

Rapport de mise en place d'une Infrastructure à Clé Publique (PKI)

1. Création de la structure des dossiers

a) Pour organiser la PKI, j'ai créé la structure de dossiers suivante, séparant la CA racine et la CA intermédiaire avec les commandes suivantes :

```
mkdir -p ~/ca/root/{certs,crl,newcerts,private}
mkdir -p ~/ca/intermediate/{certs,crl,newcerts,private,csr}
```

```
root@debian:~# tree ca
ca
├── intermediate
│   ├── certs
│   ├── crl
│   ├── crlnumber
│   ├── csr
│   ├── index.txt
│   ├── newcerts
│   ├── private
│   └── serial
└── root
    ├── certs
    ├── crl
    ├── index.txt
    ├── newcerts
    ├── private
    └── serial
```

b) Création du fichier de configuration OpenSSL

J'ai créé un fichier `openssl.cnf` dans le dossier `~/ca/root/` (et un autre dans `~/ca/intermediate/`) avec les paramètres adaptés à chaque CA.

La configuration inclut notamment :

- Les extensions de certificat
- Les chemins vers les dossiers et fichiers importants
- Les politiques de signature

```
nano ~/ca/root/openssl.cnf
```

```
nano ~/ca/intermediate/openssl.cnf
```

2. Configuration de la CA racine

a) Génération de la clé CA racine :

Commandes utilisés :

```
openssl genrsa -aes256 -out ~/ca/root/private/ca.key.pem 4096
```

```
chmod 400 ~/ca/root/private/ca.key.pem
```

J'ai généré une clé privée RSA 4096 bits protégée par mot de passe (test) :

```
root@debian:~# openssl genrsa -aes256 -out ~/ca/root/private/ca.key.pem 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....++++
.++++
e is 65537 (0x010001)
Enter pass phrase for /root/ca/root/private/ca.key.pem:
Verifying - Enter pass phrase for /root/ca/root/private/ca.key.pem:
root@debian:~# chmod 400 ~/ca/root/private/ca.key.pem
```

b) Création du certificat racine autosigné (valide 20 ans)

Avec la clé privée et la configuration, j'ai créé le certificat racine valide 20 ans :

```
openssl req -config ~/ca/root/openssl.cnf -key
```

```
~/ca/root/private/ca.key.pem -new -x509 -days 7300 -sha256
```

```
-extensions v3_ca -out ~/ca/root/certs/ca.cert.pem
```

```
chmod 444 ~/ca/root/certs/ca.cert.pem
```

```

root@debian:~/ca# openssl req -config ~/ca/root/openssl.cnf -key ~/ca/root/private/ca.key.pem -new -x509 -days 7300 -sha256 -out ~/ca/root/certs/ca.cert.pem
Enter pass phrase for /root/ca/root/private/ca.key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Haute-Garonne
Locality Name (eg, city) []:Toulouse
Organization Name (eg, company) [Internet Widgits Pty Ltd]:esgi
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:eduardo
Email Address []:epinal@myges.fr

```

Verification :

Le certificat est signé par lui même

```

root@debian:/etc/ssl/ca-server# openssl x509 -noout -subject -issuer -in ~/ca/root/certs/ca.cert.pem
subject=C = FR, ST = Occitanie, O = Eduardo Pina - Inc, CN = Mon CA Racine
issuer=C = FR, ST = Occitanie, O = Eduardo Pina - Inc, CN = Mon CA Racine

```

3. Création de l'autorité intermédiaire

a. Génération de la clé privée intermédiaire

```

openssl genrsa -aes256 -out
~/ca/intermediate/private/intermediate.key.pem 4096
chmod 400 ~/ca/intermediate/private/intermediate.key.pem

```

```

root@debian:~/ca# openssl genrsa -aes256 -out ~/ca/intermediate/private/intermediate.key.pem 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for /root/ca/intermediate/private/intermediate.key.pem:
Verifying - Enter pass phrase for /root/ca/intermediate/private/intermediate.key.pem:
root@debian:~/ca# chmod 400 ~/ca/intermediate/private/intermediate.key.pem

