# CHAPITRE 4 : Infrastructure de gestion des clés

Afin de mettre en œuvre les mécanismes nécessaires à la réalisation des systèmes de chiffrement asymétriques, des infrastructures de gestion de clés (ou PKI : public Key Infrastructure) qui assurent la gestion et la distribution des clés sont nécessaires.
Effectivement, il est impossible de mémoriser l'ensemble des clés publiques de tous les correspondants potentiels d'un site Internet. Leur demander préalablement à chaque envoi ne serait pas optimal. L'IGC (ou PKI) permet de répondre à la nécessité de disposer des clés de chiffrement afin de mettre en œuvre un système de chiffrement asymétrique à clé publique.

## 4.1 Les principales fonctions :

- La génération d'un couple de clés (clé privée, clé publique), son attribution à une entité et la sauvegarde des informations nécessaires à sa gestion : archivage, procédure de recouvrement en cas de perte ou de demande de mise à disposition pour les autorités judiciaires.
- La gestion des certificats numériques : création, signature, émission, validation, révocation ou renouvellement de certificats.
- La diffusion des clés publiques aux ressources qui les solliciteraient et qui seraient habiletés à l'obtenir.
- La certification des clés publiques (signature des certificats numériques)

## 4.2 Architecture de l'infrastructure de gestion des clés :

a. Autorité d'Enregistrement (Registration Authority : RA) : vérifie l'identité des utilisateurs et soumet les demandes de certificats à l'autorité de certification.
b. Autorité de certification (Certification Authority : CA) :est chargée de générer des certificats en associant l'identité d'une personne ou d'un système ç une signature numérique.
c. Opérateur de certification : est chargé de distribuer les certificats par l'intermédiaire d'un annuaire LDAP ou d'un serveur habileté. Les certificats peuvent être enregistrés sur des dispositifs physiques tels que : carte à puce ou clé usb.

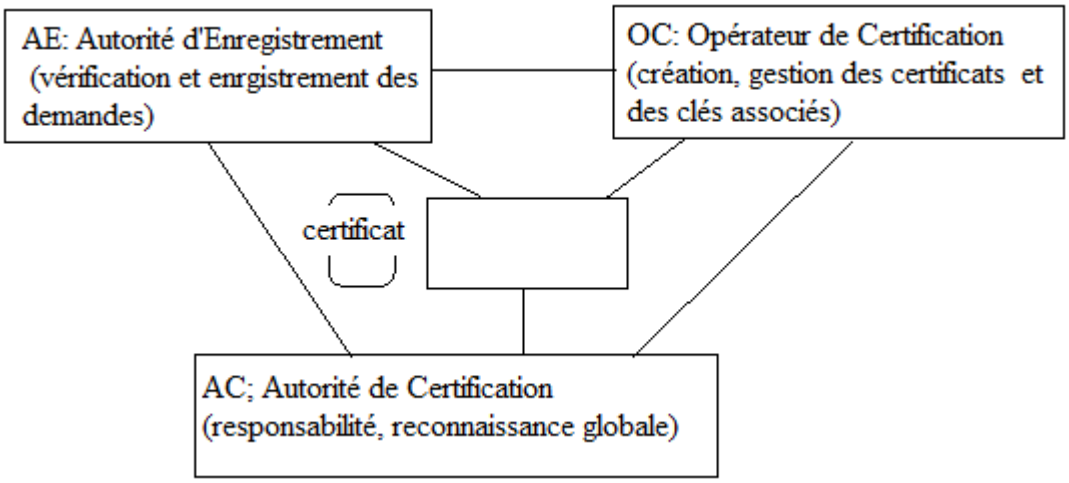



Figure 4.1 Architecture PKI

L'utilisation de couple de clés entraine la nécessité de publication en toute confiance de la clé publique. La PKI offrir l'assurance que :

- La clé est bien celle appartenant à la personne avec qui les échanges sont envisagés.
- La possession de cette clé est digne de confiance.
- La clé est toujours valide.

