PKI : Infrastructures à clés publiques

Master Ingénierie des logiciels

1.0

Table des matières

PKI : Infrastructures à clés publiques

I

1. Systèmes asymétriques : atouts et limites

La gestion des clés est plus facile avec les systèmes asymétriques

Dans ce scénario, si le réseau est composé de n noeud alors il faudra gérer n.(n-1)/ 2 clé, ce qui ne s'adapte pas au facteur d'échelle. Avec 500 noeud, on arrive déjà à plus de 12 millions de clés à gérer.

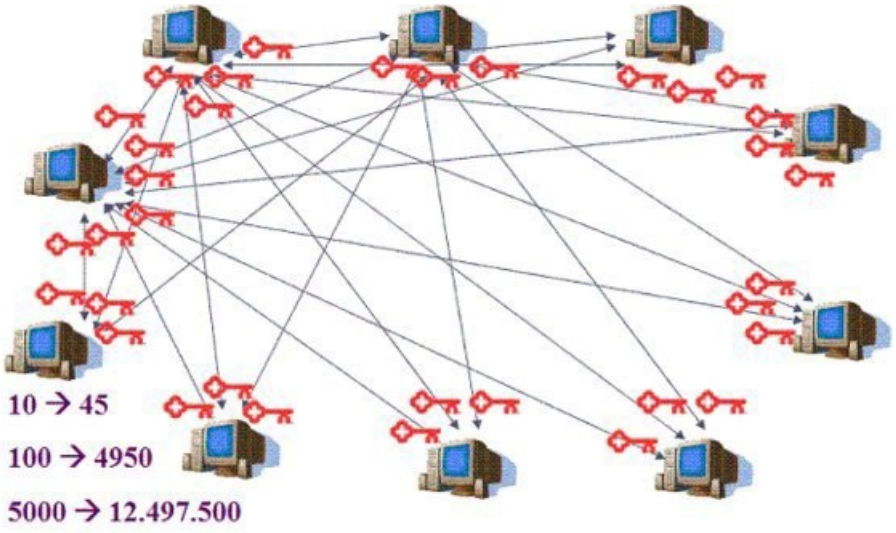

Image 16 : Limites de la gestion de clés symétriques

Par contre, avec un système asymétrique chaque utilisateur aura besoin d'une paire de clés. Donc on aura à gérer seulement 2.n clés au lieu des n.(n-1)/2 clés dans le cas symétrique.

Utilité d'un système asymétrique dans l'authentification

Nous avions déjà vus que l'usage d'un système asymétrique est indispensable pour garantir la non-répudiation de l'origine.

L'usage d'un système asymétrique est également utile pour l'identification comme expliqué plus bas.

Dans ce scénrio, Alice veut s'assurer de l'identité de Bob. Elle ne connaît de Bob que sa clé publique.

Pour s'assurer de l'identité de Bob, Alice lui envoie un défi (un nombre aléatoire).

Pour prouver son identité à Alice, Bob signe le défi avec sa clé privée et envoie sa signature sur le défi à Alice.

Pour vérifier l'identité de Bob, il suffit que Alice vérifie la signature de Bob avec sa clé publique comme illustré sur la figure ci-contre.

