TP OPENSSL 2

ETAPE1 : CRÉATION DU CERTIFICAT DE L'AUTORITÉ DE CERTIFICATION

Pour signer un certificat, vous devez devenir votre propre autorité de certification, cela nécessite la génération d'une paire de clef et d'un certificat auto-signé.

(a) La création de la clef privée de l'autorité de certification se fait comme vu précédemment : "openssl genrsa -out CLEF_auth -des3 4092". Nous avons rajouté l'option -des3 qui introduit l'usage d'une "passphrase", cette "passphrase" sera de- mandée à chaque appel de la CLEF auth.

```
kali@kali:~/Desktop$ openssl genrsa -out CLEF_auth -des3 4092
Generating RSA private key, 4092 bit long modulus (2 primes)
.........++++
.....................................++++
e is 65537 (0×010001)
Enter pass phrase for CLEF_auth:
Verifying - Enter pass phrase for CLEF_auth:
kali@kali:~/Desktop$
```

Passphrase : CLEF_auth

(b) A partir de CLEF auth, on crée un certificat x509 pour une durée de validité de 10 ans :"openssl req -new -x509 -days 3650 -key CLEF_auth -out ANCE_cert".

```
kali@kali:~/Desktop$ openssl req -new -x509 -days 3650 -key CLEF_auth -out ANCE_cert
Enter pass phrase for CLEF_auth:
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.
```

(c) Remplissez les divers champs en simulant l'autorité de votre pays. Dans notre cas de figure, la CA est la ANCE. Le champs common name représente le site de votre autorité (ANCE.tn).

```
Country Name (2 letter code) [AU]:TN
State or Province Name (full name) [Some-State]:Tunis
Locality Name (eg, city) []:Mutuelville
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ANCE
Organizational Unit Name (eg, section) []:ANCE
Common Name (e.g. server FQDN or YOUR name) []:ANCE.tn
Email Address []:
kali@kali:~/Desktop$
```

(d) Le résultat obtenu est le certificat d'autorité de certification qui va permettre de signer les certificats crées.

```
kali@kali:~/Desktop$ ls
ANCE_cert  CLEF_auth  pass.txt  test.txt
kali@kali:~/Desktop$
```

```
kali@kali:~/Desktop$ cat ANCE_cert
-----BEGIN CERTIFICATE-----
MIIFpjCCA46gAwIBAgIUSIq8X+67ZlfPh1eJaU7JU59jnicwDQYJKoZIhvcNAQEL
BQAwYzELMAkGA1UEBhMCVE4xDjAMBgNVBAgMBVR1bmlzMRQwEgYDVQQHDAtNdXR1
ZWx2aWxsZTENMAsGA1UECgwEQU5DRTENMAsGA1UECwwEQU5DRTEQMA4GA1UEAwwH
QU5DRS50bjAeFw0yMDExMTExOTI1NTFaFw0zMDExMDkxOTI1NTFaMGMxCzAJBgNV
BAYTAlROMQ4wDAYDVQQIDAVUdW5pczEUMBIGA1UEBwwLTXV0dWVsdmlsbGUxDTAL
BgNVBAoMBEFOQ0UxDTALBgNVBAsMBEFOQ0UxEDAOBgNVBAMMB0FOQ0UudG4wggIh
MA0GCSqGSIb3DQEBAQUAA4ICDgAwggIJAoICAAwHmbMOFCRDC+bvZ+XmmcCJJ2XO
5ZCr31y07nIZKswp5g+9cHMV+SlWXExkWyMcwc83KTZev/jtgs1XmC+oCvbA74Ke
MFkWTJoY6Kw1uGV8ASqOL/qyW46K/IinEyPLPJSqlawXX8KmklXfMJULd6kYCELk
fkxnEia47CQWh3dGuKjI3zer4NWpMPeOkCyDfH6tbRTZAfG7ULrHUak0ae7RUKVh
MoJdpW+6KP3Y/AX+KTlXzrQa64QqCtjNsvfsa1y4RIgecu8hw8+4aKm/XGyNAbbL
kpby+4NMEJ3ntB4eML/sqDC05sfE1XwMa+IcumDI6Z/fqhR9SS17PqYq5MxAld+7
tFI4lhCGQHObP00NhgCCOThXPtGC/pvZouh82GlUmUGWoTXA/GnwnAREfT2WRTsC
l2hXQGU123iXUa02jQZeW74T25eHXLdk7C3c+o2SlOGLnqn3K75SIdQwbHqGCBR/
hMktE3EoKv4YRPLjfAeMyz5ZiSJ6Us6mL0C4kn90L52/h+fucWcUMSZRpmot+ADu
3Zf//I9aIV0Qba/ZIddnShtuHN3bpdfRe6f3u5wjbftjNhkvTzfneJXiQPzPiMtP
3sUzXBqSoZU3id910B67SiSsLCXMl6j0qrCporgfLKv6Ab5ZGbHgKkZlbjk8yn74
tdg+zgLShUQMqWxZAgMBAAGjUzBRMB0GA1UdDgQWBBQrjjPL5ehDEWBePuFc7pSk
//KTRjAfBgNVHSMEGDAWgBQrjjPL5ehDEWBePuFc7pSk//KTRjAPBgNVHRMBAf8E
BTADAQH/MA0GCSqGSIb3DQEBCwUAA4ICAQAEdHknbWHrkyRsFSQyFt0cVfy5QjnQ
bBmdevyo0oml2v9o2EyqEJEijfxEOup2MZMZqLZU1gDeun7C8b7Kny6ly1v1IifP
JrkcLoCVaEFBSu6ns+66dH3WEhGIY0BGM9xPXwl63N9POscWGuDUL87yRGMPY1/t
HG89cQFlKMeBJvdFhqDWy/Ng/0qSAGt8kQfOQcoASwY1rfEb6vCDvuBiovvkNPHH
E+5QAZEa9z2QNE9Dgd9bpa3I+DStCW6CY2w79SM7UNiK0keY4VP3bVA4hcVIJU8r
ATb1KtMXJ7DIheFI82z8qbX5TTkv9MhbbkdSmdYjtW9TA9eqial9ucsctkmL9pcD
JuS1soZniSlJCAW5oI2cKduM5qwLuWqGYfhRtmi/1xtDodfNLYwIsCXzxb7poeWv
OQao4CGwpxlJ6ettvyQaxsheiqhvRXygG+H3JFjYhWrDe6amOK2HFFa3dS4WU2OG
aUMZsoyQrOJ692y0dq64Kehn7LBnQYZy8013THkZecQUD3fJXw4CiAI9150KEUue
ucDvue03+dlyqLKno6jcbZWuhOnYr6jyxxw/0wGQxsOJRa1+XGNsY/EMsWep+14c
maZr270BIPCXFbzLKlzsZZV7xwlU1K/bIJFFjanCLliEy1w6bHEnU9KxEMffWP3d
ahmU8RRmpSYN2Q==
-----END CERTIFICATE-----
```

