# ✅ 🔐 LAB 1 – Certificats & PKI avec OpenSSL

## 🎯 Objectif :

Créer une infrastructure PKI, générer des certificats, gérer les révocations.

## 🔑 Commandes essentielles

| Étape | Commande |
|---|---|
| Générer clé privée CA | `openssl genrsa -out ca/fsb.key -des3 4096` |
| Certificat auto-signé CA | `openssl req -new -x509 -key ca/fsb.key -out ca/fsb.crt -config config/openssl_ca.cnf` |
| Voir certificat | `openssl x509 -in ca/fsb.crt -text -noout` |
| Convertir PEM → DER | `openssl x509 -inform PEM -outform DER -in ca/fsb.crt -out ca/fsb.der` |
| Clé utilisateur | `openssl genrsa -out certs/user.key -des3 2048` |
| Requête CSR utilisateur | `openssl req -new -key certs/user.key -out certs/user.req -config config/openssl_mail.cnf` |
| Signer CSR avec CA | `openssl ca -config config/openssl_mail.cnf -in certs/user.req -out certs/user.crt` |
| Générer fichier PKCS#12 | `openssl pkcs12 -export -inkey certs/user.key -in certs/user.crt -out certs/user.p12 -certfile ca/fsb.crt` |
| Révoquer certificat | `openssl ca -config config/openssl_ca.cnf -revoke certs/user2.crt` |
| Générer LCR | `openssl ca -gencrl -config config/openssl_ca.cnf -out crls/rev_list.crl` |
| Voir LCR | `openssl crl -in crls/rev_list.crl -text` |
| Convertir LCR PEM → DER | `openssl crl -in crls/rev_list.crl -out crls/rev_list.der -inform PEM -outform DER` |

# ✅ 🌐 LAB 2 – Apache + mod_ssl (HTTPS)

## 🎯 Objectif :

Configurer Apache pour héberger un site Web sécurisé en HTTPS + auth par certificat.

## ⚙️ Commandes essentielles

| Étape | Commande |
| --- | --- |
| Installer Apache & SSL | `sudo yum install httpd mod_ssl php` |
| Démarrer Apache | `sudo systemctl start httpd` |
| Activer Apache au boot | `sudo systemctl enable httpd` |
| Ouvrir ports 80 et 443 | `sudo firewall-cmd --permanent --add-port=80/tcp sudo firewall-cmd --permanent --add-port=443/tcp sudo firewall-cmd --reload` |
| Créer répertoire site | `mkdir -p /var/www/html/demo/logs` |
| Créer page d'accueil | `vi /var/www/html/demo/index.php` |
| Changer droits | `chown -R apache.apache /var/www/html/demo` |
| SELinux en permissif | `setenforce 0` |
| Ajouter dans /etc/hosts | `vi /etc/hosts` |

## 🔒 Certificat serveur pour SSL :

| Étape | Commande |
| --- | --- |
| Générer clé | `openssl genrsa -out certs/server/server.key -des3 2048` |
| Requête CSR serveur | `openssl req -new -key certs/server/server.key -out certs/server/server.req -config config/openssl_ssl.cnf` |
| Signer certificat serveur | `openssl ca -config config/openssl_ssl.cnf -in certs/server/server.req -out certs/server/server.crt` |

| | |
|---|---|
| Copier fichiers vers Apache | `sudo cp -r certs/server /etc/httpd/conf.d sudo cp ca/fsb.crt /etc/httpd/conf.d/server/` |
| Droits d'accès | `chmod -R 700 /etc/httpd/conf.d/server/` |
| Modifier `ssl.conf` | `vi /etc/httpd/conf.d/ssl.conf` |
| Redémarrer Apache | `sudo systemctl restart httpd` |

### 🔐 Forcer HTTPS + Auth par certificat

| Étape | Commande |
|---|---|
| Forcer HTTPS | Ajouter dans VirtualHost : `RewriteEngine on RewriteCond %{SERVER_PORT} !^443$ RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [L,R]` |
| Créer certif utilisateur | `openssl genrsa -out certs/user/user.key -des3 2048` |
| CSR utilisateur | `openssl req -new -key certs/user/user.key -out certs/user/user.req -config config/openssl_user.cnf` |
| Signer certif utilisateur | `openssl ca -config config/openssl_user.cnf -in certs/user/user.req -out certs/user/user.crt` |
| Exporter PKCS#12 | `openssl pkcs12 -export -inkey certs/user/user.key -in certs/user/user.crt -out certs/user/user.p12 -certfile ca/fsb.crt` |
| Modifier `ssl.conf` (zone admin) | `vi /etc/httpd/conf.d/ssl.conf` |
| Redémarrer Apache | `sudo systemctl restart httpd` |

## ✅ 🔍 LAB 3 – Évaluation TLS avec SSLyze

### 🎯 Objectif :

Analyser la configuration SSL/TLS d'un serveur web

### 🛠️ Commandes essentielles

| Étape | Commande |
| --- | --- |
| Installer SSLyze | `pip install sslyze` |
| Scanner le site Web | `python -m sslyze www.demo.com` |

# ✅ 🔐 LAB 4 – Accès distant sécurisé : OpenVPN

🎯 **Objectif** :
Mettre en place un tunnel VPN sécurisé avec OpenVPN en utilisant des certificats et TLS pour authentification.