La confiance st obtenue en associant au couple (clé publique, clé privée) un certificat délivré et géré per une entité elle-même de confiance.
Un client émet une demande d'enregistrement (demande de certification) auprès d'une autorité de certification. Des preuves de l'identité du client sont demandées par l'autorité 'enregistrement. Après la validation des données, l'autorité de certification génère les clés de chiffrement et construit un certificat numérique au nom du client, signe avec sa clé privée le certificat numérique et envoie le certificat au client. Ce dernier utilisera la clé publique de l'autorité pour s'assurer que le certificat est bien produit par l'autorité en question.

### 4.2.1 Certificat numérique :

C'est un document numérique, résulta d'un traitement fixant les relations qui existent entre la clé publique, son propriétaire et l'organisme qui l'a émis. Il constitue la carte d'identité numérique d'une entité (personne morale ou physique) ou d'une ressource informatique à qui il appartient. Il contient entre autre, l'identification de son propriétaire, la clé publique qui lui est attribuée ainsi que l'identification de l'organisme qui l'a délivré.

- Pour une personne : il prouve l'identité de la personne au même titre que la carte d'identité
- Pour une application : il assure que celle-ci n'a pas été détournée de ses fonctions.
- Pour un site : il offre la garantie lors d'un accès à celui-ci que l'on est bien sur le site auquel on veut accéder.

| |
|---|
| Version du certificat |
| Numéro de série |
| Algorithme utilisé pour signer le certificat |
| Nom de l'organisme qui a généré le certificat |
| Période de validité |
| Nom du propriétaire du certificat |
| Clé publique du propriétaire |
| Informations additionnelles concernant le propriétaire, les mécanismes de chiffrement |
| Signature du certificat : algorithme et paramètres utilisés pour la signature ainsi que la signature |

Figure 4.2 : certificat numérique X509

**Remarque :** pour valider le certificat reçu, le client doit obtenir la clé publique de l'organisme qui a crée le certificat relatif utilisé pour le signer. Cette clé publique est utilisée pour déchiffrer la signature. A l'aide des informations également contenues dans le certificat, le client calcule la valeur du condensé et compare la valeur trouvée avec celle contenue dans le certificat. Si les deux valeurs correspondent, alors le certificat est authentifié. Ensuite, le client s'assure que la période de validité du certificat est correcte.

**Exemple :**
Une entreprise et ses clients veulent s'échanger des données de manière confidentielle. Chacun doit s'assurer qu'il est bien en communication avec son interlocuteur.

L'entreprise doit tout d'abord s'enregistrer auprès d'une autorité de certification qui lui délivre un certificat numérique. Le certificat est publié par la PKI et peut être délivré sur demande à des entités qui souhaitent communiquer avec l'entreprise.

