

CRY 2025

Laboratoire #4

03-06-2025

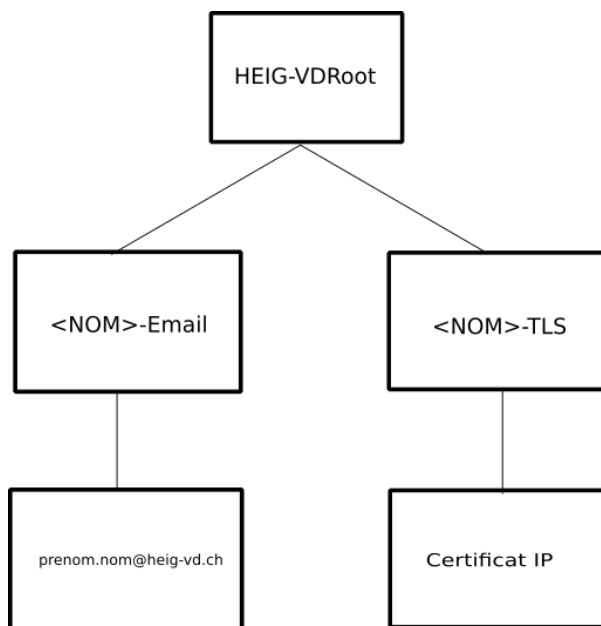
- Si vous utilisez des mots de passe pour sécuriser vos clefs, utilisez le mot de passe **123456**.
- Le rendu est décrit dans la Section 9.
- N'oubliez pas de répondre aux questions de la Section 8.
- Afin de faire le labo à distance, il vous faut utiliser un VPN vers le réseau de l'école.
 - Il est important d'utiliser le VPN à l'URL vpn.iict-heig-vd.ch
- Le laboratoire nécessite de pouvoir utiliser les commandes `openssl`. L'idéal est de le faire depuis Linux mais il est aussi possible de le faire sous Windows.
- Une excellente ressource (gratuite) pour les commandes openssl est l'openssl cookbook : <https://www.feistyduck.com/library/openssl-cookbook/online/>

1 Introduction

Le but de ce laboratoire est d'implémenter une PKI et de l'utiliser pour signer des emails ainsi que pour configurer une connexion HTTPS. Le laboratoire se divise en trois parties :

1. Configuration des CAs.
2. Signatures d'emails.
3. Configuration d'un serveur pour connexion HTTPS.

L'architecture de la PKI aura l'allure suivante avec <NOM>, votre nom de famille :



Le certificat racine HEIG-VDRoot est géré par nous mais vous devrez générer vous même tous les autres certificats.

2 Fichiers Fournis

Nous vous fournissons les fichiers suivants :

- Le certificat racine HEIG-VDRoot.
- Un template de fichier de configuration pour OpenSSL.
- Un mot de passe, une IP et un port afin de vous connecter à votre serveur TLS.

3 Commandes Utiles

Nous allons utiliser `openssl` afin de générer les certificats. Vous trouverez dans cette section toutes les commandes utiles à ce laboratoire.

Créer une nouvelle demande de signature de certificat (CSR). Afin d'obtenir un certificat, il est nécessaire de générer une demande de signature de certificat qui contient toutes les informations du certificat. En particulier, elle va contenir le **common name** du certificat (CN). Cette demande devra ensuite être signée par un CA. Vous pouvez obtenir la CSR (certificate signing request) à l'aide de la commande suivante :

```
openssl req -new -config <FICHIER_CONFIG> -out <OUTPUT_CSR>.csr -keyout <OUTPUT_KEY>.key
```

Le fichier de config pour un certificat intermédiaire vous est fourni mais est incomplet, à vous de le compléter.

Signer un nouveau certificat. Les certificats sont gérés dans une base de donnée qu'il faut initialiser de la manière suivante :

```
touch <NOM_FICHIER>.db  
touch <NOM_FICHIER>.db.attr
```

Finalement, pour signer un certificat, nous utilisons la commande suivante : ¹

```
openssl ca -config <FICHIER_CONFIG> -in <INPUT_CSR> \  
-out <OUTPUT_CERTIFICAT>.crt -create_serial
```

Il est possible d'y ajouter une extension avec l'option `-extensions`. Pour obtenir un certificat auto-signé, ajoutez l'option `-selfsign`.

