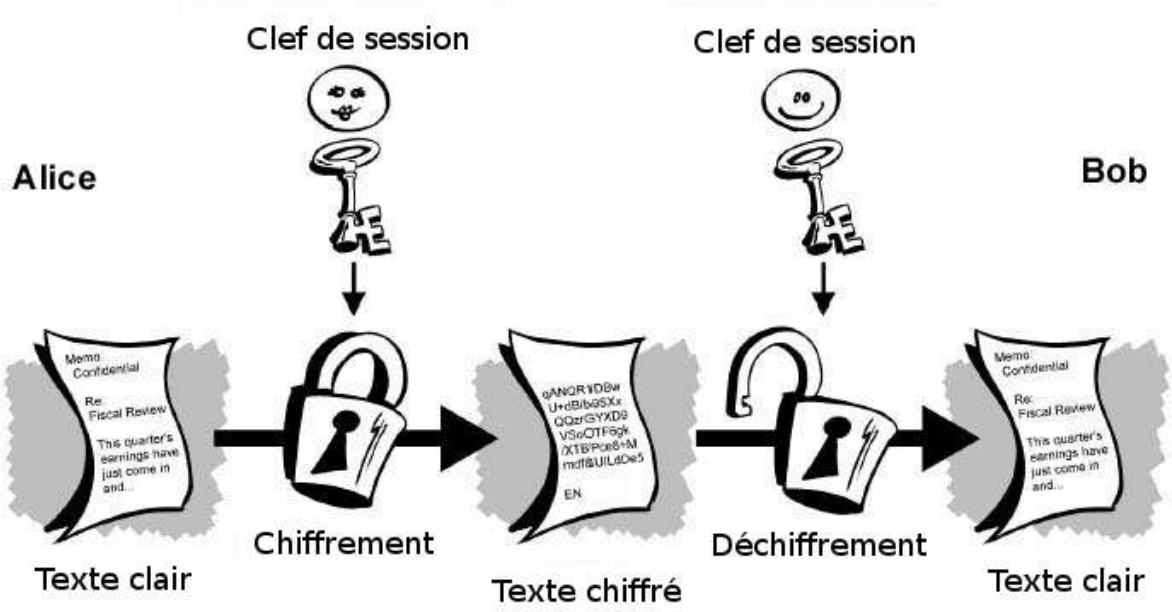
servira à chiffrer leurs messages.

Prenons l'exemple d'Alice souhaitant envoyer un message à Bob. Alice et Bob commencent par se mettre d'accord sur la clef de session.

Alice envoie alors son message chiffré à l'aide de la clef à Bob. Si la clef est F, le message M, le message crypté C et l'algorithme de cryptage t, on obtient : C = t(M, F)

Bob doit maintenant décrypter C. L'algorithme de chiffrement t est symétrique, cela signifie que les même opérations sont effectuées pour chiffrer ou déchiffrer les messages. Bob obtient donc le message en clair avec la formule suivante : M = t(C, F).

D'une manière schématique on a :



