# Introduction

Un certificat est un document signé numériquement au format X.509. Un certificat permet principalement à identifier et à garantir l’authenticité d’un objet.

Il comporte généralement plusieurs champs, dont les suivants :

* **Subject** – propriétaire
* **Public Key** – clé publique associée au propriétaire
* **Dates NotBefore et NotAfter** – définissant la durée de validité
* **Serial Number** – numéro de série donné par le CA
* **Issuer** – émetteur du certificat (en général le CA)
* **SubjectAlternativeName** – noms alternatif du propriétaire
* **Basic Constraints** – identifie si le certificat est un CA ou non et les contraintes liées
* **Extended Key Usages (EKUs)** – définit par des identifiants d’objet (OIDs), ils permettent de définir simplement comment le certificat va être utilisé. Voici les plus communs :
  + Signature de code (OID 1.3.6.1.5.5.7.3.3)
  + Chiffrement de fichier (OID 1.3.6.1.4.1.311.10.3.4)
  + Sécurisation de courriel (OID 1.3.6.1.5.5.7.3.4)
  + Authentification client (OID 1.3.6.1.5.5.7.3.2)
  + Authentification serveur (OID 1.3.6.1.5.5.7.3.1)
* **Signature Algorithm**
* **Signature** – permettant de certifier le certificat à l’aide de la clef privé de l’émetteur du contrat

Une Autorité de Certification dite CA est une entité responsable de l'émission et de la gestion des certificats de sécurité. Lorsque l’on parle de certificats CAs, on parle alors des certificats qui sont responsables et autorisés à être source d’émission et de validation de l'identité pour d'autres certificats.

# Délivrance de certificat dans l’AD

Dans l’A.D., les serveurs Services de certificats Active Directory (AD CS) sont responsables de l’émission et la gestion des certificats. AD CS définit les certificats CAs de confiance dans quatre conteneurs à la localisation :

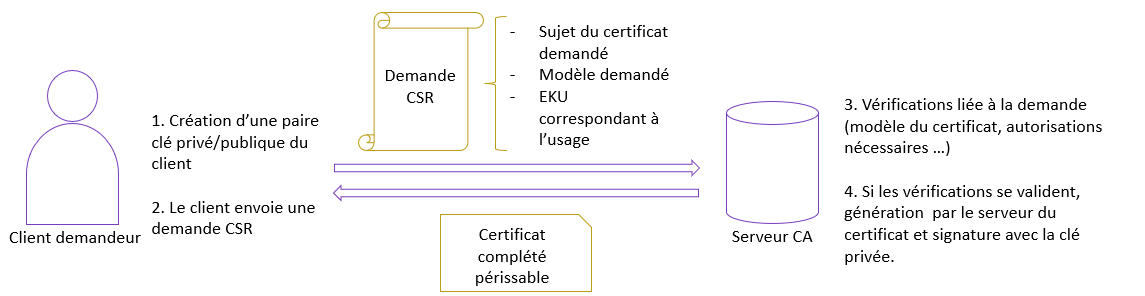
CN=Public Key Services, CN=Services, CN=Configuration, DC=<DOMAIN>, DC=<COM>

Afin de standardiser, on met en place des modèles des certificats. Ceux-ci permettent aussi la classification des certificats selon leurs usages :

* Ils permettent aussi le pré-remplissage de certains paramètres : période de validité, période de renouvellement.
* Ces objets de l’AD définissent aussi les listes de contrôle d’accès (ACL) pour l’utilisation (demande de déploiement) et la modification du modèle.
* Pour prédéfinir les usages des certificats issus de ce modèle, il est possible de renseigner le champ *pKIExtendedKeyUsage* avec un tableau des OIDs possibles.

Les autorités de certification sont chargées de délivrer des certificats. Lors de sa création, l'autorité de certification doit d'abord créer sa propre paire de clés privée-publique.

L'autorité de certification génère ensuite son propre certificat d'autorité de certification racine en signant un nouveau certificat à l'aide de sa clé privée (le certificat d'autorité de certification racine est donc autosigné).

Une fois les CAs harmonisés, les clients en demande de certificats passent par un processus d’inscription. Le processus précis varie en fonctions des CAs mais certaines étapes restent constantes.

Premièrement, le client génère sa propre paire de clés publique-privée ; et envoie sa clé publique via une demande CSR (Certificate Signing Request). Cette demande inclut aussi le sujet du certificat demandé, nom du modèle requis ainsi que l’EKU correspondant à l’usage. La demande devra alors être signée avec la clef privé du demandeur et envoyée au serveur de gestion des certificats. Celui-ci vérifie la requête et l’identité du demandeur via la signature. Il vérifie aussi que le modèle demandé corresponde à l’utilisation mais aussi qu’il donne l’autorisation au demandeur d’y faire appel.

Si les vérifications sont validées, le serveur répond avec un certificat généré sur la base du modèle demandé complété à l’aide des informations fournies ainsi que la signature issue de la clé privée du CA