TP : PKI

Amel Meddeb Makhlouf
2024-2025

Pour construire le compte rendu, vous répondez aux questions suivantes en donnant à chaque fois la syntaxe et la sémantique de la commande utilisée (si nécessaire) en précisant le rôle de chaque champ de la commande. Vous affichez et commentez aussi le résultat de chaque commande utilisée.

Création du certificat de l'AC

- A l'aide de la commande « openssl », créez une paire de clef privée/publique pour votre machine qui sera autorité de certification. Entre parenthèses seront indiqués les paramètres correspondant dans le fichier de configuration /etc/ssl/openssl.cnf à modifier pour s'adapter à vos noms de fichier.
- Créez un répertoire /var/CA (dir) où vous créerez également les répertoires suivants :
  - certs : (certs) qui contient les certificats valides
  - crl : (crl dir) qui contient la liste des révocations
  - csr : qui contient les requêtes de certification
  - newcerts : qui contient les certificats
  - private : qui contient les clefs privées

    Créez également les fichiers suivants :
  - index.txt : (database) qui contient la liste de tous les certificats de l'AC. (à l'initialisation, créez simplement un fichier index.txt vide).
  - serial : (serial) qui tient à jour le numéro d'index des certificats de l'AC (à l'initialisation, créez simplement un fichier serial contenant la ligne 00).
- Copier le fichier /etc/ssl/openssl.cnf dans votre répertoire /var/CA
- Modifiez le nouveau fichier /var/CA/openssl.cnf pour positionner la localisation de ces fichiers et répertoires que vous venez de créer.
- Travaillez sous le répertoire /var/CA

Pour créer le certificat de l'AC

- Générer une paire de clés RSA cryptée par AES dans private/cakey.pem de taille 2048
- Générer un certificat autosigné par la commande :

- **openssl req -new -x509 -config openssl.cnf –days nbjours -key cakey.pem –out cacert.pem**

Création d'un certificat web

A l'aide de la commande openssl

- générer une paire de clés RSA pour le serveur
- générer une requête de certification en utilisant la commande

openssl req -new –key clefmachine.key -config openssl.cnf –out certificatmachine.csr

Attention, par défaut, l'AC est configuré pour ne certifier que les machines se déclarant dans la même organisation, région et pays. Pour passer outre cette limite, vous modifierez match par optional pour les champs countryName, stateOrPro-vinceName et organizationName dans la rubrique policy match dans le fichier de configuration openssl.cnf

- générer le certificat signé par l'AC que vous avez généré

openssl ca –days nbjours –in certicatmachine.csr –config openssl.cnf –out certicatmachine.crt