Compte Rendu TP1

Exercice 3

Tahye Lehbib 22254

IRT-Polytechnique-Nouakchott

Préparation de l'environnement:

```
tahya@tahya-HP-EliteBook-840-G5:~$ mkdir Exo3_TP
tahya@tahya-HP-EliteBook-840-G5:~$ cd Exo3_TP/
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP$ mmkdir CA
La commande « mmkdir » n'a pas été trouvée, mais peut être installée avec :
sudo apt install mblaze
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP$ mkdir CA
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP$ cd CA
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ mkdir certs newcerts crl
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ touch index.txt
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ echo 00>serial

tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ mkdir private
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ cp /etc/ssl/openssl.cnf
cp: opérande de fichier cible manquant après '/etc/ssl/openssl.cnf'
Saisissez « cp --help » pour plus d'informations.
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ cp /etc/ssl/openssl.cnf .
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ ls
certs  crl  index.txt  newcerts  openssl.cnf  private  serial
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ nano openssl.cnf
```

1.Création de la paire de clés RSA pour l'AC :

```
openssl genrsa -aes256 -out private/cakey.pem 2048
```

- **Explication du commande:**
  - **openssl:** C'est la commande principale d'OpenSSL, utilisée pour effectuer diverses opérations liées à la cryptographie.
  - **genrsa**: C'est une sous-commande pour générer une paire de clés RSA.
  - **-aes256**: Spécifie que la clé privée générée sera chiffrée avec l'algorithme de chiffrement AES (Advanced Encryption Standard) utilisant une longueur de clé de 256 bits. Cela ajoute une couche de sécurité en protégeant la clé privée avec un mot de passe.
  - **-out private/cakey.pem**: Indique le chemin et le nom du fichier où la clé privée générée sera enregistrée. Dans cet exemple, la clé privée sera enregistrée dans le répertoire "private" sous le nom "cakey.pem".
  - **2048**: Spécifie la longueur de la clé RSA à générer, en bits. Dans ce cas, une clé de 2048 bits sera générée.

Capture depuis la terminal:

```
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ openssl genrsa -aes256 -out private/cakey.pem 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

2.Génération du certificat auto signé pour l'AC

```
openssl req -new -x509 -config openssl.cnf -days 365 -key private/cakey.pem -out cacert.pem
```

- **Explication du commande:**
- **req:** C'est une sous-commande d'OpenSSL utilisée pour créer et traiter les requêtes de certificat.
- **-new**: Spécifie que nous voulons créer une nouvelle requête de certificat.
- **-x509**: Indique que nous voulons générer un certificat auto-signé plutôt qu'une demande de signature de certificat.
- **-config** openssl.cnf: Indique le fichier de configuration OpenSSL à utiliser pour configurer les paramètres de la requête de certificat.
- **-days 365**: Spécifie la durée de validité du certificat en jours.
- **-key private/cakey.pem**: Indique le chemin et le nom du fichier contenant la clé privée avec laquelle le certificat sera signé. Dans cet exemple, la clé privée est stockée dans le fichier "cakey.pem" dans le répertoire "private".
- **-out cacert.pem**: Indique le chemin et le nom du fichier où le certificat auto-signé sera enregistré. Dans cet exemple, le certificat sera enregistré dans le fichier "cacert.pem".

Capture depuis la terminal:

```
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ openssl req -new -x509 -config openssl.cnf -days 365
-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]:Mauritanie
String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:MR
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:NKTT
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:22254@esp.mr
```

3.Création d'un certificat server :

- **Génération d'une paire de clés RSA pour le serveur avec la commande :**

openssl genrsa -out private/serverkey.pem 2048

❖ **Explication:**

Même l'explication de la commande du premier question, sauf que dans ce cas, je modifie le nom du fichier de sauvegarde.

Capture depuis la terminal:

