Escuela Superior
de Ingeniería y Tecnología
Universidad de La Laguna

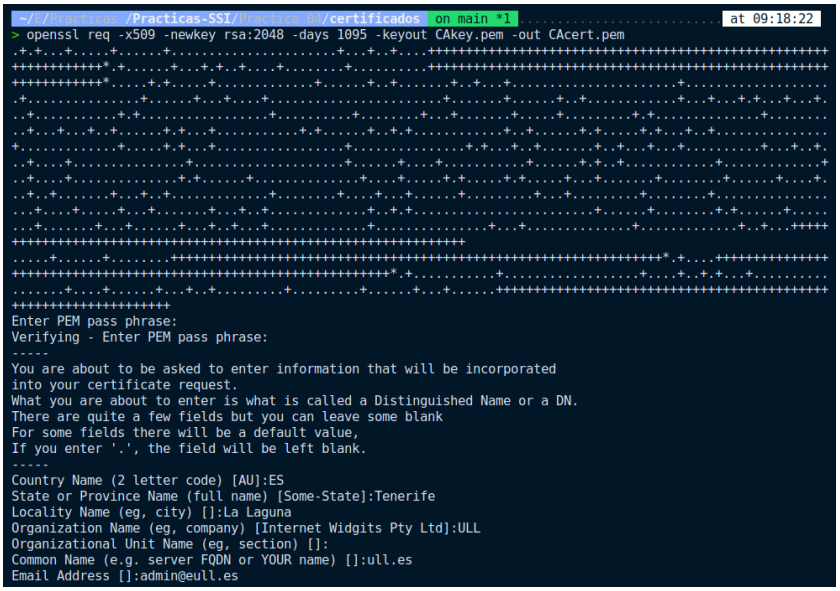
Práctica 05. Creación de una Autoridad Certificadora (CA) con OpenSSL

Seguridad de Sistemas Informáticos

Cheuk Kelly Ng Pante
alu0101364544@ull.edu.es

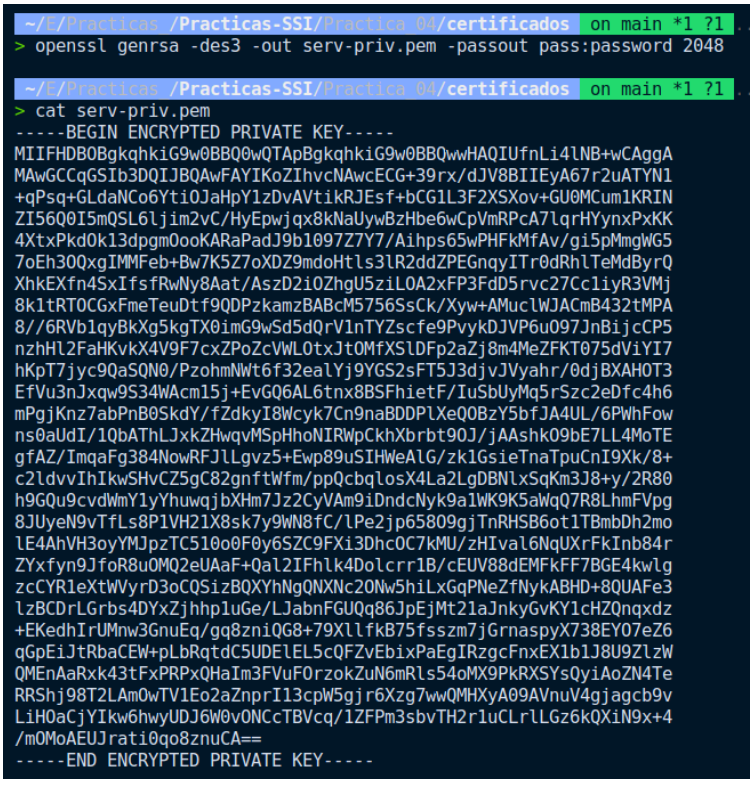
1. Generación de la Autoridad Certificadora **2**
2. Generación del certificado del servidor **2**
2.1. Generamos la clave privada del que será nuestro certificado digital 2
2.2. Realizar una petición definiendo el propietario 3
2.3. Generamos un fichero de configuración denominado config1.txt 3
2.4. Emitimos el certificado del servidor 3
3. Generación de los certificados de los clientes **4**
3.1. Generamos la clave privada del cliente 4
3.2. Generamos la petición del certificado 4
3.3. Generamos un fichero de configuración denominado config2.txt 5
3.4. Emitimos el certificado 5
4. Exportando los certificados de los clientes **6**
5. Definiendo la lista de revocación **6**
5.1. Generamos un fichero index.txt 6
5.2. Configuramos openssl.cnf 7
5.3. Creamos una lista de revocación o CRL 7
5.4. Creamos el mismo fichero pero con extensión .pem 7
5.5. Revocamos un certificado 7