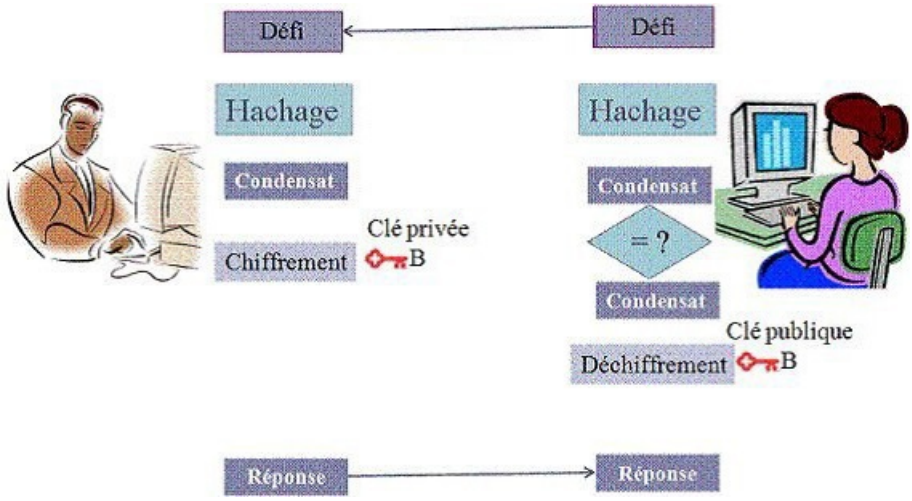

Image 17 : Identification avec un système asymétrique

⚠ *Attention : Comment garantir qu'une clé publique correspond bien à l'entité avec qui on communique ?*

Jusque là, nous avions toujours supposé que la clé publique est distribuée d'une manière sécurisée. Si cette hypothèse n'est pas vérifiée, un schéma asymétrique peut subir une attaque de type "Man in the Middle". Une telle attaque est illustréedans le scénario ci-après.

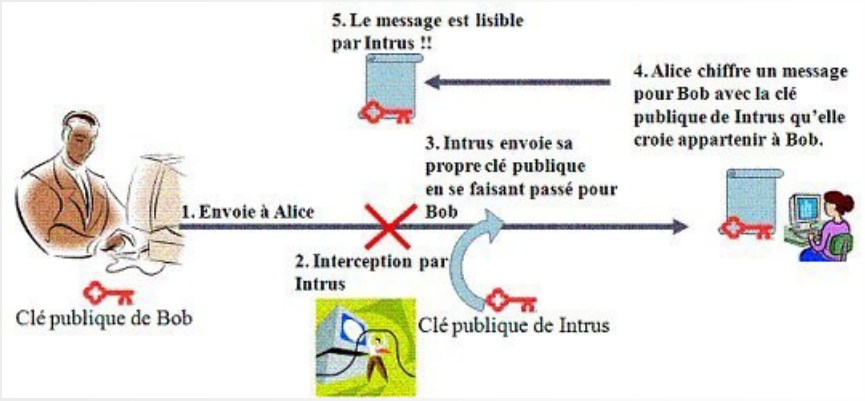

Image 18 : Man in the middle

Méthode : Certification numérique

La solution au problème dit "man in the middle" est l'usage d'un certificat numérique qui assure la liaison entre l'identité et la clé publique correspondante dans un document numérique signé par une tierce partie de confiance dite autorité de certification.

2. La certification numérique

Définition : Certificat numérique

- Un certificat à clé publique est un certificat numérique qui lie l'identité d'un système à une clé publique, et éventuellement à d'autres informations;
- C'est une structure de donnée signée numériquement qui atteste sur l'identité du possesseur de la clé privée correspondante à une clé publique.
- Un certificat est signé numériquement par une autorité de certification à qui font confiance tous les usagers et dont la clé publique est connue par tous d'une manière sécurisée. Ainsi, afin de publier sa clé publique, son possesseur doit fournir un certificat de sa clé publique signé par l'autorité de certification. Après vérification de la signature apposée sur le certificat en utilisant la clé publique de l'autorité de certification, le récepteur peut déchiffrer et vérifier les signatures de son interlocuteur dont l'identité et la clé publique sont inclus dans le certificat.

Exemple : Structure d'un certificat X.509

- Version
- Numéro de série
- Algorithme de signature du certificat
- Signataire du certificat
- Validité (dates limite)
    - Pas avant
    - Pas après
- Détenteur du certificat
- Informations sur la clé publique
    - Algorithme de la clé publique
    - Clé publique
- Identifiant unique du signataire (Facultatif)
- Identifiant unique du détenteur du certificat (Facultatif)
- Extensions (Facultatif)
    - Liste des extensions...

