HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Enzo Allemano

10/06/2022

Duc Alexandre
Fortunato Filipe

Cryptographie

Rapport laboratoire 4:
Certificat SSL/TLS

Réponse aux questions

Question 1

Eventuellement lorsque la demande de signature est faite sur un serveur qui nécessite le certificat et que la clé est générée sur un système différent.

Un autre cas de cette implémentation, serait lorsque l'on souhaite réutiliser cette clé privée. Mais cela semble être une mauvaise idée. (réutilisation de la clé)

Question 2

Pour simplifier la réalisation du labo j'ai choisi de ne pas chiffrer la clé privé du serveur.

Dans un cas plus concret, il faudrait évidemment chiffrer la clé pour la stocker sur le serveur. Dans quel cas, il faut entrer le password lors du démarrage du serveur pour déchiffrer la clé et ainsi valider le certificat.

Chiffrer la clé est une mesure nécessaire dans le cas où un attaquant parvient à la récupérer.

Question 3

Il est nécessaire pour nginx d'avoir le chemin complet vers le root CA pour vérifier l'authenticité du certificat.

Nécessaire pour les étapes :

- Récupérer le certificat client
- Vérification de la validité avec les CA intermédiaires
- Vérification de la validité avec le root CA

Question 4

Le fichier .db des CAs est appelé « index file », il contient un historique des certificats créé.

Notamment les champs suivants [1]:

- Certificate status flag (V=valid, R=revoked, E=expired).
- Certificate expiration date in YYMMDDHHMMSSZ format.
- Certificate revocation date in YYMMDDHHMMSSZ[,reason] format. Empty if not revoked.
- Certificate serial number in hex.
- Certificate filename or literal string 'unknown'.
- Certificate distinguished name.

La commande «`openssl ca`» utilise ce fichier comme base de données de certificats.

[1] https://pki-tutorial.readthedocs.io/en/latest/cadb.html

Question 5

J'ai pris la configuration de base proposé par https://ssl-config.mozilla.org/ et j'ai adapté à mes besoins.

J'ai notamment changé :

- Le chemin d'accès à ma chaine de certificat
- Le chemin d'accès à ma clé privé du certificat TLS client
- Les ciphersuite utilsées
    - J'ai décidé de ne garder que les ciphersuite qui sont recommandées par https://ciphersuite.info/cs/.

J'ai notamment retiré :

- Les paramètre de configuration de OCSP
- La commande pour générer mes paramètres Diffie-Hellman
    - ECDHE n'utilise pas de `dhparam`

Configuration dans default_nginx.txt