1. Generación de la Autoridad Certificadora



2. Generación del certificado del servidor

2.1. Generamos la clave privada del que será nuestro certificado digital



2.2. Realizar una petición definiendo el propietario

```
/mnt/d/D/1/4/P/Se/Practicas-SSI/Practica_04/certificados on main !1 ?2 at 09:17:51
openssl req -new -subj "/DC=root.com/OU=com/CN=root" -key serv-priv.pem -passin pass:hola -out petic-cert-client
.pem

/mnt/d/D/1/4/P/Se/Practicas-SSI/Practica_04/certificados on main !1 ?3 at 09:20:17
cat petic-cert-client.pem
-----BEGIN CERTIFICATE REQUEST-----
MIICfDCCAWQCAQAwNzEYMBYGCgmSJomT8ixkARkWCHJvb3QuY29tMQwwCgYDVQQL
DANjb20xDTALBgNVBAMMBHJvb3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDT+vZGkDQrjxmdTU+lC7ORxAbWVHknSKc1i6TBnIXWPLxNRsi6FYDiaPRG
TyDvOhkqiFCt+y3Eu7QUmK8081CWvOrcLMHC7RHd4xZg4Pn8mbU7EQCjhE32WAbt
Wu2vyquqagxSsUfrnWTRtCMhZkARHQPjqFYp9lsZR7Qt6HvKd8CTPRlQ4vdW1/C7
Zy85GDrRnN2BpJVG2nBPQpmWprsiYlFlJ2jZQ3UztvrCKSmX137VbflO1RzqXzQ9
M42i5hMQ53qL61EzLgGQzYi25wDjyk96+s/Q5AXfRFftA7hdbjc5hFVhqJmSCYlt
K3DM/AsBe1wPEbIHrL/2qcpnVr2tAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEA
yD6l/zHqRLye/AeY0Un3ag3IoLKp8hqj4YtbMSAG0ZXYtLn6RiVnk5rtjyxXyipM
1+8ZuIUsfGSq+Z7GBC7R+ZtxSi4uMFlPsTODHUrUKQPsHib8w0BPgrBPIGkRX2wv
ZhEUxUchXSLCR2jHeZL9pAYUgSm4FiomT0U8uh7qpRG6wZaWXr40UnAa/fJEHO2l
ikk577qSym55R7A/IecS86AQP+c3eJn/meRVkzKzMvD9eY7B3xIdiCMU37QgBH+b
hcFK3alIIVrEEgASqjVvX1FNY+pE5H5pLQVXnb3MRX3ERRQKr9Xy3SY4Uq/XP1Az
yZTdWrQVJWqprNC5F2FZhg==
-----END CERTIFICATE REQUEST-----
```

2.3. Generamos un fichero de configuración denominado `config1.txt`

```
~/E/Practicas /Practicas-SSI/Practica_04/certificados on main *1 ?1 ..... at 09:25:51
> touch config1.txt

~/E/Practicas /Practicas-SSI/Practica_04/certificados on main *1 ?1 ..... at 09:26:18
> vi config1.txt

~/E/Practicas /Practicas-SSI/Practica_04/certificados on main *1 ?1 ..... took 1m 2s at 09:27:49
> cat config1.txt
basicConstraints = critical,CA:FALSE
extendKeyUsage = serverAuth
```