```
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ openssl genrsa -out private/serverkey.pem 2048
```

- **Générez une requête de certification (CSR) avec la commande**

openssl req -new -key private/serverkey.pem -config openssl.cnf -out certificatmachine.csr

❖ Explication:

- ➢ **openssl req**: C'est la commande OpenSSL utilisée pour les opérations liées aux requêtes de certification (Certificate Signing Requests - CSR).
- ➢ **-new**: Cette option spécifie la création d'une nouvelle requête de certification.
- ➢ **-key private/serverkey.pem:** Cette option spécifie le chemin vers la clé privée du serveur à utiliser pour générer la requête de certification. Dans ce cas, la clé privée est stockée dans le fichier serverkey.pem situé dans le répertoire private.
- ➢ **-config openssl.cnf**: Cette option spécifie le fichier de configuration OpenSSL à utiliser pour la génération de la requête de certification. Le fichier openssl.cnf contient les paramètres de configuration pour les certificats et les requêtes de certification.
- ➢ **-out certificatmachine.csr**: Cette option spécifie le nom et le chemin du fichier de sortie où la requête de certification générée sera enregistrée. Dans ce cas, la requête de certification sera enregistrée dans un fichier nommé certificatmachine.csr.

Capture depuis la terminal:

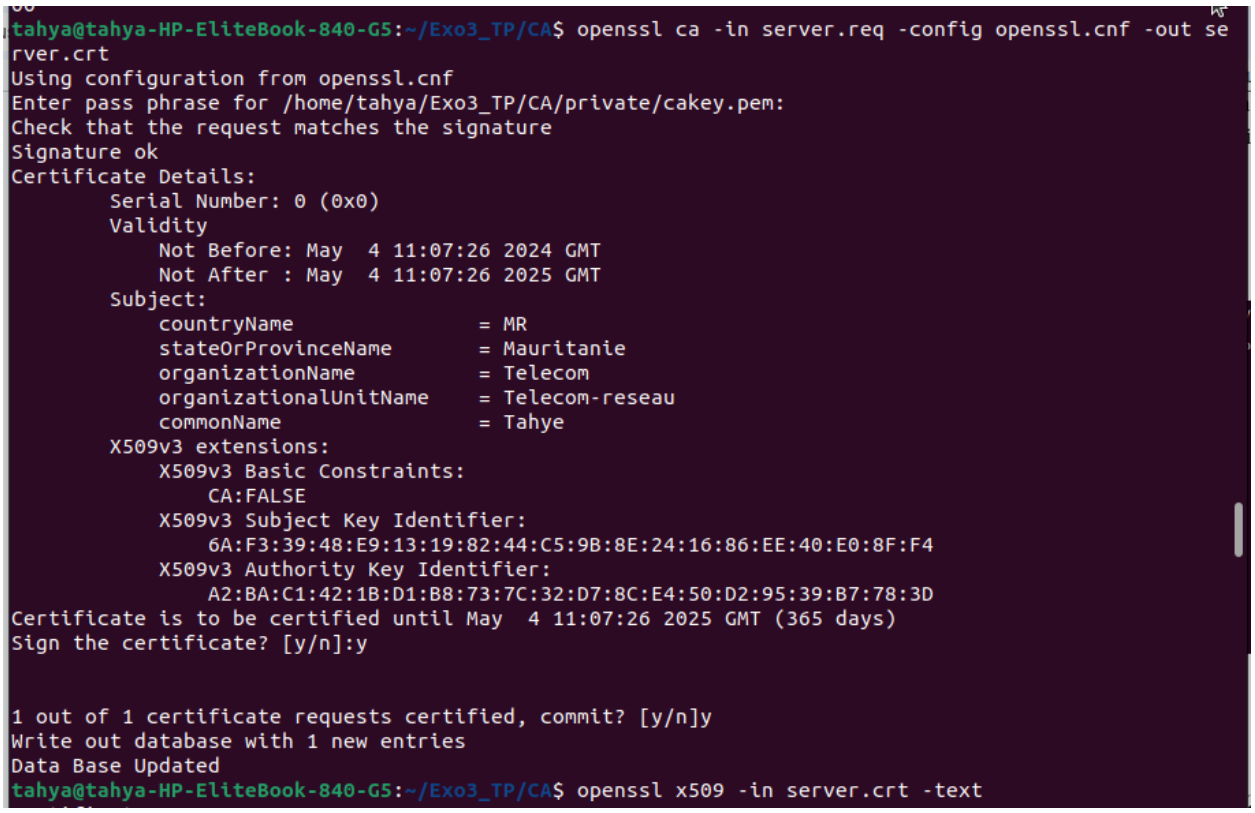
```
tahya@tahya-HP-EliteBook-840-G5:~/Exo3_TP/CA$ openssl req -new -key private/serverkey.pem -config o
penssl.cnf -out server.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name 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]:MR
State or Province Name (full name) [Some-State]:Mauritanie
Locality Name (eg, city) []:Polytechnique
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Telecom
Organizational Unit Name (eg, section) []:Telecom-reseau
Common Name (e.g. server FQDN or YOUR name) []:Tahye
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

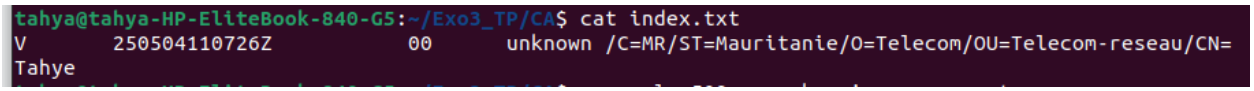
openssl ca -in server.req -config openssl.cnf -out server.crt

- **Explication:**
- **openssl ca**: c'est la commande OpenSSL utilisée pour signer une requête de certification et générer un certificat.
- **-in server.req**: Cette option spécifie le chemin vers la requête de certification à signer. Dans ce cas, la requête de certification est stockée dans un fichier appelé server.req.
- **-config openssl.cnf**: cette option spécifie le fichier de configuration OpenSSL à utiliser pour le processus de certification.
- **-out server.crt**: Cette option spécifie le nom et le chemin du fichier de sortie où le certificat signé sera enregistré. Dans ce cas, le certificat signé sera enregistré dans un fichier appelé server.crt.

Capture depuis la terminal:



Enfin voici le détail de mon Certificat:



Merci pour la lecture