ETAPE2 : GENERATION D'UNE DEMANDE DE SIGNATURE D'UN CERTIFICAT A UN SERVEUR

(a) On génère la clef privée CLEF serv avec les commandes précédentes.

```
kali@kali:~/Desktop$ openssl genrsa -out CLEF_serv -des3 4092
Generating RSA private key, 4092 bit long modulus (2 primes)
.....................................................................................
............+++++
.........................+++++
e is 65537 (0×010001)
Enter pass phrase for CLEF_serv:
Verifying - Enter pass phrase for CLEF_serv:
kali@kali:~/Desktop$
```

Passphrase : CLEF_serv

(b) Ensuite, on lance une demande de signature de certificat (CSR Certificate Signing Request) avec la commande suivante : "openssl req -new -key CLEF_serv -out demande_serveur". Comme précédemment, remplissez tous les champs de la demande de votre serveur.

```
kali@kali:~/Desktop$ openssl req -new -key CLEF_serv -out demande_serveur
Enter pass phrase for CLEF_serv:
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]:TN
State or Province Name (full name) [Some-State]:Tunis
Locality Name (eg, city) []:Mutuelville
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Serveur
Organizational Unit Name (eg, section) []:Serveur
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:certif_serv
An optional company name []:
kali@kali:~/Desktop$
```

ETAPE3 : LA SIGNATURE DE LA DEMANDE DU SERVEUR PAR LE CA (CERTIFICATE AUTORITY)

(a) La commande qui signe la demande de certificat est la suivante : ”openssl x509 - req -in demande_serveur -out serveur_cert -CA ANCE_cert -CAkey CLEF_auth -CAcreateserial -CAserial serveur.srl”. L’option CAcreateserial n’est néces- saire que la première fois. Le certificat signé est le fichier ”serveur_cert”.

```
kali@kali:~/Desktop$ openssl x509 -req -in demande_serveur -out serveur_cert -CA ANCE
_cert -CAkey CLEF_auth -CAcreateserial -CAserial serveur.srl
Signature ok
subject=C = TN, ST = Tunis, L = Mutuelville, O = Serveur, OU = Serveur
Getting CA Private Key
Enter pass phrase for CLEF_auth:
kali@kali:~/Desktop$
```