2.4. Emitimos el certificado del servidor

```
/mnt/d/D/1/4/P/Se/Practicas-SSI/Practica_04/certificados on main !1 ?3
openssl x509 -CA CAcert.pem -CAkey CAkey.pem -req -in petic-certificado-serv.pem -days 15 -sha1 -CAcreateserial
-out servidor-cert.pem
Certificate request self-signature ok
subject=DC = root.com, OU = com, CN = root
Enter pass phrase for CAkey.pem:

/mnt/d/D/1/4/P/Se/Practicas-SSI/Practica_04/certificados on main !1 ?4
cat servidor-cert.pem
-----BEGIN CERTIFICATE-----
MIIDLzCCAhcCFGAPyKo9tlNjyNF50gJ7LknCmAxyMA0GCSqGSIb3DQEBBQUAMHEx
CzAJBgNVBAYTAkVTMREwDwYDVQQIDAhUZW51cmlmZTESMBAGA1UEBwwJTGEgTGFn
dW5hMQwwCgYDVQQKDANVTEwxDzANBgNVBAMMBnVsbC5lczEcMBoGCSqGSIb3DQEJ
ARYNYWRtaW5AZXVsbC5lczAeFw0yMzEwMTkwODI0MjlaFw0yMzExMDMwODI0Mjla
MDcxGDAWBgoJkiaJk/IsZAEZFghyb290LmNvbTEMMAoGA1UECwwDY29tMQ0wCwYD
VQQDDARyb290MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0/r2RpA0
K48ZnU1PpQuzkcQG1lR5J0inNYukwZyF1jy8TUbIuhWA4mj0Rk8g7zoZKohQrfst
xLu0FJivNPJQlrzq3CzBwu0R3eMWYOD5/Jm1OxEAo4RN9lgG7Vrtr8qrqmoMUrFH
651k0bQjIWZAER0D46hWKfZbGUe0Leh7ynfAkz0ZUOL3Vtfwu2cvORg60ZzdgaSV
RtpwT0KZlqa7ImJRZSdo2UN1M7b6wikp15d+1W35TtUc6l80PTONouYTEOd6i+tR
My4BkM2ItucA48pPevrP0OQF30RX7QO4XW43OYRVYaiZkgmJbStwzPwLAXtcDxGy
B6y/9qnKZ1a9rQIDAQABMA0GCSqGSIb3DQEBBQUAA4IBAQAJYgM0xyr0pL9s0TOz
WEyjM/hdI5K8g3ltOGlB3pbi2WyNvzFhX0rJNLjOPeLxirzjv/mqbR6zIV8Y7vev
TibBW1sbfDeIOM1w/k/4HJcb5b+kYWBZIHQPI4Vnmve9oV5/U5JKoycCEg2kEjYg
3/DkOIxiTvD+nfGfuiuTSFHBbC73wP2EAWmony+KEjsaTQ2SfDK16ddM23dTPdkd
oOsnq2iXkJ6YJxQP7CLrPAiHxNN92nFrTuOfL8sh/k79K1KsmOl1F4iBEE+aqunQ
3m8L1FuEVcPOXhDUrwY16KoAsbUm+a9KYQgYU7I3uiAewTOXwLFmSpr1sd+E5kfJ
3P6C
-----END CERTIFICATE-----
```