## ⚙️ Installation côté Serveur

| Étape | Commande |
| --- | --- |
| Mettre à jour et installer OpenVPN | `sudo yum updatesudo yum install epel-releasesudo yum install openvpn` |
| Copier la config exemple | `sudo cp /usr/share/doc/openvpn-2.4.9/sample/sample-config-files/server.conf /etc/openvpn` |

## 🔐 Certificat côté Serveur

| Étape | Commande |
| --- | --- |
| Aller dans PKI | `cd /home/fsb/pki` |
| Créer dossier et clé privée | `mkdir certs/vpn-serveropenssl genrsa -out certs/vpn-server/server.key -des3 2048` |
| Créer CSR | `openssl req -new -config config/openssl_vpn-server.cnf -key certs/vpn-server/server.key -out certs/vpn-server/server.req` |
| Signer CSR | `openssl ca -config config/openssl_vpn-server.cnf -in certs/vpn-server/server.req -out certs/vpn-server/server.crt` |
| Générer paramètres Diffie-Hellman | `openssl dhparam -out /etc/openvpn/dh1024.pem 1024` |

| | |
|---|---|
| Générer clé TLS pour anti DoS | `openvpn --genkey --secret /etc/openvpn/ta.key` |

## ⚙️ Configuration serveur

| Étape | Commande |
|---|---|
| Éditer config serveur | `vi /etc/openvpn/server.conf` |
| Lancer le serveur | `openvpn /etc/openvpn/server.conf` |
| Vérifier interface VPN | `ifconfig` |
| Désactiver SELinux | `vi /etc/selinux/config` (changer à `SELINUX=disabled`) |

## 🔥 Pare-feu serveur

| Étape | Commande |
|---|---|
| Autoriser OpenVPN | `sudo firewall-cmd --zone=public --add-service=openvpnsudo firewall-cmd --zone=public --add-service=openvpn --permanentsudo firewall-cmd --reload` |

## 🖥️ Certificat côté Client

| Étape | Commande |
|---|---|
| Créer dossier et clé privée | `mkdir certs/vpn-clientopenssl genrsa -out certs/vpn-client/client.key -des3 2048` |
| Créer CSR client | `openssl req -new -config config/openssl_vpn-client.cnf -key certs/vpn-client/client.key -out certs/vpn-client/client.req` |
| Signer certificat client | `openssl ca -config config/openssl_vpn-client.cnf -in certs/vpn-client/client.req -out certs/vpn-client/client.crt` |

## 📤 Transfert fichiers vers client

| Étape | Commande |
|---|---|

| | |
|---|---|
| Copier certificats avec `scp` | `scp -r certs/vpn-client fsb@<IP_CLIENT>:/home/fsb`<br>`scp ca/fsb.crt fsb@<IP_CLIENT>:/home/fsb/vpn-client`<br>`scp /etc/openvpn/ta.key fsb@<IP_CLIENT>:/home/fsb/vpn-client` |

### 💻 Client OpenVPN (Linux)

| Étape | Commande |
|---|---|
| Installer le client | `sudo yum install NetworkManager-openvpn NetworkManager-openvpn-gnome` |
| Configurer via GUI | Ajouter : `ca`, `cert`, `key`, `ta.key`, serveur, port `1194`, UDP |

### 🪟 Client OpenVPN (Windows)

- Télécharger : https://openvpn.net/community-downloads/
- Exemple fichier `.ovpn` :

```
client
dev tun
proto udp
remote <IP_SERVER> 1194
ca fsb.crt
cert client.crt
key client.key
tls-auth ta.key 1
cipher AES-256-CBC
auth SHA256
```

# ✅ 📧 LAB 5 – Messagerie Sécurisée : S/MIME avec Thunderbird

🎯 **Objectif** :
Signer et chiffrer des e-mails avec des certificats électroniques via Thunderbird (S/MIME).

### ⚙️ Préparation

| Étape | Détails |
|---|---|
| Installer Thunderbird | Windows ou Linux |

| | |
|---|---|
| Avoir un compte email | Gmail, FSB, etc. |
| Générer certificat utilisateur | Avec OpenSSL (`openssl_mail.cnf`) depuis TP1 |

## 🔐 Certificat dans Thunderbird

| Étape | Action |
|---|---|
| Importer fichier `.p12` | Menu Thunderbird > Paramètres du compte > Sécurité > Certificats |
| Définir comme signature + chiffrement | Dans "S/MIME" section, associer certificat |

## ✍️ Signer un message

| Étape | Détails |
|---|---|
| Coche « Signer numériquement » | Avant l'envoi |
| Si erreur sur FSB AC | Modifier la **confiance du certificat** via `View Certificates > Authorities` |

## 🔐 Envoyer un mail chiffré

| Étape | Détails |
|---|---|
| Ajouter certificat destinataire | `Certificate Manager > Onglet People > Import` |
| Coche « Chiffrer ce message » | Avant l'envoi |

## 📚 Annuaire LDAP

- Ajouter un annuaire pour récupérer les certificats automatiquement

## 🧪 Déchiffrer message avec OpenSSL

```
openssl smime -decrypt -inform DER -in smime.p7m \
-recip certs/user.crt -inkey certs/user.key -out clear.txt
```

## 🔎 Voir certificats SSL Gmail

openssl s_client -connect imap.gmail.com:995 -showcerts
openssl s_client -connect smtp.gmail.com:465 -showcerts