(b) Pour vérifier le certificat générer, il est nécessaire de disposer du certificat de l’autorité qui l’a émis : ”openssl verifiy -CAfile ANCE_cert serveur_cert”

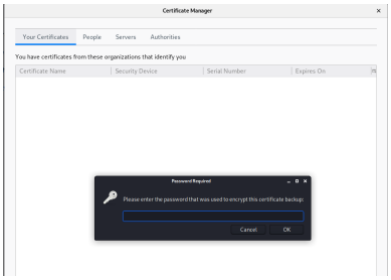
```
kali@kali:~/Desktop$ openssl verify -CAfile ANCE_cert serveur_cert
serveur_cert: OK
kali@kali:~/Desktop$
```

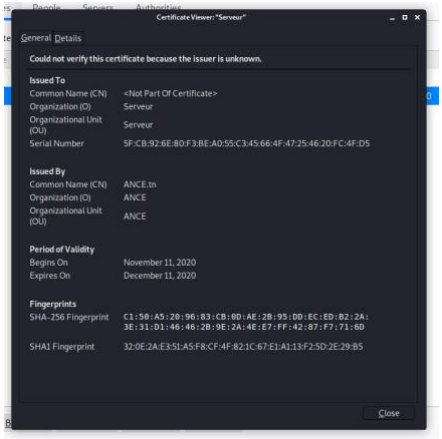
(c) Pour pouvoir exporter le certificat dans le magasin du navigateur, il faut le convertir en extension PKCS12 certificate et le résultat est la combinaison du fichier certifi- cat/clef:”openssl pkcs12 -export -out serveur_cert.pfx -in serveur_cert -inkey CLEF_serv -name "Certificate of server"”

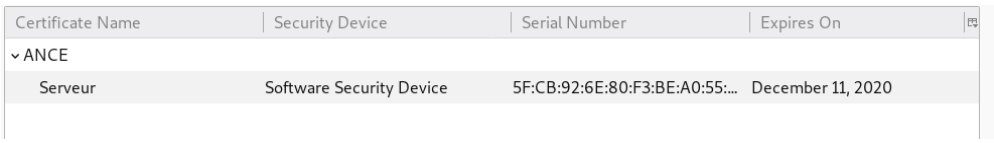
```
kali@kali:~/Desktop$ openssl pkcs12 -export -out serveur_cert.pfx -in serveur_cert -i
nkey CLEF_serv -name "Certificate of server"
Enter pass phrase for CLEF_serv:
Enter Export Password:
Verifying - Enter Export Password:
kali@kali:~/Desktop$
```

password : Export_pass

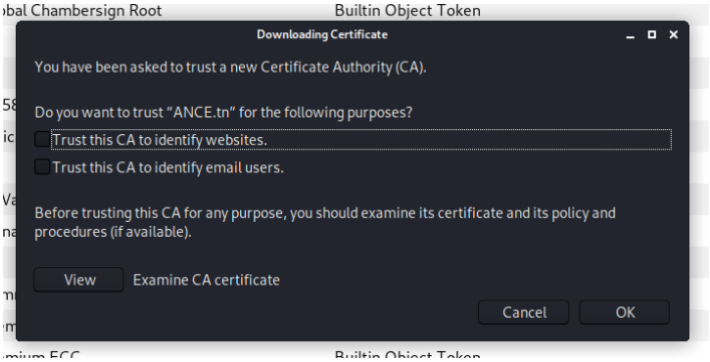
(d) Une fois le certificat ”serveur_cert.pfx” uploadé, remarquez que ce certificat n’est pas vérifié par votre navigateur.