3. Generación de los certificados de los clientes

3.1. Generamos la clave privada del cliente

```
/mnt/d/D/I/4/P/Se/Practicas-SSI/Practica_04/certificados on main !2 ?4
openssl genrsa -des3 -passout pass:hola -out client-priv.pem 2048

/mnt/d/D/I/4/P/Se/Practicas-SSI/Practica_04/certificados on main !2 ?5
cat client-priv.pem
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQI2uRpi9TeukMCAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECAVpUYo8S1jWBIIEyAbqY/TYTvLj
GjpIFTk9Gy0lop1kb9S3EnVC4WBsC5Lkl5bTnvQj47Otgdlb+dY0gWfwo9XGJebI
QrPro0/k38zSmSCuFWUVmWVT9xiPuOx+m99klGX7fHq6q7GgCBRjV+jv8FG3FWug
TKfNJqU3gH6YnHoMEoLBluPTm3g3NXDfKjqfaW2XhBDW9m3tn02zKbfZcu4HNmPV
UgfLCgzv7TJIkwu+JcMKE+OYutyNjOxDXGmyppwABffq0wQ2/YW+l+3PDo7irfqw
ywNGK8I/VokLTrPqUIhd6Oy8upLbN8r/OJMnbBiR47srvU2xpezHzG3VeHcV+Y+4
6aeqRVHFyAmDeE/FsDyZHDB4T5FdvmmpDYaAU5vSnrf17ED5cRiA9CRtIuo6VCXp
TSRZHIuAtfDEYYgeycbkQaQBIUqYGne3z4EPMbFrqxkZVdz8JJN9rDohwV2S9dnE
FgIVkvsIA9uzQvbtB1aPXuZrxY5EuKxEOmh4U0IbANkVCD7R1u+Kahl6FKN5NTkM
o9v3VT/ZVtBqr1KdpTiAu+zX4Zne8AU4mPnS/0RHHakiehG6eN1L1QNmmJQq9vHx
zUpvCAxenbPzqsZzExwg8xuEM1DXCkMrdooyrCGxTjjDYpMFNd28NTx9cLgeCX25
bGUSSqRWkwmRiolZteJBJUayMRBz2BSYqaQLFLRTFLMhdeNHiV7gzrwkng+galj0
1Mw/P8GKfd6JDubXxv234D4vyzvdstceOS3a15KNLba5dp7ju2FTT1/pcEHbrFF8
H/sYP5RrwCwpcS083x7th2LvOUFTS9i8R/uWbhtxS0p2iWkWcj0Q6aNB9A3a8sLC
dJ/5T0CrZu1S1SAT6rYDjx7fIvSPuplsbdKl15LXSt2Dk4+acuyk8kHxfU2ycdga
md16YVhZdGOu5YrvZOaE1Zfb4ygNEw8iiAkka8J18uL0mB3yFXCXmGgP5UB0te6W
byQZi9X8QHJ73bd5AUxJAvmqWBnlqVXfDVnKhsVs9vHTI/gOzSNpNAso94+ik8Iw
yAQyDLm5/IbQkI8KKo4F4g2Brye0RKfpFbo6RjBkjfxG6hwvprMJQercxYxLqbzD
o6+AFXqwd5YIAPACdDUmPQKxUsTE3AfoovC+m6uXL1gfqoHIxLT5rdUscswuaBRx
NbXKwL8M9JDYvaiVbuB0DxWlCeaPhyzYrrEw2vyQwxXvM/OnVtuh5KRLa42KtiNO
j10C4Ej3O2qU8P6uOGdYPDJmIyqIDvGtiKynaSH+LpVn8HjidCbKBOC4UzodCIVM
9LemDl4gTthxA+jzVwsanxpoTF/V0v5GI+/z+OBKZ88txx2PUionLvavV+1OCiGd
IMIimKSi1QahiCGPI9Ltrrh3aoPqUm4yzNZ4bwZNRg+ituRUtMUAH3myHtx3+E29
XAhhtaH8j2La0FujH13QdgTIDlJnG6mVduWL6KwH4n5dqNV4Cm7/6YT+6Man1d5/
Lan8dCemCM4r6+nS3ZDX3ve7aIqPAVFPEI/7rpjDo6WbATKycDjluBiHpdpcyT+j
gGy8zeMaY2/vYdc+n6EMesUIWD2ctYGSkm/bXH4SwRV01Becfn6gnK4gV1g2kuiO
DpTyAQE7/NPAx+WodO5i8w==
-----END ENCRYPTED PRIVATE KEY-----
```

