03 - Gérer l’inscription de certificats

L’objectif de l’autorité de certification est de permettre aux utilisateurs et aux appareils de s’inscrire à des certificats et de les utiliser. Toutefois, tout comme pour l’implémentation de l’autorité de certification, cela requiert une planification et une préparation soignées qui déterminent le type de certificats qu’une autorité de certification peut émettre.

Qu’est-ce qu’un certificat ?

Un certificat est un petit fichier qui contient plusieurs éléments d’information sur son propriétaire. Ces données peuvent inclure l’adresse e-mail du propriétaire, le nom du propriétaire, le type d’utilisation du certificat, la période de validité et les URL des emplacements AIA et CDP.

Un certificat contient également la clé publique et les métadonnées correspondantes, qui se composent d’une clé privée et de la clé publique correspondante. Vous pouvez utiliser ces clés dans les processus de validation des identités, de signatures numériques et de chiffrement. La paire de clés générée par chaque certificat présente les conditions suivantes :

- Lorsque le contenu est chiffré avec la clé publique, il ne peut être déchiffré qu’avec la clé privée.
- Lorsque le contenu est chiffré avec la clé privée, il ne peut être déchiffré qu’avec la clé publique.
- Aucune autre clé n’est impliquée dans la relation entre les clés d’une paire de clés.
- La clé privée ne peut pas être déduite d’une clé publique dans un laps de temps raisonnable et inversement.

Dans le cadre du processus d’inscription de certificats, le client génère la paire de clés publique/privée. Le client envoie ensuite la clé publique à l’autorité de certification, qui confirme les informations du client, la signe avec sa propre clé privée, puis renvoie le certificat, qui comprend la clé publique du client, au client.

> **Vous pouvez considérer qu’un certificat est comme un permis de conduire. De nombreuses entreprises acceptent le permis de conduire comme une forme d’identification, car elles considèrent l’émetteur du permis (un organisme gouvernemental) comme digne de confiance. Les entreprises connaissant le processus par lequel un utilisateur peut obtenir un permis de conduire, il fait confiance à l’émetteur qui a vérifié l’identité de l’individu avant de délivrer le permis. Par conséquent, le permis de conduire est une forme acceptable et valide d’identification. Un certificat de confiance est établi de la même manière.**

Atelier

Objectif

- Créer un modèle de certificat personnalisé.
- Configurer le modèle afin qu'il puisse être émis.
- Créer un modèle de certificat personnalisé:
  - Bouton droit sur `Modèles de certificats`
    et choisir `Nouveau` puis `Modèle de certificat à déliverer`
  - Choisir le modèle que nous avons créé.
  - Lancer la console `Autorité de certification`
  - Bouton droit sur `Modèles de certificats` pour dupliquer le modèle de serveur web.
  - Dans l'onglet Démonstration `Général`, donner un nom `Production Web Server`, une période de validité d'1 an. Puis `Appliquer`
  - Dans l'onglet `Traitement de la demande`, cocher `Autoriser l'exportation de la clé privée`. Puis `Appliquer` et `Ok`
  - Quitter `Console des modèles de certificat`
- Configurer le modèle afin qu'il puisse être émis.
  - Bouton droit sur `Modèles de certificats`
    et choisir `Nouveau` puis `Modèle de certificat à déliverer`
  - Choisir le modèle que nous avons créé.