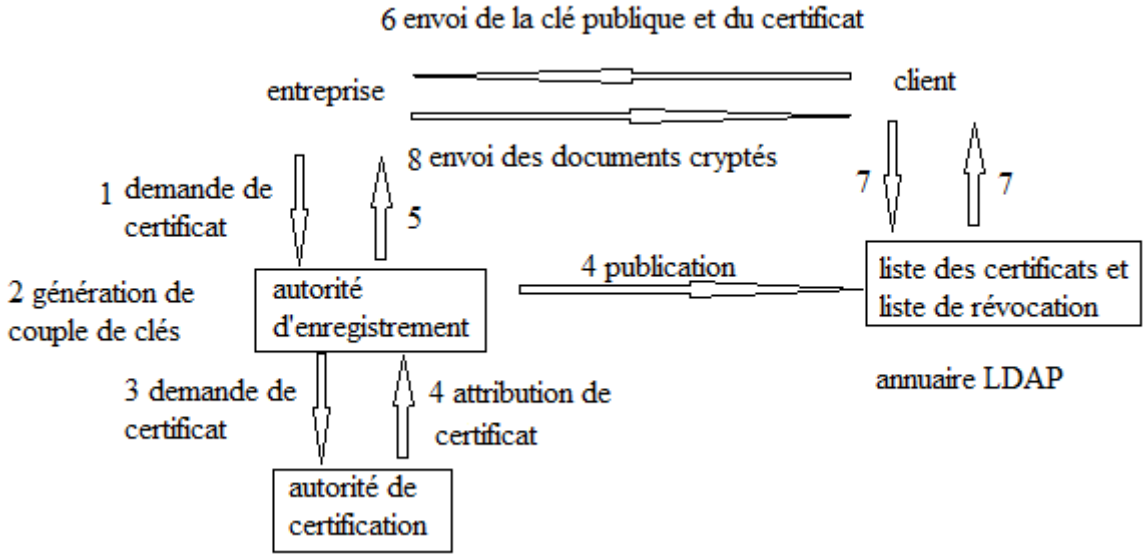


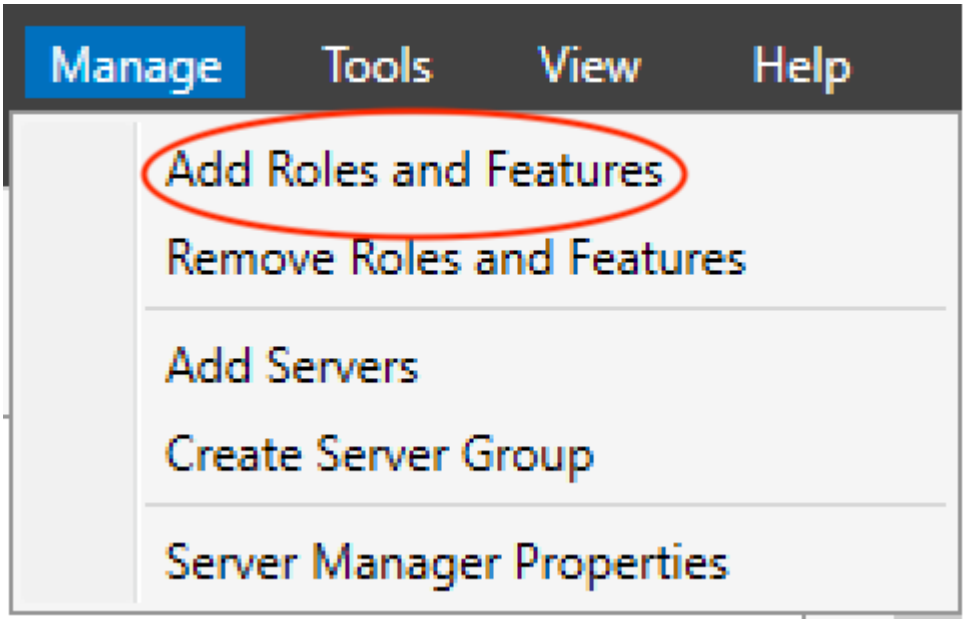

Figure 4.3 transaction sécurisée en utilisant le certificat numérique

Pour réaliser une transaction Internet sécurisée entre un client et l'entreprise, le client se connecte au site de l'entreprise et obtient le nom de la PKI ainsi que la référence du certificat numérique de l'entreprise (numéro de série). Ensuite, il se connecte sur le site de la PKI et télécharge le certificat numérique. Il s'assure de l'authenticité du certificat en vérifiant la signature du certificat avec la clé publique de la PKI. Il s'assure de l'intégrité des données en appliquant l'algorithme de hachage. Enfin il extrait la clé publique de l'entreprise.
Le client génère ensuite une clé de session puis l'envoie en la chiffrant avec la clé publique de l'entreprise. A sa réception, l'entreprise utilise sa lé privée et obtient la clé de session qu'elle utilisera pour chiffrer/déchiffrer les données échangées avec le client durant toute la session.