La figure suivante illustre un tel certificat inclus dans un navigateur web

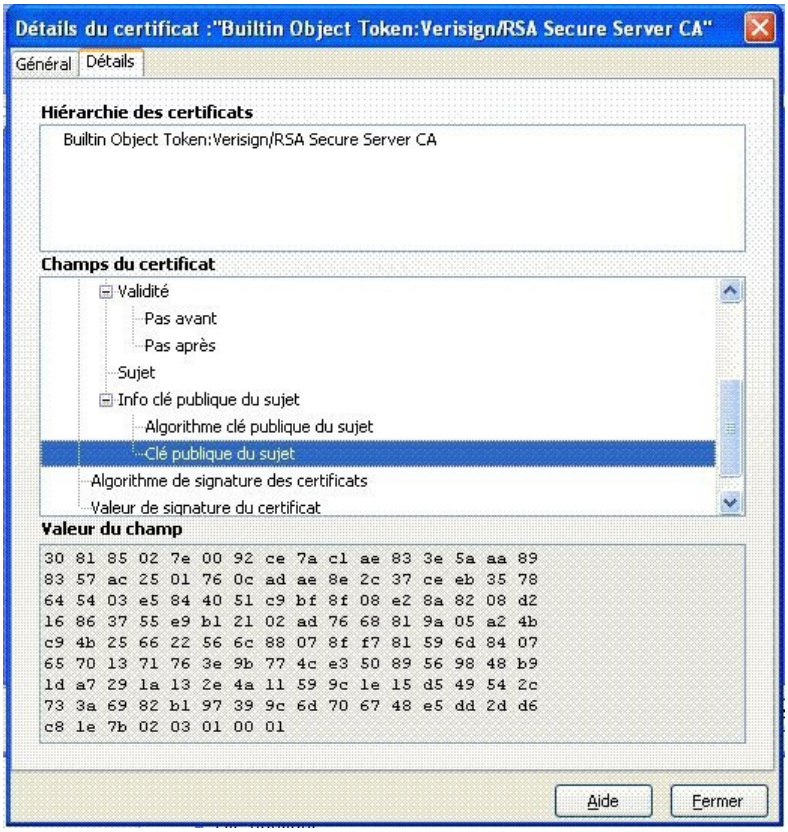

Image 19 : Certificat Numérique

Définition : Autorité de certification

Une autorité de certification est toute entité qui délivre des certificats de clé publique

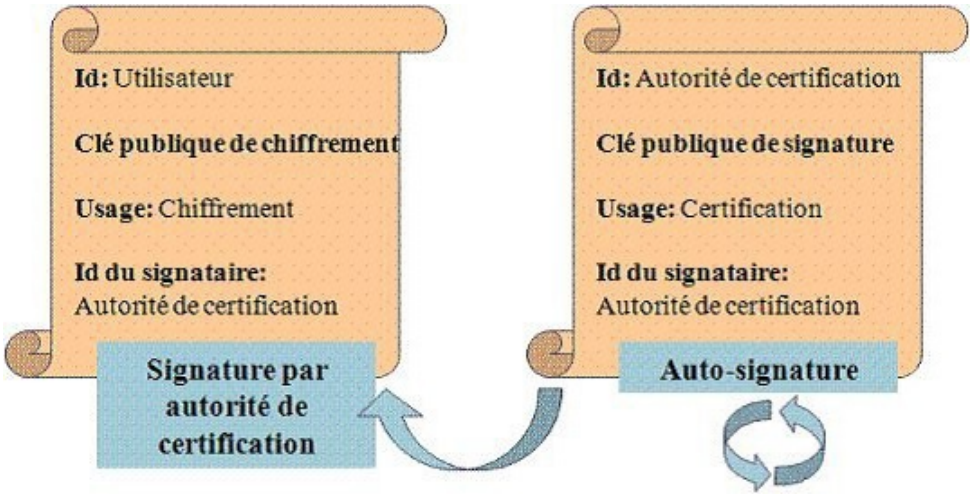

Image 20 : Autorité de certification

Remarque : Auto signature

Une autorité de certification auto-signe son certificat numérique. ceci ne posant pas de problème puisque la clé publique d'une autorité de certification est censée connue d'une manière sécurisée (remise en main propre pas exemple).

