Exercice 1: Compréhension des certificats

1. Expliquer la différence entre une **clé publique** et une **clé privée**.

2. Donner un exemple concret d'utilisation d'un **certificat numérique** dans la vie quotidienne.

3. Pourquoi une CSR (Certificate Signing Request) doit-elle être signée par le propriétaire de la clé privée ?

Exercice 2: Processus de création de certificats

1. Classer ces étapes dans l'ordre correct :

    - Validation par l'AC
    - Signature de la CSR par le propriétaire
    - Génération des clés
    - Émission du certificat
    - Création de la CSR

2. Expliquer pourquoi l'AC signe le certificat avec sa propre clé privée.

3. Qu'est-ce que cela signifie lorsqu'un certificat peut être vérifié par sa **clé publique** ?

Exercice 3: Hiérarchies d'AC et certificats racine

1. Dessine un schéma simple montrant la hiérarchie : **AC racine** → **AC subordonnée** → **Certificat utilisateur**.

2. Pourquoi la clé privée d'une AC racine doit-elle être protégée **plus strictement** que celle d'une AC subordonnée ?

3. Quelle est la durée de vie typique d'un certificat racine et pourquoi doit-elle être limitée ?

Exercice 4 : Révocation de certificats

1. Explique à quoi sert une **CRL (Certificate Revocation List)**.

2. Donne un exemple de situation où un certificat devrait être révoqué.

3. Pourquoi certains systèmes choisissent de **ne pas vérifier systématiquement** les CRL ?

4. Que se passe-t-il si une CRL expire sans être mise à jour ?

Exercice 5 : Questions de réflexion

1. Si une AC subordonnée est compromise, quelles sont les conséquences sur les certificats qu'elle a émis ?

2. Pourquoi ne peut-on pas révoquer un certificat racine ?

3. Discute des avantages et des inconvénients d'une hiérarchie à plusieurs niveaux d'AC.