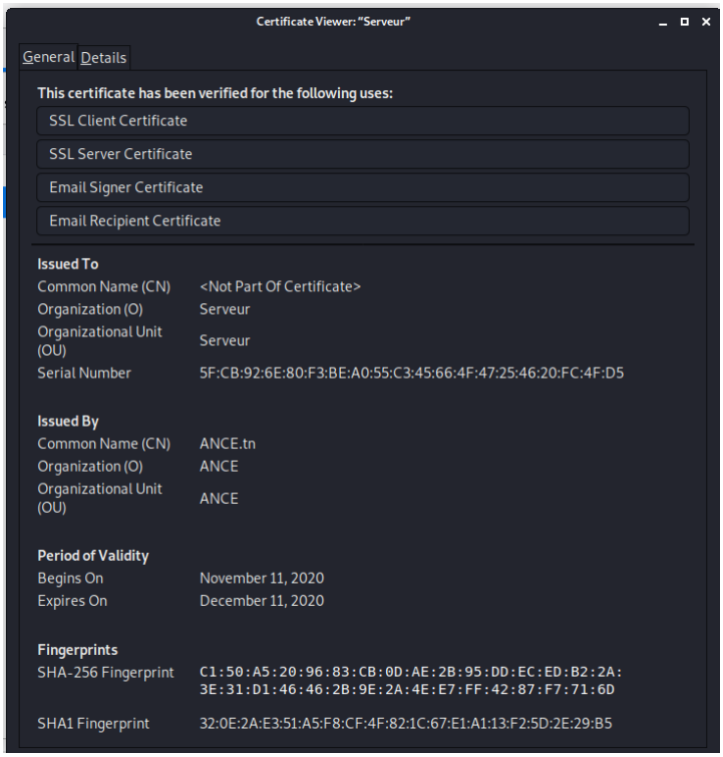






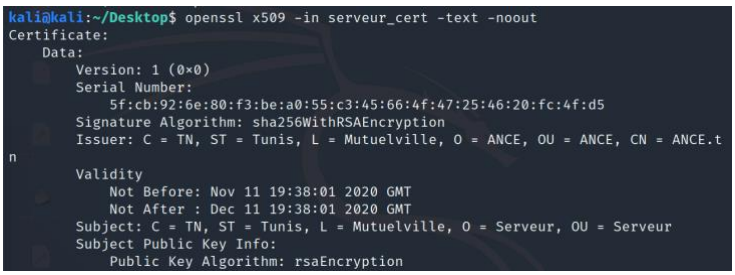
(e) Pour valider cette vérification, uploader le certificat de l'autorité de certification dans le navigateur. C'est ce dernier qui va valider le certificat du serveur "serveur_cert.pfx".





4. ETAPE4 : AFFICHAGE DES INFORMATIONS CONTENUES DANS UN CERTIFICAT

(a) Le certificat du serveur "openssl x509 -in serveur_cert -text -noout", remar- quez la présence de qui a émis le certificat et pour qui.



(b) Qui a émis le certificat ?"openssl x509 -noout -in serveur_cert -issuer"

```
kali@kali:~/Desktop$ openssl x509 -noout -in serveur_cert -issuer
issuer=C = TN, ST = Tunis, L = Mutuelville, O = ANCE, OU = ANCE, CN = ANCE.tn
kali@kali:~/Desktop$
```

(c) Pour qui a-t-il été émis ? "openssl x509 -noout -in serveur_cert -subject"

```
kali@kali:~/Desktop$ openssl x509 -noout -in serveur_cert -subject
subject=C = TN, ST = Tunis, L = Mutuelville, O = Serveur, OU = Serveur
kali@kali:~/Desktop$
```

(d) Quelle est sa période de validité ? "openssl x509 -noout -in serveur_cert - dates"

```
kali@kali:~/Desktop$ openssl x509 -noout -in serveur_cert -dates
notBefore=Nov 11 19:38:01 2020 GMT
notAfter=Dec 11 19:38:01 2020 GMT
kali@kali:~/Desktop$
```

(e) Toutes les infos précédentes : "openssl x509 -noout -in serveur_cert -issuer -subject -dates"

```
kali@kali:~/Desktop$ openssl x509 -noout -in serveur_cert -issuer -subject -dates
issuer=C = TN, ST = Tunis, L = Mutuelville, O = ANCE, OU = ANCE, CN = ANCE.tn
subject=C = TN, ST = Tunis, L = Mutuelville, O = Serveur, OU = Serveur
notBefore=Nov 11 19:38:01 2020 GMT
notAfter=Dec 11 19:38:01 2020 GMT
kali@kali:~/Desktop$
```

(f) Quelle est sa valeur de hachage ?"openssl x509 -noout -in serveur_cert -hash"

```
kali@kali:~/Desktop$ openssl x509 -noout -in serveur_cert -hash
05b59a56
kali@kali:~/Desktop$
```

(g) Quelle est son empreinte ?"openssl x509 -noout -in serveur_cert -fingerprint"

```
kali@kali:~/Desktop$ openssl x509 -noout -in serveur_cert -fingerprint
SHA1 Fingerprint=32:0E:2A:E3:51:A5:F8:CF:4F:82:1C:67:E1:A1:13:F2:5D:2E:29:B5
kali@kali:~/Desktop$
```