```

b. Création de la demande de signature (CSR) pour l'intermédiaire

```
openssl req -config ~/ca/intermediate/openssl.cnf -new -sha256 -key
~/ca/intermediate/private/intermediate.key.pem -out
~/ca/intermediate/csr/intermediate.csr.pem
```

```
root@debian:~/ca/intermediate# openssl req -config ~/ca/intermediate/openssl.cnf -new
-sha256 -key ~/ca/intermediate/private/intermediate.key.pem -out ~/ca/intermediate/c
sr/intermediate.csr.pem
Enter pass phrase for /root/ca/intermediate/private/intermediate.key.pem:
```

c. Signature du CSR par la CA racine

```
openssl ca -config ~/ca/root/openssl.cnf \
    -extensions v3_intermediate_ca \
    -days 3650 \
    -notext \
    -md sha256 \
    -in ~/ca/intermediate/csr/intermediate.csr.pem \
    -out ~/ca/intermediate/certs/intermediate.cert.pem
chmod 444 ~/ca/intermediate/certs/intermediate.cert.pem
```

```
root@debian:~/ca/root# openssl ca -config openssl.cnf -days 3650 -notext -md sha256
-in ../intermediate/csr/intermediate.csr.pem -out ../intermediate/certs/intermediate.c
ert.pem
Using configuration from openssl.cnf
Enter pass phrase for /root/ca/root/private/ca.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 4096 (0x1000)
    Validity
        Not Before: May 21 08:59:05 2025 GMT
        Not After : May 19 08:59:05 2035 GMT
    Subject:
        countryName             = FR
        stateOrProvinceName     = Occitanie
        organizationName        = Eduardo Pina - Inc
        commonName               = PINA Eduardo
Certificate is to be certified until May 19 08:59:05 2035 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@debian:~/ca/root# chmod 444 ~/ca/intermediate/certs/intermediate.cert.pem
```

Verification :

Le certificat intermédiaire (**PINA Eduardo**) est signé par le certificat racine (**Mon CA Racine**):

```
root@debian:/etc/ssl/ca-server# openssl x509 -noout -subject -issuer -in ~/ca/intermediate/certs/intermediate.cert.pem
subject=C = FR, ST = Occitanie, O = Eduardo Pina - Inc, CN = PINA Eduardo
issuer=C = FR, ST = Occitanie, O = Eduardo Pina - Inc, CN = Mon CA Racine
```

d. Signature du CSR par la CA racine

On concatène le certificat intermédiaire et le certificat racine pour créer la chaîne de certificats utilisée par les serveurs :

```
cat ~/ca/intermediate/certs/intermediate.cert.pem
~/ca/root/certs/ca.cert.pem >
~/ca/intermediate/certs/ca-chain.cert.pem
```

```
chmod 444 ~/ca/intermediate/certs/ca-chain.cert.pem
```

```
root@debian:~/ca/root# cat ~/ca/intermediate/certs/intermediate.cert.pem \
~/ca/root/certs/ca.cert.pem > ~/ca/intermediate/certs/ca-chain.cert.pem
chmod 444 ~/ca/intermediate/certs/ca-chain.cert.pem
```

4. Gestion des certificats serveur

a. Génération de la clé privée serveur

```
openssl genrsa -out ~/ca/intermediate/private/server.key.pem
2048
```

```
chmod 400 ~/ca/intermediate/private/server.key.pem
```

```
root@debian:~/ca/root# openssl genrsa -out ~/ca/intermediate/private/server.key.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
....+++++
.....+++++
e is 65537 (0x010001)
```

b. Création de la CSR serveur

```
openssl req -config ~/ca/intermediate/openssl.cnf -key
~/ca/intermediate/private/server.key.pem -new -sha256 -out
~/ca/intermediate/csr/server.csr.pem
```

```
root@debian:~/ca/root# openssl req -config openssl.cnf \
-key ~/ca/intermediate/private/user.key.pem \
-new -sha256 \
-out ~/ca/intermediate/csr/server.csr.pem
```

c. Signature du certificat serveur par l'autorité intermédiaire

```
openssl ca -config ~/ca/intermediate/openssl.cnf -extensions
usr_cert -days 375 -notext -md sha256 -in
~/ca/intermediate/csr/server.csr.pem -out
~/ca/intermediate/certs/server.cert.pem
```

```
chmod 444 ~/ca/intermediate/certs/server.cert.pem
```

```
root@debian:~/ca/intermediate# openssl ca -config ~/ca/intermediate/openssl.cnf -extensions usr_cert -
days 375 -notext -md sha256 -in ~/ca/intermediate/csr/server.csr.pem -out ~/ca/intermediate/certs/serv
er.cert.pem
Using configuration from /root/ca/intermediate/openssl.cnf
Enter pass phrase for /root/ca/intermediate/private/intermediate.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 4096 (0x1000)
  Validity
    Not Before: May 21 09:19:50 2025 GMT
    Not After : May 31 09:19:50 2026 GMT
  Subject:
    countryName           = FR
    stateOrProvinceName   = Occitanie
    organizationName      = Eduardo Pina - Inc
    commonName            = Mon CA Racine
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Cert Type:
      SSL Client, S/MIME
    Netscape Comment:
      Certificat utilisateur
    X509v3 Subject Key Identifier:
      D1:D3:23:CD:E8:7F:3C:C5:96:2A:6D:2C:FA:37:59:16:0B:B5:53:AE
    X509v3 Authority Key Identifier:
      DirName:/C=FR/ST=Occitanie/O=Eduardo Pina - Inc/CN=Mon CA Racine
      serial:10:00

    X509v3 Key Usage: critical
      Digital Signature, Non Repudiation, Key Encipherment
    X509v3 Extended Key Usage:
      TLS Web Client Authentication, E-mail Protection
Certificate is to be certified until May 31 09:19:50 2026 GMT (375 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Verification :

Le certificat du serveur (**localhost**) est signé par le certificat intermédiaire (**Eduardo Pina**):