Visualiser un certificat. Pour visualiser un certificat dans le terminal, il faut utiliser la commande suivante :

```
openssl x509 -noout -text -in <CERTIFICAT>
```

Obtention d'une chaîne de certificats. Il est parfois nécessaire d'utiliser une chaîne de certificats. C'est typiquement le cas pour TLS, qui fournit les certificats intermédiaires en plus du certificat final afin de pouvoir tester facilement tous les certificats utilisés. Une chaîne de certificats est simplement la **concaténation** des certificats. Vous pouvez utiliser la commande suivante pour obtenir une chaîne de certificats :

```
cat <CERTIF_CLIENT> <CERTIF_INTERMEDIAIRE> > <CERTIF_CHAIN>.crt
```

Exporter un certificat en format PKCS#12. Le format PKCS#12 permet de combiner dans un même fichier le certificat et la clef privée associée. Il est typiquement utilisé pour signer des messages. Il va aussi parfois contenir une chaîne de certificats (dans notre cas, le certificat racine ainsi que le certificat intermédiaire). Afin d'exporter une clef et un certificat en PKCS#12, utilisez la commande suivante :

```
openssl pkcs12 -export -name <NOM> -inkey <CLEF> \  
-in <CERTIFICAT> -certfile <CHAIN> -out <FILE>.p12
```

La variable `<NOM>` sert uniquement à identifier le certificat de manière lisible.

1. Le `\` indique un retour à la ligne dans la commande et peut-être supprimé

4 Certificats Intermédiaires

La première étape de ce laboratoire va consister en l'obtention de certificats intermédiaires. Le premier est le certificat d'une CA qui sera utilisée pour signer des certificats utilisés pour les emails. Le second est le certificat d'une CA qui sera utilisée pour signer des certificats utilisés pour des connexions TLS.

1. Créez des CSR correspondant aux deux CA intermédiaires. Le *common name* doit correspondre au schéma de la Section 1, le *pays* doit être CH et *l'organisation* HEIG-VD.
2. Faites signer le certificat par notre CA racine en utilisant l'interface située à l'adresse <https://secuctfd.iict-heig-vd.in>. Faites-y un simple copier-coller **du contenu** de votre CSR. **Très important** : ce serveur n'est accessible uniquement par VPN ou depuis le réseau de l'école.
3. Enregistrez le résultat dans un fichier `.crt` qui contiendra le certificat signé.
4. À la fin de cette étape, vous devez avoir un certificat ainsi qu'une clef privée pour chacune de deux CA.

5 Signatures des emails

Le but de cette étape va être d'envoyer un mail à alexandre.duc@heig-vd.ch signé par un certificat attestant de votre adresse email. Nous conseillons d'utiliser Thunderbird² pour envoyer l'email mais tout autre client mail acceptant le format S/MIME est autorisé. Concernant la configuration de Thunderbird, vous aurez besoin des paramètres suivants pour accéder à votre boîte mail HEIG-VD :

— **Reception** : outlook.office365.com port 993, Connection security SSL/TLS, Authentication OAuth2

— **Envoi** : smtp.office365.com, port 587, Connection security STARTTLS, Authentication OAuth2

Pour signer les emails, vous allez devoir effectuer les étapes suivantes :

1. Créez une CSR correspondant à votre certificat client. Attention au champ email !
2. Signez votre CSR avec votre CA intermédiaire utilisée pour les emails.
3. Configurez Thunderbird afin de le connecter à votre compte mail HEIG-VD.
4. Créez une chaîne de certificats comprenant le certificat racine et votre certificat intermédiaire utilisé pour les emails.
5. Créez un bundle PKCS#12 comportant votre clef privée, votre certificat client, et la chaîne de certificats du point précédent.
6. Vous pouvez gérer les certificats dans les *settings*.
7. Ajoutez y le certificat racine puis votre certificat client.
8. Allez ensuite dans les paramètres de votre compte pour choisir quelle clef vous souhaitez utiliser pour signer vos messages.
9. Envoyez le mail. N'oubliez pas de le signer !