**4.3 Installation d'autorité de certification sur windows serveur 2016 :**
Pour réaliser l'installation d'une autorité de certification sur windwos serveur 2016, il faut suivre la procédure suivante :

1. Ouvrez une session en tant que membre du groupe Administrateurs de l'entreprise et du groupe Admins du domaine du domaine racine.
2. Dans le Gestionnaire de serveur, cliquez sur **Gérer**, puis sur **Ajouter des rôles et des fonctionnalités**. L'Assistant Ajout de rôles et de fonctionnalités s'ouvre.
3. Dans **Avant de commencer**, cliquez sur **Suivant**.
4. Dans **Sélectionner le type d'installation**, vérifiez que **Installation basée sur un rôle ou une fonctionnalité** est sélectionné, puis cliquez sur **Suivant**.
5. Dans **Sélectionner le serveur de destination**, vérifiez que **Sélectionner un serveur du pool de serveurs** est sélectionné. Dans **Pool de serveurs**, vérifiez que l'ordinateur local est sélectionné. Cliquez sur **Suivant**.
6. Dans **Sélectionner des rôles de serveurs**, dans **rôles**, sélectionnez Active Directory les **services de certificats**. Lorsque vous êtes invité à ajouter les

fonctionnalités requises, cliquez sur **Ajouter des fonctionnalités**, puis sur **suivant**.


7. Dans **Sélectionner des fonctionnalités**, cliquez sur **suivant**.
8. Dans **Active Directory les services de certificats**, lisez les informations fournies, puis cliquez sur **suivant**.
9. Dans **Confirmer les sélections pour l'installation**, cliquez sur **Installer**. Ne fermez pas l'Assistant pendant le processus d'installation. Une fois l'installation terminée, cliquez sur **configurer Active Directory les services de certificats**

**sur le serveur de destination**. L'Assistant Configuration des services AD CS s'ouvre. Lisez les informations d'identification et, si nécessaire, fournissez les informations d'identification d'un compte membre du groupe administrateurs de l'entreprise. Cliquez sur **Suivant**.

10. Dans **services de rôle**, cliquez sur **autorité de certification**, puis sur **suivant**.
11. Sur la page **type d'installation** , vérifiez que l'option **autorité de certification d'entreprise** est sélectionnée, puis cliquez sur **suivant**.
12. Dans la page **spécifier le type de l'autorité de certification** , vérifiez que **autorité de certification racine** est sélectionné, puis cliquez sur **suivant**.
13. Dans la page **spécifier le type de la clé privée** , vérifiez que l'option **créer une nouvelle clé privée** est sélectionnée, puis cliquez sur **suivant**.
14. Dans la page **chiffrement pour l'autorité de certification** , conservez les paramètres par défaut pour CSP (**RSA # Microsoft Software Key Storage Provider**) et algorithme de hachage (**SHA2**), et déterminez la meilleure longueur de clé pour votre déploiement. Les longueurs de caractères clés offrent une sécurité optimale ; Toutefois, ils peuvent avoir un impact sur les performances du serveur et peuvent ne pas être compatibles avec les applications héritées. Il est recommandé de conserver le paramètre par défaut 2048. Cliquez sur **Suivant**.
15. Dans la page nom de l' **autorité de certification** , conservez le nom commun suggéré pour l'autorité de certification ou modifiez le nom en fonction de vos besoins. Assurez-vous que le nom de l'autorité de certification est compatible avec vos conventions d'affectation de noms et à vos objectifs, car vous ne pouvez pas modifier le nom de l'autorité de certification après avoir installé les services AD CS. Cliquez sur **Suivant**.
16. Sur la page **période de validité** , dans **spécifier la période de validité**, tapez le nombre et sélectionnez une valeur de temps (années, mois, semaines ou jours). Le paramètre par défaut de cinq ans est recommandé. Cliquez sur **Suivant**.
17. Dans la page **base de données de l'autorité de certification** , dans **Spécifiez les emplacements des bases** de données, spécifiez l'emplacement du dossier pour la base de données de certificats et le journal de la base de données Si vous spécifiez des emplacements autres que les emplacements par défaut, assurez-vous que les dossiers sont sécurisés à l'aide de listes de contrôle d'accès (ACL) qui empêchent les utilisateurs ou les ordinateurs non autorisés d'accéder à la base de données et aux fichiers journaux de l'autorité de certification. Cliquez sur **Suivant**.
18. Dans **confirmation**, cliquez sur **configurer** pour appliquer vos sélections, puis cliquez sur **Fermer**.