```
root@debian:/etc/ssl/ca-server# openssl x509 -in ~/ca/intermediate/certs/user.cert.pem  
-noout -issuer -subject  
issuer=C = FR, ST = Occitanie, O = Eduardo Pina - Inc, CN = PINA Eduardo  
subject=C = FR, ST = France, O = esgieduardo, OU = WebServer, CN = localhost
```

d. Création de la chaîne complète pour le serveur

```
cat ~/ca/intermediate/certs/server.cert.pem \  
~/ca/intermediate/certs/intermediate.cert.pem \  
~/ca/root/certs/ca.cert.pem >  
~/ca/intermediate/certs/ca-chain.cert.pem  
  
chmod 444 ~/ca/intermediate/certs/ca-chain.cert.pem
```

```
root@debian:/etc/ssl/ca-server# cat ~/ca/intermediate/certs/server.cert.pem ~/ca/intermediate/certs/intermediate.cert.pem ~/ca/root/certs/ca.cert.pem > ~/ca/intermediate/certs/ca-chain.cert.pem  
root@debian:/etc/ssl/ca-server# chmod 444 ~/ca/intermediate/certs/ca-chain.cert.pem
```

5. Mise en place du serveur Apache avec SSL

a. Création d'un dossier sécurisé contenant les certificats

/etc/ssl/ca-server/ pour serveur Apache

```
cp ~/ca/intermediate/private/serveur.key.pem  
/etc/ssl/ca-server/  
cp ~/ca/intermediate/certs/serveur-chain.cert.pem  
/etc/ssl/ca-server/  
  
chmod 600 /etc/ssl/ca-server/serveur.key.pem  
chmod 644 /etc/ssl/ca-server/serveur-chain.cert.pem
```

```
root@debian:/# ls -l etc/ssl/ca-server/  
total 12  
-r--r--r-- 1 root root 3700 May 21 05:53 ca-chain.cert.pem  
-r--r--r-- 1 root root 1850 May 21 05:53 server.cert.pem  
-rw----- 1 root root 1675 May 21 05:52 server.key.pem
```

b. Installation d'Apache

```
apt update && apt install apache2
```

c. Configuration d'Apache pour utiliser les certificats SSL

Activation des modules SSL

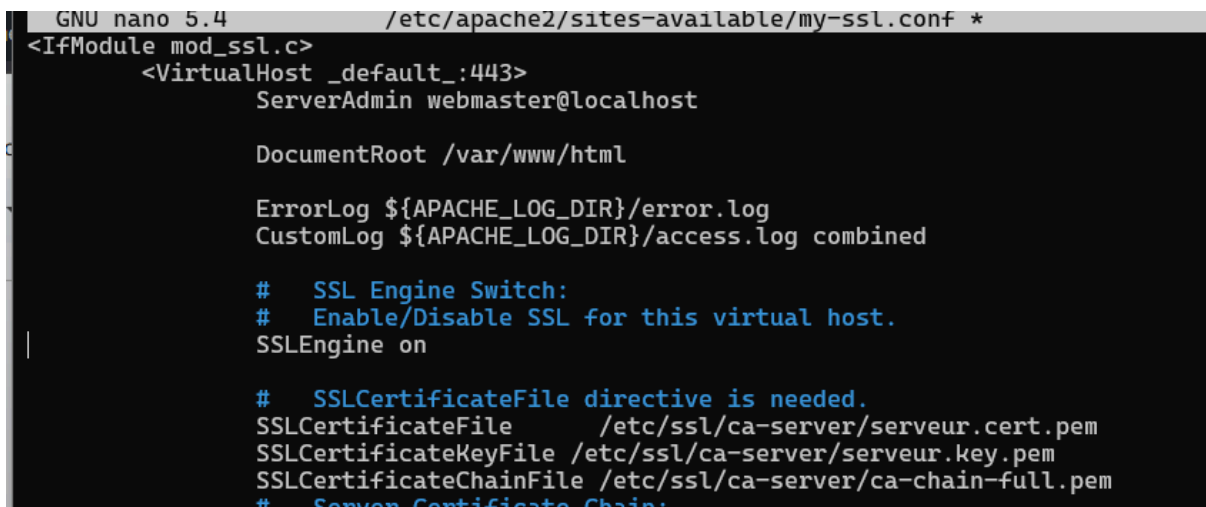
```
a2enmod ssl
```

Création d'un fichier de config basé sur le default ssl :

