📚 Cours : Certificats et Infrastructures à Clé Publique (PKI)

🔹 1. Définitions de base

- **PKI (Public Key Infrastructure)** : Ensemble de technologies, procédures et personnes permettant de **gérer les clés publiques** et de garantir leur **authenticité**.
- **Certificat numérique** : Fichier électronique signé numériquement, associant une **identité** (nom, adresse, etc.) à une **clé publique**.
- **AC (Autorité de Certification)** : Entité de confiance qui **délivre, valide ou révoque** des certificats.

🔹 2. Contenu d'un certificat numérique (X.509)

Un certificat contient :

- Nom de l'émetteur (Autorité de Certification)
- Nom du propriétaire (utilisateur, serveur, etc.)
- Clé publique du propriétaire
- Dates de validité
- Numéro de série
- Algorithme de signature
- Signature de l'AC

📄 Exemple : certificat SSL d'un site web HTTPS

🔑 3. Fonctionnement global d'une PKI

1. **Génération de clé** : L'utilisateur génère une paire clé publique / clé privée.
2. **Demande de certificat** (CSR) : Il envoie sa clé publique à une AC.
3. **Validation** : L'AC vérifie l'identité du demandeur.
4. **Signature du certificat** : L'AC signe la clé publique et renvoie le certificat.
5. **Utilisation** : Le certificat est utilisé pour authentifier l'utilisateur ou le serveur.
6. **Vérification** : Les clients vérifient la signature avec la clé publique de l'AC.
7. **Révocation** : Si nécessaire, l'AC peut invalider un certificat via des listes CRL ou OCSP.

🔒 4. Utilité d'une PKI

- **Authentification** : Vérifie l'identité de la source (ex : site web HTTPS).
- **Confidentialité** : Échange sécurisé via le chiffrement asymétrique.
- **Intégrité** : Garantit que le message ou le fichier n'a pas été modifié.
- **Non-répudiation** : Preuve que l'expéditeur est bien l'auteur du message.

🕶 5. Hiérarchie des autorités de certification

- **Racine (Root CA)** : Autorité de certification principale, auto-signée.
- **Intermédiaire (Intermediate CA)** : Délivre des certificats pour les entités finales.
- **Utilisateur final (End Entity)** : Détient un certificat signé.

🔑 Les systèmes d'exploitation et navigateurs contiennent une liste de **root CAs** de confiance.

🛠 6. Outils utilisés avec la PKI

- **OpenSSL** : création de paires de clés, de CSR, de certificats auto-signés.
- **Certbot / Let's Encrypt** : génération automatique de certificats HTTPS.
- **Navigateur** : vérification des certificats SSL/TLS des sites.

⛔ 7. Révocation d'un certificat

Deux méthodes principales :

- **CRL (Certificate Revocation List)** : liste noire périodiquement mise à jour.
- **OCSP (Online Certificate Status Protocol)** : vérification en temps réel du statut d'un certificat.

🔐 8. Exemple de cas d'usage : HTTPS

1. Le navigateur demande une connexion sécurisée.
2. Le serveur envoie son certificat SSL.
3. Le navigateur vérifie que le certificat est :
    - Valide,

    - Signé par une AC reconnue,
    - Non expiré ni révoqué.
4. Une clé de session est échangée de manière chiffrée.
5. La session HTTPS est établie.

🛡 9. Risques et attaques

Risque	Contre-mesure
Faux certificat	Validation stricte de la chaîne
Certificat expiré	Contrôle automatique de validité
Compromission de l'AC	Retrait de la confiance
Phishing avec un certificat valide	Analyse comportementale & DNSSEC

✅ 10. Résumé visuel

- 📄 Un **certificat numérique** est comme une **carte d'identité électronique**.
- 🔐 La **PKI** garantit que la **clé publique appartient bien à la bonne entité**.
- 🌐 Utilisée partout : HTTPS, mails sécurisés, VPN, signatures numériques, etc.