2. <https://www.thunderbird.net>

6 Configuration d'un serveur TLS

Le but de cette étape va être de configurer un serveur nginx afin de visualiser de manière sûre une page en HTTPS.³ Nous allons utiliser TLS 1.2 et 1.3 pour effectuer la connexion HTTPS.⁴ En particulier, la configuration du serveur sera très importante : aucune ciphersuite vulnérable n'est autorisée !

Vous avez reçu l'IP et le port de votre serveur ainsi que les credentials de connexion qui vous permettront de vous connecter via SSH sur le serveur. **Très important** : le serveur n'est accessible uniquement via VPN de l'IICT. Le nom d'utilisateur sera **labo**. Vous pouvez donc vous connecter avec la commande :

```
ssh -p PORT labo@secuctfd.iict-heig-vd.in
```

Si vous souhaitez copier un fichier de votre machine vers la machine remote, vous pouvez utiliser **scp** de la manière suivante :

```
scp -P PORT FICHIER_LOCAL labo@secuctfd.iict-heig-vd.in:CHEMIN_SERVEUR
```

Nous allons faire ceci à l'aide des étapes suivantes :

1. Créez une CSR correspondant à votre certificat client.
2. Signez votre CSR avec votre CA intermédiaire utilisée pour TLS.
3. Connectez-vous à votre serveur web.
4. Configurez nginx afin d'avoir une connexion HTTPS sûre. Le fichier à configurer se trouve sur le serveur à `/etc/nginx/sites-available/default`. Ce fichier n'est modifiable uniquement en tant que root. Vous pouvez utiliser la commande `sudo` pour cela. Pour configurer TLS, vous pouvez vous aider du lien suivant : <https://ssl-config.mozilla.org>.⁵
 - Pour tester la syntaxe de la configuration nginx déployée, utilisez la commande `nginx -t`
 - Pour recharger une nouvelle configuration, utilisez la commande `nginx -s reload`
5. Vous pouvez tester votre connexion depuis le browser.

7 Test du serveur TLS

Testez votre serveur TLS à l'aide de l'outil `testssl` (<https://testssl.sh/>). Fournissez dans votre rapport le résultat du scan et commentez le, si nécessaire.

3. La page web est une blague d'un ancien assistant et ne doit pas être prise sérieusement.
4. **Attention** : la connexion TLS 1.2 doit être aussi activée !
5. Note : nous n'activerons pas l'OCSP stapling.

8 Questions

Répondez dans votre rapport aux questions suivantes :

1. Pourquoi devons nous transmettre une chaîne de certificats dans les deux applications (email et TLS) ?
2. Comment avez-vous configuré nginx ? Donnez votre fichier de configuration.
3. Fournissez le résultat du scan de `testssl` sur votre serveur ainsi que des commentaires, si nécessaire.
4. Quelle durée de validité avez-vous choisie pour le certificat du serveur TLS ? Pourquoi ? Comment cette durée va-t-elle évoluer dans un futur proche ?

9 Rendu

Vous serez évalués sur les points suivants :

1. Mail envoyé.
2. Configuration correcte du serveur TLS.
3. Petit rapport répondant aux questions de la Section 8.
4. Fichiers générés dans le laboratoire en suivant **l'arborescence suivante**⁶ :

```
├── mail_CA
│   ├── config.conf
│   ├── <NOM>-Email.crt
│   ├── <NOM>-Email.csr
│   └── <NOM>-Email.key
├── mail_client
│   ├── prenom.nom@heig-vd.ch.crt
│   ├── prenom.nom@heig-vd.ch.csr
│   ├── prenom.nom@heig-vd.ch.key
│   └── prenom.nom@heig-vd.ch.p12
├── TLS_CA
│   ├── config.conf
│   ├── <NOM>-TLS.crt
│   ├── <NOM>-TLS.csr
│   └── <NOM>-TLS.key
└── TLS_client
    ├── IP.crt
    ├── IP.csr
    └── IP.key
```

Soumettez sur cyberlearn votre rapport ainsi que l'arborescence demandée.

6. Vous pouvez changer les noms des fichiers mais pas ceux des dossiers.