```
cp /etc/apache2/sites-available/default-ssl.conf  
/etc/apache2/sites-available/my_ssl.conf
```

Modification du fichier de configuration d'apache :

```
nano /etc/apache2/sites-available/my-ssl.conf :
```



```
GNU nano 5.4 /etc/apache2/sites-available/my-ssl.conf *  
<IfModule mod_ssl.c>  
  <VirtualHost _default_:443>  
    ServerAdmin webmaster@localhost  
  
    DocumentRoot /var/www/html  
  
    ErrorLog ${APACHE_LOG_DIR}/error.log  
    CustomLog ${APACHE_LOG_DIR}/access.log combined  
  
    # SSL Engine Switch:  
    # Enable/Disable SSL for this virtual host.  
    SSLEngine on  
  
    # SSLCertificateFile directive is needed.  
    SSLCertificateFile /etc/ssl/ca-server/serveur.cert.pem  
    SSLCertificateKeyFile /etc/ssl/ca-server/serveur.key.pem  
    SSLCertificateChainFile /etc/ssl/ca-server/ca-chain-full.pem  
    # Server Certificate Chain:
```

e. Redémarrer Apache

```
systemctl reload apache2
```


d. Preuve de l'intégration effective des certificats SSL créés dans la configuration du serveur Apache

Certificat du serveur ->

Certificat		
localhost	PINA Eduardo	Mon CA Racine
Nom du sujet		
Pays	FR	
État / Province	France	
Organisation	esgieduardo	
Unité organisationnelle	WebServer	
Nom courant	localhost	
Nom de l'émetteur		
Pays	FR	
État / Province	Occitanie	
Organisation	Eduardo Pina - Inc	
Nom courant	PINA Eduardo	
Validité		
Pas avant	Wed, 21 May 2025 12:32:59 GMT	
Pas après	Sun, 31 May 2026 12:32:59 GMT	
Informations sur la clé publique		
Algorithme	RSA	
Taille de la clé	2048	
Exposant	65537	
Module	C1:CD:0D:52:FB:83:D4:6C:E2:2B:D0:B0:66:CC:F0:47:32:07:EC:17:EF:3A:CA:1A:EF:F...	

Certificat intermediaire >

Certificat		
localhost	PINA Eduardo	Mon CA Racine
Nom du sujet		
Pays	FR	
État / Province	Occitanie	
Organisation	Eduardo Pina - Inc	
Nom courant	PINA Eduardo	
Nom de l'émetteur		
Pays	FR	
État / Province	Occitanie	
Organisation	Eduardo Pina - Inc	
Nom courant	Mon CA Racine	
Validité		
Pas avant	Wed, 21 May 2025 08:59:05 GMT	
Pas après	Sat, 19 May 2035 08:59:05 GMT	
Informations sur la clé publique		
Algorithme	RSA	
Taille de la clé	4096	
Exposant	65537	
Module	B9:68:BB:27:F9:75:18:03:61:08:25:DA:EA:E1:0A:8E:D5:5C:64:6C:08:DE:70:D0:28:F...	

Certificat CA Racine ->

Certificat

localhost

PINA Eduardo

Mon CA Racine

Nom du sujet

PaysFR

État / ProvinceOccitanie

OrganisationEduardo Pina - Inc

Nom courantMon CA Racine

Nom de l'émetteur

PaysFR

État / ProvinceOccitanie

OrganisationEduardo Pina - Inc

Nom courantMon CA Racine

Validité

Pas avantWed, 21 May 2025 08:44:51 GMT

Pas aprèsTue, 16 May 2045 08:44:51 GMT

Informations sur la clé publique

AlgorithmeRSA

Taille de la clé4096

Exposant65537

ModuleDF:70:EB:29:81:FB:9F:61:CF:5C:22:79:95:F5:12:61:C4:E4:0F:B3:5D:E0:54:87:8E:28:...