3.2. Generamos la petición del certificado

```
/mnt/d/D/I/4/P/Se/Practicas-SSI/Practica_04/certificados on main !2 ?5
openssl req -new -key client-priv.pem -passin pass:hola -subj "/DC=localhost/OU=com/CN=Fsv" -out petic-certifica
do-client.pem

/mnt/d/D/I/4/P/Se/Practicas-SSI/Practica_04/certificados on main !2 ?6 ✔ at 09:38:52
cat petic-certificado-client.pem
-----BEGIN CERTIFICATE REQUEST-----
MIICfDCCAWQCAQAwNzEZMBcGCgmSJomT8ixkARkWCWxvY2FsaG9zdDEMMAoGA1UE
CwwDY29tMQwwCgYDVQQDDANGc3YwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCvmrDv73mbX91+BlBggAZo1QKIyDsuA5sF7YJzO3qdcD2ZUOJecWxw/zDl
PgSP+rAHIKzCWiYDIRFgm52idsMVD6VaGzm+F2jyGDOfQLU2n4ILcAWu9uXodd45
m22LfzwCmlcE1e8j5qFRneZtsGJ47cTIVntuS++1FQJVgIHOZajG1OACUSHCRJ2e
yXW346Uv0jewqd959SqTEroAq3B0BjqccSO0PyVRdVoJhlfC4cT46NBjmKSQKb1L
oJGbxnXBgLBkv91RG+nmF4ahkWSrNgulF9SBpEHx/umq5xGv3BerywDC4Psnb+Nc
LzsmjN1t7U2450icVNcqZtCImN2pAgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEA
HdZX+HopJ8LwLFFJoFCAPw/y6K6ihN/sNDFYWdG54EEH1aoKEXvRDQoursbBxmkr
G5CfUuvMq7YuwCDGWWNA/AkS2Uqo0O3iWx+fjJNC8ONePPzCRsxiSBDQaigx3zZk
vpX5GbyWP8Zk0iNVq307WHdoWeNK+isYI9MxfoOMw2HHefKfpi16h/DJ7IUpmk0r
ORMfq2Uw7k1tb7S4mJ8WLD5dohMfeq0DbTg3iqznKNE8mlfoe3fiX074Si8Dbm53
CL9HadCbiOCygkygReTIRKN8S+p48H4cpXSe42YI58wfXxYs8C8GEbtu0xdwtoGE
QBotSvUyiWz4lRiHzDca7A==
-----END CERTIFICATE REQUEST-----
```

