Compte rendu : Création et gestion de certificats SSL avec OpenSSL

MARIEM EJIWEN 23018

6 MARS 2025

1. Création du certificat de l'Autorité de Certification (AC)

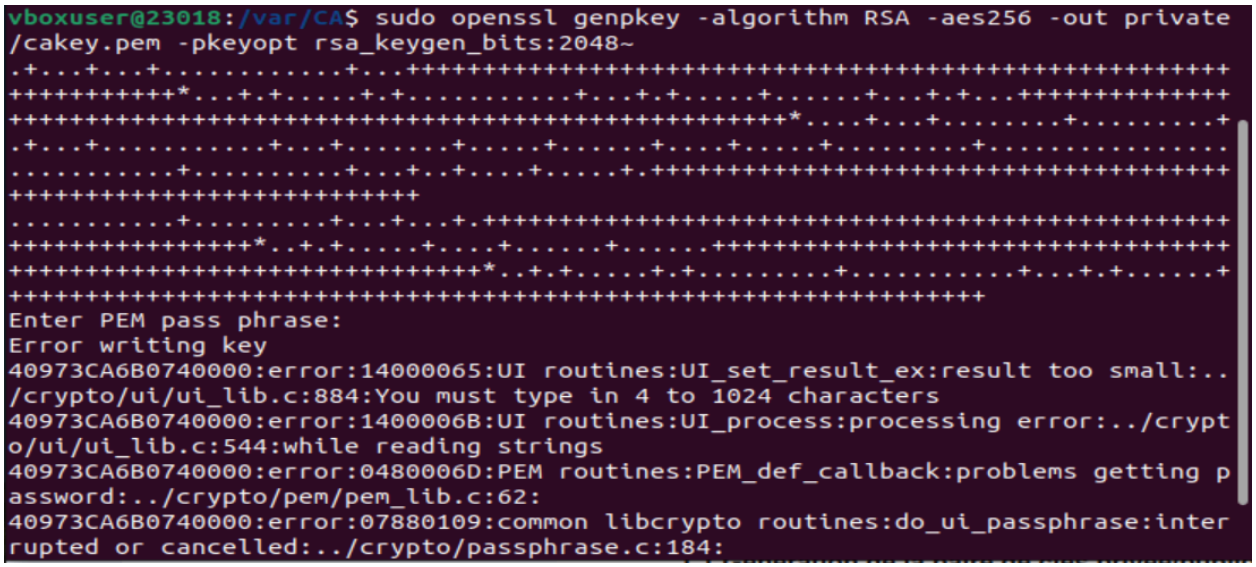
1.1 Génération de la paire de clés privée/publique pour l'AC

Commande :

openssl genpkey -algorithm RSA -aes256 -out private/cakey.pem -pkeyopt rsa_keygen_bits:2048

Sémantique :

- `openssl genpkey` : Génère une clé privée.
- `-algorithm RSA` : Utilisation de l'algorithme RSA.
- `-aes256` : Chiffrement de la clé avec AES-256.
- `-out private/cakey.pem` : Fichier de sortie pour la clé privée.
- `-pkeyopt rsa_keygen_bits:2048` : Génération d'une clé de 2048 bits.



1.2 Création de la structure des répertoires et fichiers

Commandes :

mkdir -p /var/CA/{certs,crl,csr,newcerts,private}

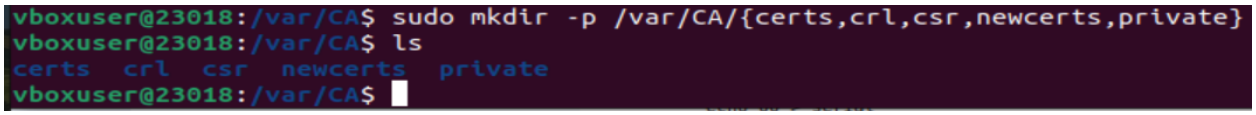
cd /var/CA

> index.txt

echo 00 > serial

Rôle des fichiers/répertoires :

- `certs/` : Contient les certificats valides.
- `crl/` : Stocke la liste des certificats révoqués.
- `csr/` : Stocke les requêtes de certification.
- `newcerts/` : Contient les certificats délivrés.
- `private/` : Contient les clés privées.
- `index.txt` : Base de données des certificats délivrés.
- `serial` : Contient le numéro séquentiel des certificats.