Autorité de certification et confiance

L'autorité de certification certifie la correspondance Clé publique – Identité pour l'ensemble d'une population. Ceci mène à faire régner la confiance par transitivité :

- A fait confiance à l'Autorité de Certification
- L'Autorité de Certification délivre un certificat à B
- A est assuré de l'identité de B

3. PKI : Infrastructure à clés publiques

Définition : Infrastructure à clés publiques

« Ensemble de composants, fonctions et procédures dédié à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique ». [Politique de certification type: Ministère de l'Economie, des Finances et de l'Industrie, Fr]

Méthode : Cycle de vie d'un certificat

La figure suivante illustre le cycle de vie d'un certificat de sa délivrance et à sa destruction

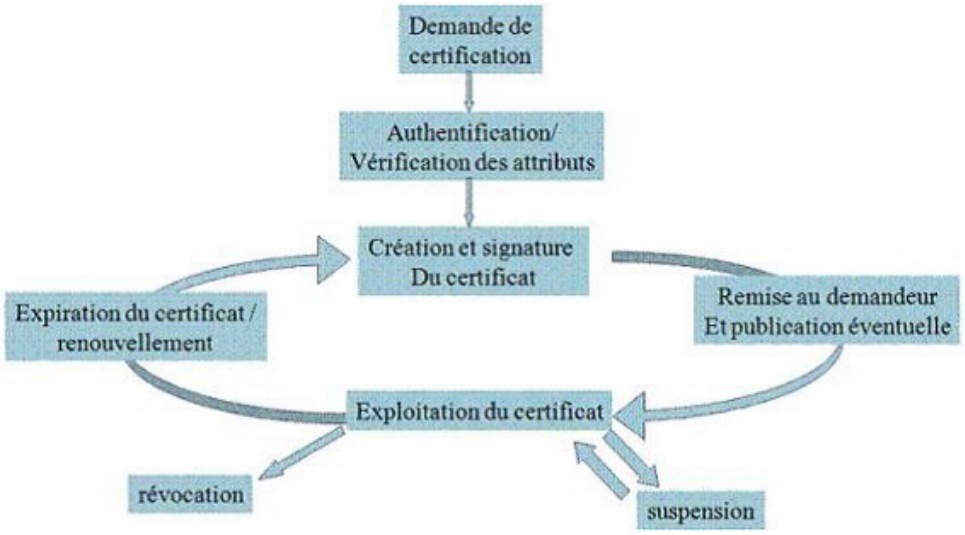

Image 21 : Cycle de vie d'un certificat numérique

Fonctions d'une PKI

Enregistrer et vérifier les demandes de certificats

- Autorité d'enregistrement

Créer et distribuer des certificats

- Autorité de certification

Vérification de validité de certificats

- Autorité de validation

Gérer à tout moment l'état des certificats et prendre en compte leur révocation

- Dépôt de listes de certificats révoqués – CRL (Certificate Revocation List)

Publier les certificats dans un dépôt

- Dépôt de certificats (Annuaire)

Modèles de confiance dans les PKI

Modèle monopoliste

- Une CA pour tout le monde

Modèle monopoliste avec Autorités d'enregistrement

- Une CA avec plusieurs RAs pour la vérification des identités, ...

Délégation de pouvoir de certification

- Une CA délègue le pouvoir de certification à d'autres entités qui deviennent CA à leur tour, en leur fournissant un certificat qui certifie leur capacité d'être CA.