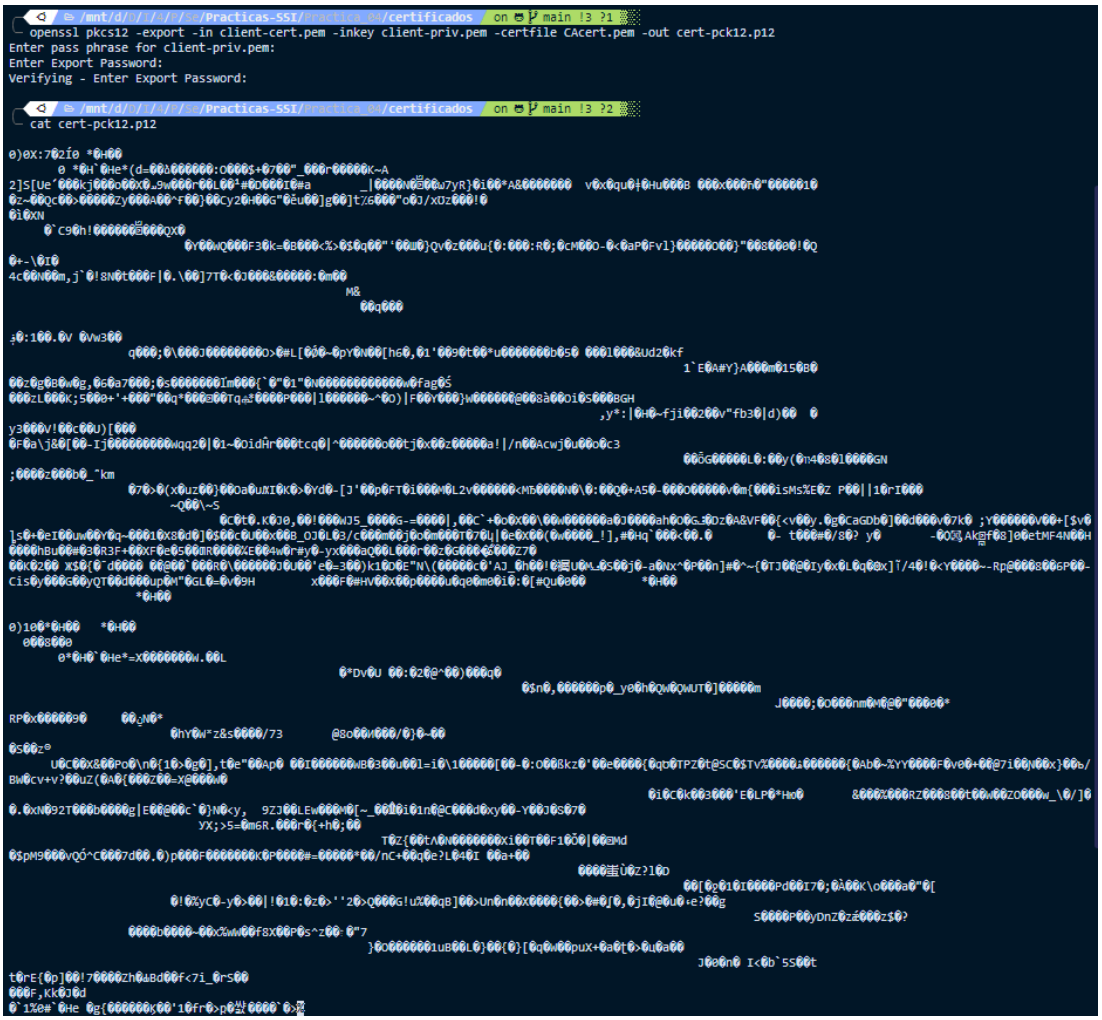
3.3. Generamos un fichero de configuración denominado `config2.txt`

```
/mnt/d/D/I/4/P/Se/Practicas-SSI/Practica_04/certificados on main !2 ?6
touch config2.txt

/mnt/d/D/I/4/P/Se/Practicas-SSI/Practica_04/certificados on main !2 ?7
vi config2.txt

/mnt/d/D/I/4/P/Se/Practicas-SSI/Practica_04/certificados on main !2 ?7
cat config2.txt
basicConstraints = critical,CA:FALSE
extendedKeyUsage = clientAuth
```