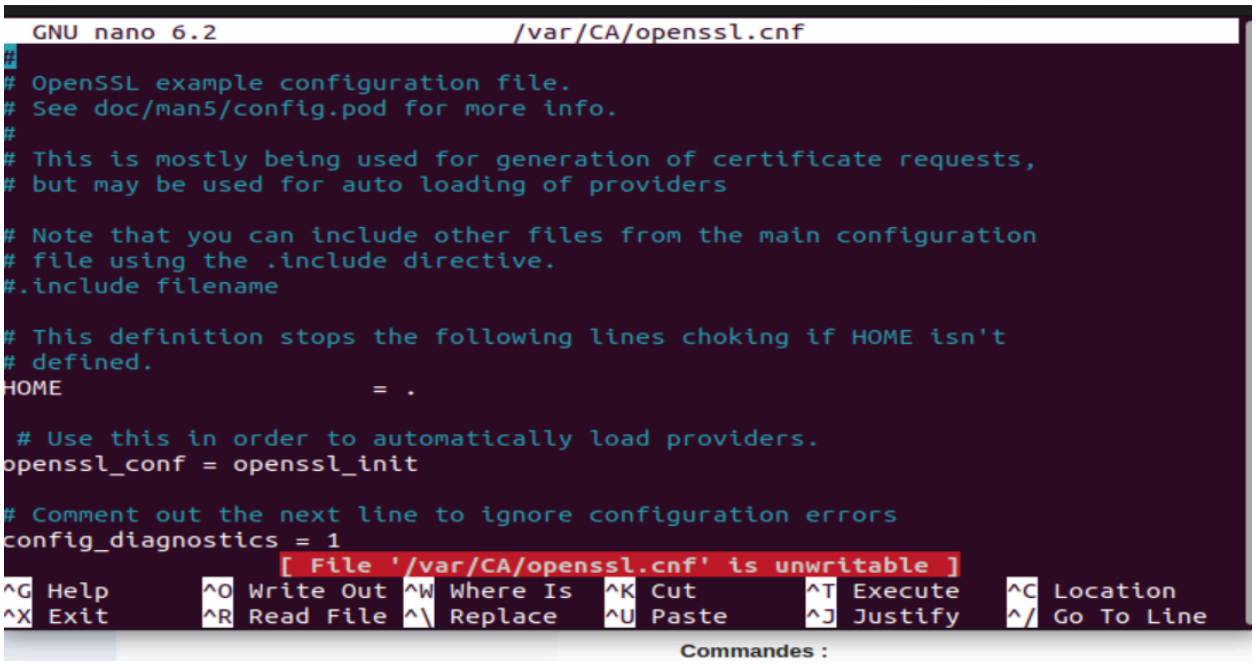
1.3 Copie et modification du fichier de configuration

Commandes :

cp /etc/ssl/openssl.cnf /var/CA/openssl.cnf

nano /var/CA/openssl.cnf

- Modifier les chemins pour qu'ils pointent vers `/var/CA`.
- Dans la section `[ CA_default ]`, adapter `dir` et les sous-sections.
- Modifier la section `policy_match` pour mettre `optional` sur `countryName`, `stateOrProvinceName` et `organizationName`.



1.4 Génération du certificat autosigné de l'AC

Commande :

openssl req -new -x509 -days 3650 -config openssl.cnf -key private/cakey.pem -out cacert.pem

Sémantique :

- `-new -x509` : Crée un certificat autosigné.
- `-days 3650` : Durée de validité de 10 ans.
- `-key private/cakey.pem` : Clé privée de l'AC.
- `-out cacert.pem` : Certificat généré.

2. Création d'un certificat web

2.1 Génération d'une paire de clés pour le serveur

Commande :

openssl genpkey -algorithm RSA -out clefmachine.key -pkeyopt rsa_keygen_bits:2048

```
vboxuser@23018:/var/CA$ sudo openssl req -new -x509 -days 3650 -config openssl.c
nf -key private/cakey.pem -out cacert.pem
Enter pass phrase for private/cakey.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]:ma
State or Province Name (full name) [Some-State]:mauritanie
Locality Name (eg, city) []:nktt
Organization Name (eg, company) [Internet Widgits Pty Ltd]:esp
Organizational Unit Name (eg, section) []:esp
Common Name (e.g. server FQDN or YOUR name) []:esp
Email Address []:23018@esp.mr
```

Champ	Valeur saisie	Explication
Country Name (2-letter code)	`ma`	Code pays (Mauritanie = `MA`).
State or Province Name	`mauritanie`	Nom complet de la région/pays.
Locality Name (City)	`nktt`	Ville (Nouakchott).
Organization Name	`esp`	Nom de l'organisation (ESP).
Organizational Unit Name	`esp`	Département ou section (ESP).
Common Name	`esp`	Nom commun (peut être le FQDN du serveur ou le nom de l'AC).
Email Address	`23018@esp.mr`	Adresse email associée au certificat.

2.2 Génération d'une requête de certification

Commande :

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

Sémantique :

- `-new` : Crée une nouvelle requête.
- `-key clefmachine.key` : Utilise la clé privée du serveur.
- `-out certificatmachine.csr` : Requête de certification générée.

```
vboxuser@23018:/var/CA$ sudo openssl req -new -key clefmachine.key -config opens
sl.cnf -out certificatmachine.cs
Enter pass phrase for clefmachine.key:
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]:ma
State or Province Name (full name) [Some-State]:mauritanie
Locality Name (eg, city) []:nktt
Organization Name (eg, company) [Internet Widgits Pty Ltd]:esp
Organizational Unit Name (eg, section) []:esp
Common Name (e.g. server FQDN or YOUR name) []:esp
Email Address []:23018@esp.mr

Please enter the following 'extra' attributes
to be sent with your certificate request
```

2.3 Génération du certificat signé par l'AC

Commande :

openssl ca -days 365 -in certificatmachine.csr -config openssl.cnf -out certificatmachine.crt

Sémantique :

- `-ca cacert.pem -cakey private/cakey.pem` : Utilisation de l'AC pour signer.
- `-days 365` : Validité d'un an.
- `-in certificatmachine.csr` : Requête à signer.
- `-out certificatmachine.crt` : Certificat signé généré.

Conclusion

Ce processus permet de créer une infrastructure PKI de base avec OpenSSL, incluant une autorité de certification et des certificats SSL signés pour un serveur web.