Modèle oligarchique

- Déploiement des produits (comme les navigateur web) avec plusieurs entités de confiance qui sont des CA. Le navigateur fera confiance à tout certificat signé par l'une de ces CA dans sa liste

Modèle anarchique

- Chaque utilisateur établit la liste des entités à qui il fait confiance

Validation de certificat

Pour pouvoir se fier au contenu d'un certificat, il est nécessaire de réaliser les vérifications suivantes:

Vérification	Commentaire
Signature de l'AC	L'application doit vérifier que le certificat est intègre et authentique
Chemin de certification	L'application doit vérifier qu'il existe une chaîne de certificats valide permettant de remonter à une AV de confiance
Période de validité	L'application doit vérifier que le certificat présenté n'est pas expiré
Statut du certificat	L'application doit vérifier que le certificat n'est pas révoqué (ni suspendu)

Tableau 1 : Validation d'un certificat numérique

Il existe par ailleurs différents moyens et techniques standards pour offrir ce service

- Vérification du statut du certificat par récupération régulière de CRL
- Vérification du statut du certificat en ligne : OCSP (On-line Certificate Status Protocol)
- Vérification complète du certificat en ligne : SCVP (Simple Certificate Validation Protocol)

Image 22 : Protocoles de vérification de certificats

⚠ *Attention : Révocation de certificats*

Un certificat peut être révoqué. La révocation intervient quand la fin de validité réelle précède la fin de validité prévue. La révocation peut avoir plusieurs motifs :

- Compromission réelle ou suspectée de la clé privée
- Modification d'un au moins de attributs certifiés
- Perte de la clé privée (effacement d'un disque dur, perte ou détérioration d'une carte à puce, oubli du code PIN, ...)
- Évolution de l'état de l'art cryptographique (la cryptanalyse de la clé privée entre dans le domaine du possible)
- Perte de confiance vis-à-vis d'un acteur ou d'un composant de la PKI

Le demandeur doit être habilité et authentifié

- Le propriétaire du certificat
- Son supérieur hiérarchique
- Le service de gestion du personnel ...

La méthode de révocation dépend de la méthode de validation

- Utilisation d'annuaire « positif » ==> La révocation consiste à enlever le certificat révoqué de l'annuaire
- Utilisation d'un annuaire « négatif » ou CRL ==> La révocation consiste à inscrire le certificat dans une liste de révocation de certificat

Remarque : La gestion des CRL

La gestion des CRL peut devenir complexe et lourde :

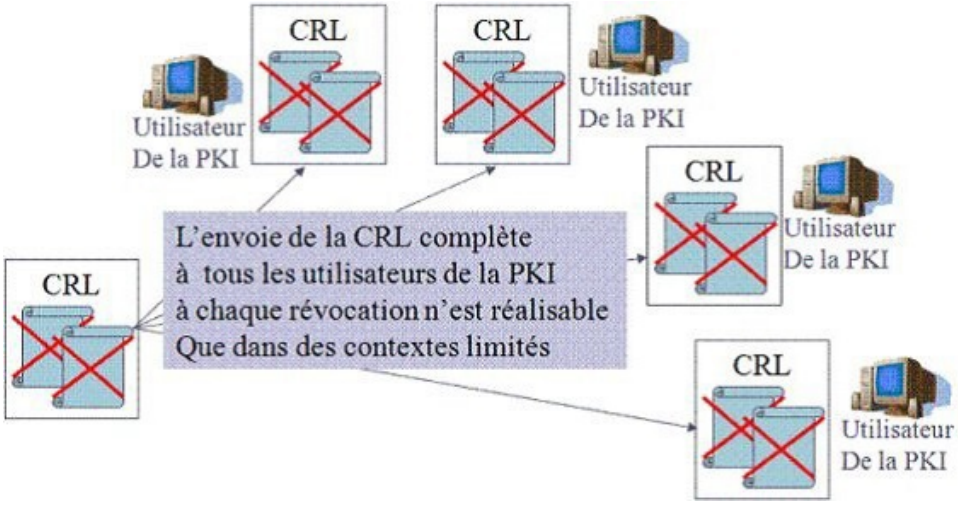

Image 23 : Gestion des CRL

Les delta CRL ne contiennent que les changements depuis la dernière diffusion :

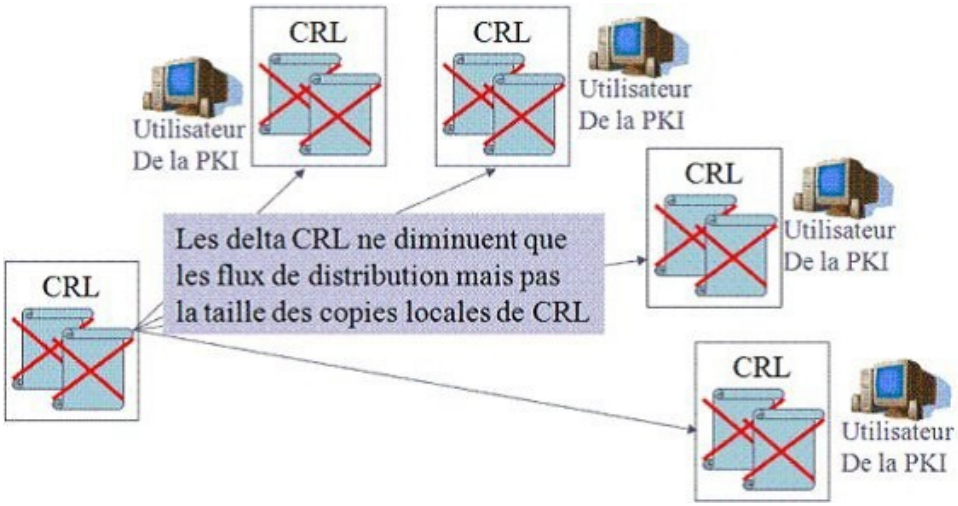

Image 24 : Gestion des delta CRL

Fondamental : Schéma fonctionnel simplifié d'une PKI

En résumé, voici les différents composants d'une PKI :

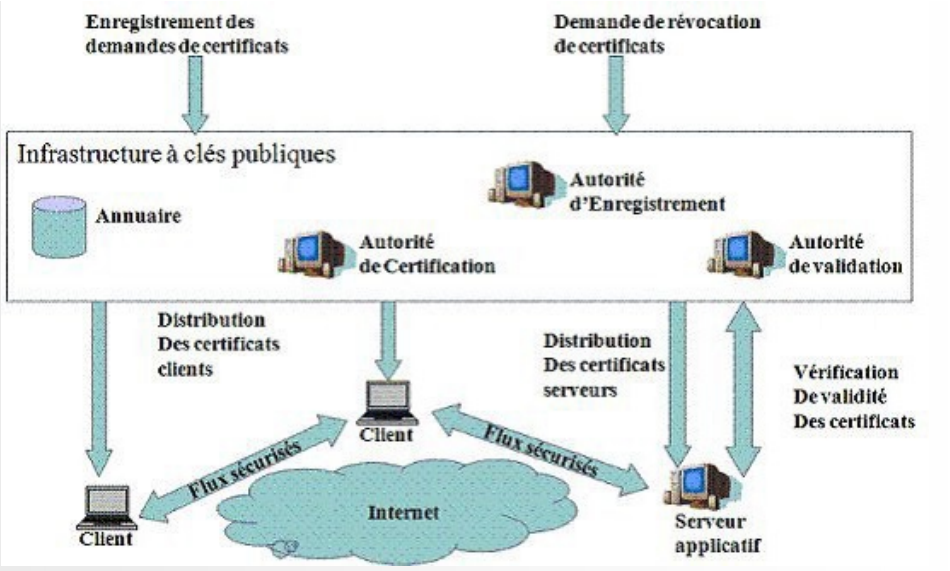

Image 25 : Schéma fonctionnel d'une PKI

4. Secure Socket Layer : SSL

Aperçus générale

SSL/TLS est un protocole de sécurisation des échanges développé par Netscape. Il assure les transactions Client / Serveur sur Internet. Il a été intégré dans les navigateurs web depuis 1994. La vesrion 3.1 est baptisée Transport Layer Security TLS. Cette version a été standardisée à l'IETF: RFC 2246. Le protocole fonctionne au dessus de la couche TCP