3.4. Emitimos el certificado

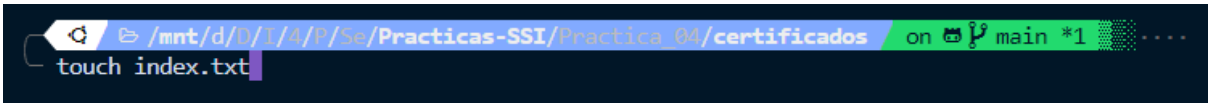
```
/mnt/d/D/I/4/P/Se/Practicas-SSI/Practica_04/certificados on main ····· at 16:39:45
openssl x509 -CA CAcert.pem -CAkey CAkey.pem -req -in petic-certificado-client.pem -set_serial 3 -days 15 -extfi
le config2.txt -out client-cert.pem
Certificate request self-signature ok
subject=DC = localhost, OU = com, CN = Fsv
Enter pass phrase for CAkey.pem:

/mnt/d/D/I/4/P/Se/Practicas-SSI/Practica_04/certificados on main ?1 ···· at 16:41:17
cat client-priv.pem
-----BEGIN CERTIFICATE-----
MIIDiDCCAnCgAwIBAgIBAzANBgkqhkiG9w0BAQsFADBxMQswCQYDVQQGEwJFUzER
MA8GA1UECAwIVGVuZXJpZmUxEjAQBgNVBAcMCUxhIExhZ3VuYTEMMAoGA1UECgwD
VUxMMQ8wDQYDVQQDDAZ1bGwuZXMxHDAaBgkqhkiG9w0BCQEWDWFkbWluQGV1bGwu
ZXMwHhcNMjMxMDE5MDg0MzU3WhcNMjMxMTAzMDg0MzU3WjA3MRkwFwYKCZImiZPy
LGQBGRYJbG9jYWxob3N0MQwwCgYDVQQLDANjb20xDDAKBgNVBAMMA0ZzdjCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK+asO/veZtf3X4GUGCABmjVAojI
Oy4DmwXtgnM7ep1wPZlQ4l5xbHD/MOU+BI/6sAcgrMJaJgMhEWCbnaJ2wxUPpVob
Ob4XaPIYM59AtTafggtwBa725eh13jmbbYt/PAKaVwTV7yPmoVGd5m2wYnjtxMhW
e25L77UVAlWAgc5lqMbU4AJRIcJEnZ7JdbfjpS/SN7Cp33n1KpMSugCrcHQGOpxx
I7Q/JVF1WgmGV8LhxPjo0GOYpJApvUugkZvGdcGAsGS/3VEb6eYXhqGRZKs2C6UX
1IGkQfH+6arnEa/cF6vLAMLg+ydv41wvOyaM3W3tTbjnSJxU1ypm0IiY3akCAwEA
AaNlMGMwDAYDVR0TAQH/BAIwADATBgNVHSUEDDAKBggrBgEFBQcDAjAdBgNVHQ4E
FgQU2zUruAsD7UNxmRFPwoQQ5YAHDDMwHwYDVR0jBBgwFoAUwWKcVHN5Jet6GsyT
4maLxAzgtScwDQYJKoZIhvcNAQELBQADggEBAMJ+9KlnK8JJ5ncB6zXtaj1WI2/6
wPMBq4nTwrfKA1zu9JMydw729tvLLjkiuT5Xk/6b1fm/iTarMSi6uXFub+yNLXNB
g5a96OzVboKfBSv7Lw1V6L7a1A3PWlirnUGcb7MXcgocw2PY1I4Qs2YAS3t/V0Xo
T4o5ePlSEPlESZTlGXkG7SNJHa+WLFtvHT7ecAUg0pauhloPVQzezYldxR1khW4/
+yXkqEPr5CxWX1GFr2Xnjw+xxHJ+wlZJCuJqV3bQeaSpZ3vYSVzJxJN39Y2MqQOV
6wm1wIaOmNdXarSvNFL7qMqmbxvwU1pU6D4bm56BUF+umis0AJrBX6hwbYo=
-----END CERTIFICATE-----
```

4. Exportando los certificados de los clientes



5. Definiendo la lista de revocación

5.1. Generamos un fichero `index.txt`



Lo generamos en el directorio de trabajo para evitar problemas.

5.2. Configuramos `openssl.cnf`

```
#####################################################################
[ CA_default ]

dir   = /home/feichay/Escritorio/Practicas_4to_1er-Cuatrimestre/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL/certificados
certs   = $dir/certs    # Where the issued certs are kept
#crl_dir    = $dir/crl    # Where the issued crl are kept
database  = $dir/index.txt  # database index file.
#unique_subject = no      # Set to 'no' to allow creation of several certs with same subject.
new_certs_dir = $dir/newcerts   # default place for new certs.

certificate = $dir/CAcert.pem   # The CA certificate
serial    = $dir/serial     # The current serial number
#crlnumber  = $dir/crlnumber  # the current crl number must be commented out to leave a V1 CRL
#crl    = $dir/crl.pem    # The current CRL
private_key = $dir/CAkey.pem# The private key

#RANDFILE = $dir/.rand    # private random number file

x509_extensions = usr_cert    # The extensions to add to the cert
```