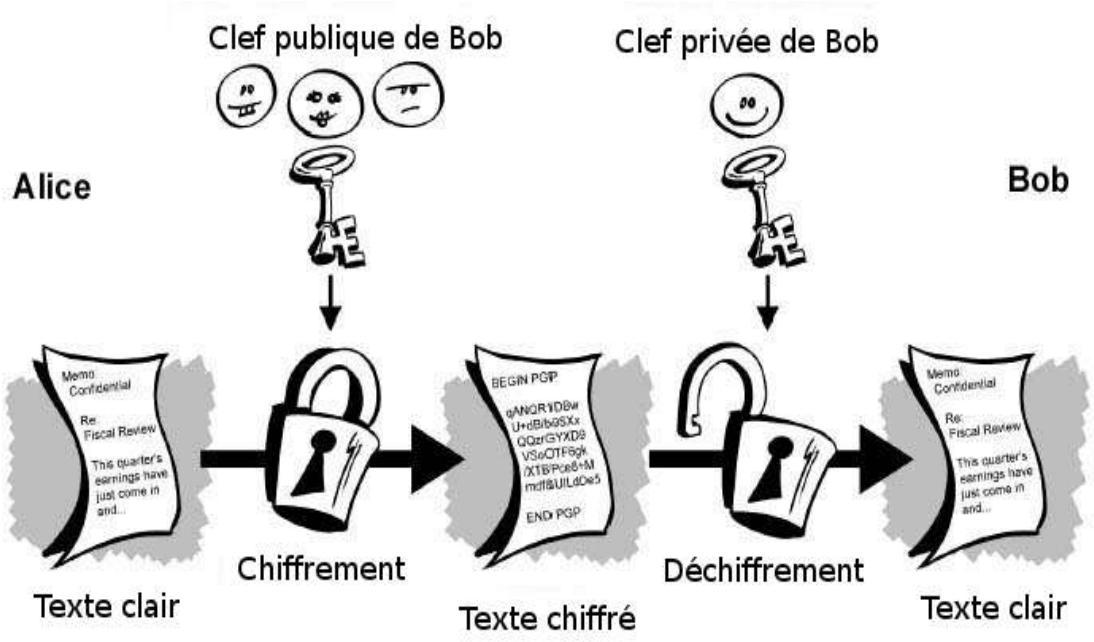
Les algorithmes symétriques les plus répandus sont par exemple RC4, RC5, DES, 3DES ou AES. Ces algorithmes sont rapides mais ils posent le problème de l'échange de la clef de session. Si cette clef est récupérée par un attaquant il peut décrypter toutes les conversations. Par défaut un réseau local d'entreprise ou internet ne sont pas assez sur pour échanger cette clef de session. Nous verrons plus loin comment la cryptographie à clef publique permet d'échanger en sécurité une clef de session avec un support de transmission qui n'est pas sur.

De plus sur un groupe de n personnes, chaque individu doit posséder n-1 clefs pour communiquer avec le groupe. Il y a donc un très grand nombre de clef au sein du groupe, et chacune doit rester connue de deux personnes. Cela fait un grand nombre de clef à gérer de manière sécurisée ! On voit rapidement les limites de la cryptographie symétrique.

La cryptographie asymétrique ou cryptographie à clef publique

Dans la cryptographie asymétrique chaque entité dispose d'une clef publique, et d'une clef privée. La clef publique est diffusée à l'ensemble des autres entités souhaitant communiquer avec la première. Elle sert à chiffrer les communications. La clef privée reste secrète et l'entité s'en sert pour déchiffrer les communications. La cryptographie à clef publique est également utilisée pour l'authentification et pour les signatures numériques. *Lorsqu'une entité signe un document, elle garantit mathématiquement qu'elle en est l'émettrice.*

Reprenons l'exemple de Alice souhaitant envoyer un message à Bob. Schématiquement on a :



Bob envoie sa clef publique à Alice, ou Alice la récupère par l'intermédiaire d'un serveur public accessible sur internet. Puis Alice chiffre le message à l'aide de la clef publique de Bob. Sur le schéma, la clef publique permet de fermer le cadenas. Alice envoit alors le message à Bob qui peut le déchiffrer avec sa clef privée.

Les algorithmes asymétriques les plus répandus sont Diffie-Hellman et RSA. La cryptographie asymétrique étant mille fois plus lente que la cryptographie symétrique, on utilise les deux couplées pour obtenir de bonnes performances sans avoir les défauts de la cryptographie symétrique. La cryptographie asymétrique est utilisée pour l'authentification et pour l'échange d'une clef de session. Une fois la clef de session échangée un algorithme symétrique est utilisé. Ce schéma est employé dans SSL (Secure Socket Layer), protocole permettant une communication réseau sécurisée entre entités, au dessus de la couche transport.

Les certificats numériques

Les certificats numériques sont l'équivalent électronique des cartes d'identités. Ils permettent d'authentifier les entités au sein d'un système d'information.

Un certificat à clef publique contient plusieurs informations dont l'identité d'une personne et sa clef publique. La clef publique allant de pair avec une clef privée, lorsqu'on parle du possesseur d'un certificat on entend en fait « possesseur de la clef privée associée au certificat ». Le certificat est signé par l'autorité de certification de la PKI, entité que nous verrons plus loin. Plusieures normes de certificats existent, les plus employées sont X509 dans sa version 2 et dans sa version 3. Cette version définit un certain nombre d'extensions qui peuvent être ajoutées au certificat. Une d'entre elle permet par exemple de savoir l'emploi du certificat : s'il s'agit d'un certificat pour un serveur web, d'un certificat pour signer du code etc. Les certificats ne sont pas uniquement employés par des personnes mais aussi par des matériels, comme les serveurs ou par les routeurs sur un réseau utilisant IPSec.

Le plus important à retenir est que le certificat fait une association clef publique/identité, association garantie par une autorité de confiance. Cette association permet l'authentification.

Principes généraux d'une PKI

Pour assurer des services d'authentification, de confidentialité et de non-répudiation des messages, la PKI fait une utilisation intensive des certificats. Par le biais de ses différentes entités elle en assure la totale gestion, de l'émission à la révocation, et c'est là l'essentiel de sa tâche.

Les entités d'une PKI

Les PKIs se décomposent habituellement en plusieurs entités :

- L'entité de certification (CA, Certification Authority).

  C'est l'entité la plus importante. Elle signe les demandes de certificats et les listes de révocation.

- L'autorité d'enregistrement (RA, Registration Authority).

  Elle a pour mission de générer les demandes de certificats. Elle effectue les vérifications d'usage sur l'identité de l'utilisateur à qui l'on remettra le certificat.

- L'autorité de dépôt

  Elle stocke les certificats numériques ainsi que les listes de révocation. Elle est souvent

confondue avec la CA.

- L'autorité de séquestre

  Cette entité permet de stocker les clefs privées des certificats générés, et de les récupérer si le besoin s'en fait sentir. Par exemple pour récupérer des documents chiffrés sans avoir à obtenir la clef privée de la personne ayant chiffrée les documents.

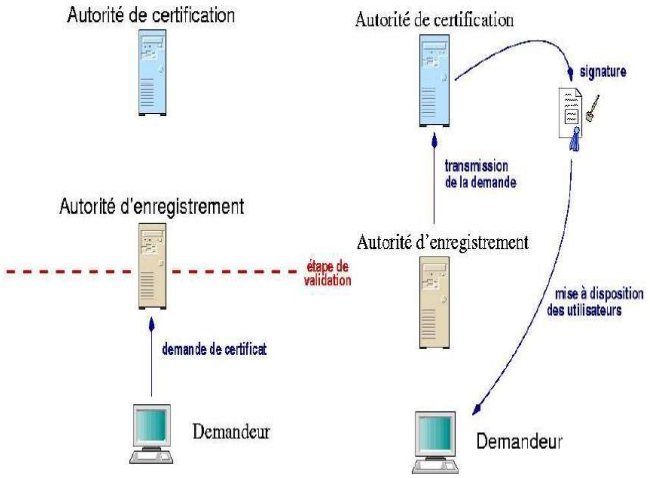
- L'entité d'enrôlement

  Cet entité enregistre les utilisateurs finaux, à qui on remettra les certificats. Elle est facultative, cependant elle fait partie des recommandations PKIX de l'IETF.

L'IETF (The Internet Engineering Task Force) est une organisation constituée en groupes de travail de volontaires intéressés par l'évolution des technologies liées au web; ces groupes émettent des recommandations ou des normes. Les standards PKIX définissent essentiellement la manière dont les différentes entités d'une PKI doivent collaborer entre elles.

Cycle de vie d'un certificat

Le schéma suivant représente les premiers échanges entre l'utilisateur et la PKI menant à l'émission d'un certificat :



L'utilisateur fait d'abord une demande de certificat auprès de l'autorité d'enregistrement (RA). La RA vérifie l'identité de l'utilisateur puis transmet une demande de certificat à l'autorité de certification (CA). La CA signe alors cette demande. On obtient un certificat, ainsi qu'une clef privée allant avec la clef publique contenue dans le certificat. Le certificat est déposé dans le dépôt. Si un module de séquestre est mis en place il conserve la clef privée associée au certificat. Puis le certificat et la clef privée sont remis à l'utilisateur.

Appelons cet utilisateur Bob. Toute personne voulant communiquer avec Bob pourra obtenir son certificat, vérifier la validité du certificat auprès d'une autorité de certification, et ainsi s'assurer que la clef publique qui sera employée pour crypter la conversation est celle de Bob. La communication sera ensuite chiffrée avec les méthodes cryptographiques détaillées ci-dessus.

On révoque un certificat lorsque la clef privée qui lui est associée est volée, cette dernière permettant de décrypter les communications. La CA ajoute alors le certificat à la liste de révocation. Les logiciels utilisant les certificats doivent veiller à récupérer régulièrement les listes de révocation auprès des CA qu'ils utilisent afin de s'assurer que les certificats employés pour chiffrer les conversations n'ont pas été révoqués.

Kototama
http://kototama.free.fr/