Services de sécurité assurés par SSL

Confidentialité

- Obtenue par chiffrement symétrique

Intégrité

- En utilisant des MAC : MD5(128 bits), SHA1(160 bits)

Authentification

- Identification des deux entités (client optionnel) basée sur les certificats X.509
- Authentification de l'origine des données basée sur des MAC

Sous protocoles de SSL

SSL se déroule selon quatre sous protocoles

1. Handshake
    - Authentification mutuelle
    - Négociation des algorithmes de chiffrement et de hachage
    - Échange des clés symétriques
2. Change Cipher Spec

- Indiques la mise en place des algorithmes de chiffrement négocié

3. Record
   - Garantir la confidentialité à l'aide du chiffrement, et L'authentification à l'aide de condensât
4. Alert
   - Émission de messages d'alertes suites aux erreurs que peuvent s'envoyer le client et le serveur

Déroulement du protocole SSL

SSL se déroule en deux phases

1. Phase 1: authentification du serveur
   - Requête client
   - Le serveur envoie son certificat et une liste d'algo de crypto à négocier
   - Le client vérifie le certificat du serveur à l'aide de la clé publique du CA contenu dans le navigateur
   - Le client génère un pré-master secret (PMS)(48 octets) qui sera utilisé pour générer le master-key (48 octets).
   - PMS est chiffré avec la clé publique du serveur
   - Les données échangées entre le client et le serveur seront chiffrées et authentifiées avec des clés dérivées du master-secret
2. Phase 2: authentification du client
   - Le serveur peut demander au client de s'authentifier en lui demandant son certificat
   - Le client répond en envoyant son certificat puis en signant un message avec sa clé privé (contient des info sur la session et le contenu des messages précédents)

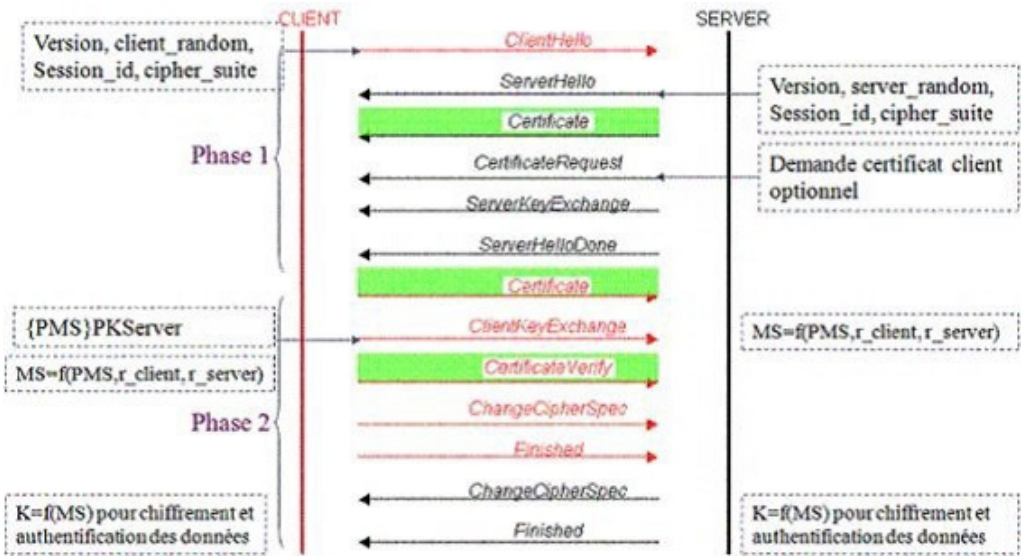

Image 26 : Le protocole SSL/TLS