5.3. Creamos una lista de revocación o CRL

```
~/../Practicas_4to_1er-Cuatrimestre/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL/certificados on main *1 !1 ?2
> openssl ca -gencrl -out listarev.crl -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for /home/feichay/Escritorio/Practicas_4to_1er-Cuatrimestre/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL/certificados/CAkey.pem:

~/../Practicas_4to_1er-Cuatrimestre/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL/certificados on main *1 !1 ?2
> cat listarev.crl
-----BEGIN X509 CRL-----
MIIBtzCBoDANBgkqhkiG9w0BAQsFADBxMQswCQYDVQQGEwJFUzERMA8GA1UECAwI
VGVuZXJpZmUxEjAQBgNVBAcMCUxhIExhZ3VuYTEMMAoGA1UECgwDVUxMMQ8wDQYD
VQQDDAZ1bGwuZXMxHDAaBgkqhkiG9w0BCQEWDWFkbWluQGV1bGwuZXMXDTIzMTAx
OTIxNTUwOFoXDTIzMTExODIxNTUwOFowDQYJKoZIhvcNAQELBQADggEBAKb4I7nh
0X4h1nFpGoLS5hXgt99UsxxkAy6FO/fVGpnOOCGuZTJEmyRiOLUCiH2rb54pdkKt
xL+dh/Mm0CaQdJ2wcjnPF1cMV2w3iL0zO271BZVYMZrblPnuV/uJXJakfjCXEAxS
PEIxToNfRpsb9VtwsDaZN/+WOfrJCGEJX1lw9BvPGPNILjm8vMLdTfEHRF72Vmpx
/zc9zpJ+6IlUznwLhd5/DxxopeiayhPVr4bDAJMYnyqcWqTbrcXCt8suFGIJJF2Y
kN+QN23KZLaAhFv8nMr0HAJ35bARbMazXqHMsSpDm4B4CZBwNR7wtaaamyWam9QC
QMq1FwO4sJ1/Fp4=
-----END X509 CRL-----
```

5.4. Creamos el mismo fichero pero con extensión .pem

```
~/../Practicas_4to_1er-Cuatrimestre/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL/certificados on main *1 !1 ?3
> openssl ca -gencrl -out listarev.pem -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for /home/feichay/Escritorio/Practicas_4to_1er-Cuatrimestre/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL/certificados/CAkey.pem:

~/../Practicas_4to_1er-Cuatrimestre/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL/certificados on main *1 !1 ?3
> cat listarev.pem
-----BEGIN X509 CRL-----
MIIBtzCBoDANBgkqhkiG9w0BAQsFADBxMQswCQYDVQQGEwJFUzERMA8GA1UECAwI
VGVuZXJpZmUxEjAQBgNVBAcMCUxhIExhZ3VuYTEMMAoGA1UECgwDVUxMMQ8wDQYD
VQQDDAZ1bGwuZXMxHDAaBgkqhkiG9w0BCQEWDWFkbWluQGV1bGwuZXMXDTIzMTAx
OTIxNTgzMVoXDTIzMTExODIxNTgzMVowDQYJKoZIhvcNAQELBQADggEBAKL4K7am
dlJ1qENultiEjvqo/Zejx2+rl2bKoOKlynQ0r1NJQNbAsWz3L9Rs84m9FgUFpvxC
e1h+xKw5UdH73EptPvblcsNQvMvFCSdwWAhAU3JthXGjd00EDUmk5AV/ikQ+a7KS
YCRqXMqEcJfdiYbnTruhl/8okQmiM/vJAdHKO4YgYPrdHyTCWaZzK6td9mjySdc6
kCZ/AA3M2ciO3LE3d4ckAUws5siaPk86lzd+tTjnkLuNnkfwuMlOl5R99nKM7oAr
yspbO0ShY5+rt/FVBZOPJ0u3m6MjW7hnMAFaSX+kdngnhMiFAi1uT8g3LnZ09w0A
oJSE6AdjVXGQ9tg=
-----END X509 CRL-----
```

5.5. Revocamos un certificado

```
~/../Practicas_4to_1er-Cuatrimestre/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL/certificados on main *1 !1 ?3
> openssl ca -revoke client-cert.pem -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for /home/feichay/Escritorio/Practicas_4to_1er-Cuatrimestre/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL/certificados/CAkey.pem:
Adding Entry with serial number 03 to DB for /DC=localhost/OU=com/CN=Fsv
Revoking Certificate 03.
Data Base Updated

~/../Practicas_4to_1er-Cuatrimestre/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL/certificados on main *1 !1 ?5
> cat index.txt
R       231103154937Z   231019215909Z   03      unknown /DC=localhost/OU=com/CN=Fsv
```

Actualizamos la lista de revocación: