Module : *Cryptographie*
Enseignante : *Ihsen NAKOURI*
Classes : *ING-4-SSIR*
2025-2026

TEK-UP
Ecole Supérieure Privée
Technologie & Ingénierie

TP : Mise en place d'une PKI

Objectif du TP

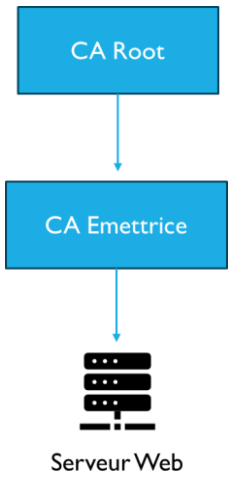
L'objectif de ce TP est de simuler la création et la gestion d'une Infrastructure à Clé Publique (PKI) complète, en utilisant l'outil en ligne de commande OpenSSL.
A la fin de ce TP, l'étudiant devra être capable de :

- Comprendre le rôle et les composants d'une PKI.
- Comprendre le rôle des CA Racines et des CA Emettrices (Issuing CA).
- Mettre en place une chaîne de confiance (Root CA signe Issuing CA, Issuing CA signe Serveur).
- Gérer les certificats et la révocation au niveau de la CA Emettrice.

Architecture

Nous allons mettre en place les trois composantes suivantes :

1. **Autorité de Certification Racine (Root CA)** : L'autorité principale, auto-signée. Son rôle est uniquement de signer la CA émettrice.
2. **Autorité de Certification émettrice (Issuing CA)** : Le maillon intermédiaire. Son rôle est de signer les certificats des entités finales (serveurs/utilisateurs) et de gérer la révocation.
3. **Serveur Web (Server)** : L'entité finale qui utilisera son certificat pour sécuriser les communications HTTPS.



Partie 1 : Préparation de la structure de fichiers

Il s'agit dans cette partie de créer une structure de répertoires pour simuler les environnements distincts de la Root CA et de l'Issuing CA.

1.1. Créez un dossier principal : mkdir PKI_TP
1.2. Créez les structures de dossiers/fichiers pour la Root CA (root_ca/) : certs, private, crl, newcerts, index.txt (vide), serial (contenant 1000).
1.3. Créez les structures de dossiers/fichiers pour l'Issuing CA (issuing_ca/) : certs, private, crl, newcerts, index.txt (vide), serial (contenant 2000).
1.4. Créez le répertoire pour le serveur : PKI_TP /server.

Partie 2 : Création de l'Autorité de Certification Racine (Root CA)

2.1. Générez une clé privée RSA de 4096 bits chiffrée. Enregistrez-la dans root_ca/private/ca_root.key.pem.
2.2. Génération du certificat de la Root CA (Auto-signé) :

- Créez un certificat X.509 auto-signé (ca_root.crt.pem) valide pour 10 ans.
- Common Name (CN): PKI Root Authority.

Partie 3 : Création et Signature de l'Autorité de Certification Emettrice (Issuing CA)

3.1. Générer une clé privée RSA de 2048 bits chiffrée. Enregistrez-la dans *issuing_ca/private/ca_issuing.key.pem*.

3.2. Générer une CSR (*ca_issuing.csr.pem*) pour l'issuing CA. CSR est la requête de signature.

- *Common Name (CN) : PKI Issuing Authority*.

3.3. La Root CA signe la CSR de l'Issuing CA. Le certificat final (*ca_issuing.crt.pem,* à placer dans *issuing_ca/certs/)* et doit être valide pour 5 ans.
Il faut s'assurer d'inclure les extensions spécifiant qu'il s'agit d'une CA capable de signer d'autres certificats (*basicConstraints=CA : TRUE*).

Phase 4 : Création de la requête et signature pour le Serveur Web

4.1. Générer une clé privée non chiffrée pour le serveur. Enregistrer-la dans *server/server.key.pem*.
4.2. Création de la Requête de Signature (CSR) du Serveur (*server.csr.pem*).

- *Common Name (CN) : www.mon-serveur-securise.com*

4.3. L'Issuing CA utilise sa propre clé et ses fichiers de gestion (*index.txt, serial*) pour signer la CSR du serveur. Le certificat final (*server.crt.pem*, à placer dans server/) doit être valide pour 1 an. Il faut inclure les extensions appropriées pour une entité finale (*e.g., keyUsage et extendedKeyUsage pour un serveur TLS*).