L'outil OpenSSL : mode opératoire

0) D'abord :

makecert
demoCA
certs
crl
newcerts
private

C:\makecert>**openssl**

+ on crée un fichier index vide : C:\makecert\demoCA>edit ***index.txt***
+ on initialise les numéros de série : C:\makecert\demoCA>echo 01 > ***serial***

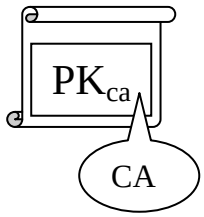
A. Fabrication d'un CA de référence

A.1) ***OpenSSL>*** **genrsa** -out ca.key 1024

➔ paire de clés (n,e)/(n,d)

A.2) ***OpenSSL***> **req** -new -x509 -key ca.key -out demoCA/**cacert.pem**

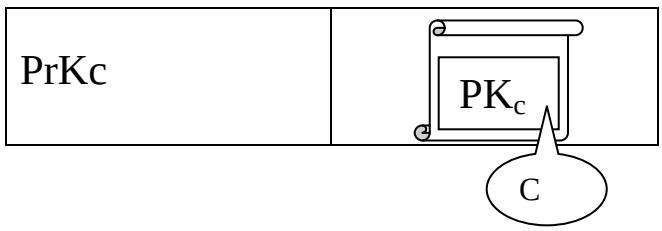
➔ certificat pem pour le CA



B. Fabrication des keystores du client et du serveur

B.1) C:\makecert>**keytool** -**genkey** -**alias** ClaudeCli -**keystore** ***client_keystore***

➔



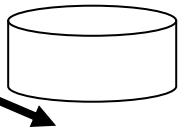
idem:

B.2) C:\makecert>**keytool** -genkey -alias ClaudeSer -keystore ***serveur_keystore***

C. Création d'un certificat validé par le CA pour le client

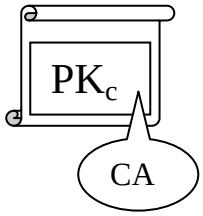
C.1) C:\makecert>**keytool** -**certreq** -**alias** ClaudeCli -**keystore** client_keystore -**file** clientJsse.csr -**keypass** sexycli -**storepass** beaugossecli -v

➔ ficher csr



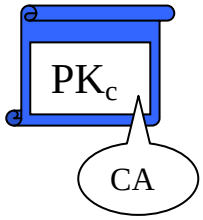
C.2) ***OpenSSL*> ca** -in clientJsse.csr -out clientJsse.pem -keyfile ca.key

➔ certificat pem pour le client



C.3) ***OpenSSL*> x509** -in clientJsse.pem -out clientJsse.der -outform DER

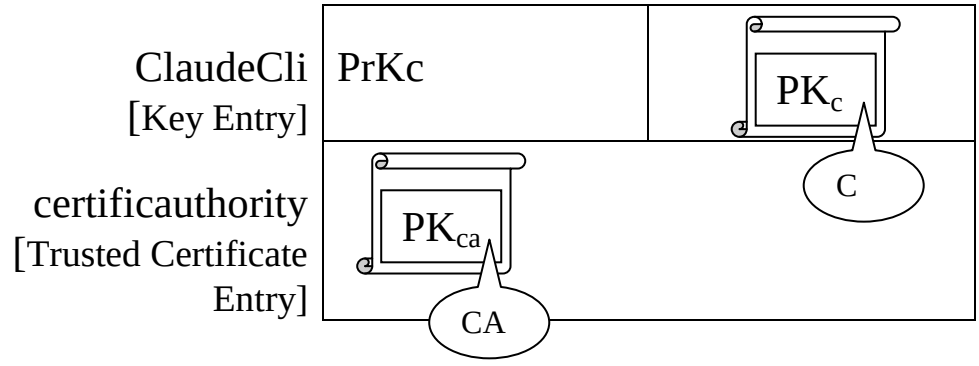
➔ certificat der (X509) pour le client



D. Importation du certificat du CA dans les keystores client et serveur

D.1) C:\makecert>**keytool** -**import** -v -alias certificauthority -file demaCA**cacert.pem** -keystore **client_keystore** -storepass beaugosecli

➔



idem:

D.2) C:\makecert>**keytool** -**import** -v -alias certificauthority -file demoCA**cacert.pem** -keystore **serveur_keystore** -storepass beaugosseser

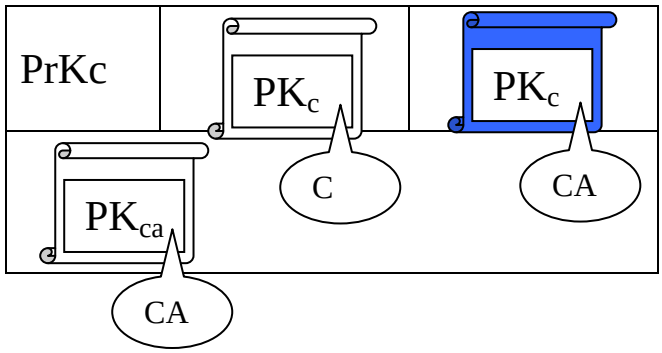
E. Importation du certificat du client signé par le CA

E.1) C:\makecert>**keytool** -**import** -v -keystore client_keystore -alias ClaudeCli –file **clientJsse.der** -storepass beaugossecli

➔

ClaudeCli
[Key Entry]

certificauthority
[Trusted Certificate Entry]



claudecli, 20-avr.-2004, **keyEntry**,
Empreinte du certificat (MD5) :
32:FB:9C:B7:31:A9:6E:3D:39:E5:10:00:03:01:4A:93
certificauthority, 20-avr.-2004, **trustedCertEntry**,
Empreinte du certificat (MD5) :
0A:77:22:6F:A8:5A:AE:3B:6F:9D:AB:A8:8E:A0:A4:94

F. Importation du certificat du serveur signé par le CA

idem:
E.1) C:\makecert>**keytool** -**import** -v -keystore serveur_keystore -alias ClaudeCli –file **serveurJsse.der** -storepass beaugosseser

certificauthority, 23-avr.-2004, **trustedCertEntry**,
Empreinte du certificat (MD5) :
0A:77:22:6F:A8:5A:AE:3B:6F:9D:AB:A8:8E:A0:A4:94
claudeser, 23-avr.-2004, **keyEntry**,
Empreinte du certificat (MD5) :
EF:F7:FD:30:61:0C:9B:30:78:3F:26:48:2F:F6:21:41