

1.1 Generación de una autoridad certificadora

Se crea el certificado y la clave privada de la CA con el siguiente comando:

```
certificados (deleted) : bash — Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
root@turbomachine:/home/martin/repos/ssl/4practica# openssl req -x509 -newkey rsa:2048 -days 1095 -keyout CAkey.pem -out servidor-cert.pem
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'CAkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:ES
State or Province Name (full name) [Some-State]:Tenerife
Locality Name (eg, city) [:]:La Laguna
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ULL
Organizational Unit Name (eg, section) [:]:
Common Name (e.g. server FQDN or YOUR name) [:]:Martin
Email Address [:]:alu0100832211@ull.edu.es
root@turbomachine:/home/martin/repos/ssl/4practica#
```

Se le está indicando que use una clave privada con RSA de 2048 bits para 1095 días.

1.2 Generación del certificado del servidor

En este paso se simula cómo un servidor pediría el certificado a una CA.

Se genera la clave privada del servidor. (Desde el servidor)

```
root@turbomachine:/home/martin/repos/ssl/4practica# openssl genrsa -des3 -out serv-priv.pem -passout pass:clave 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x010001)
root@turbomachine:/home/martin/repos/ssl/4practica#
```

Con esa clave privada, se genera una petición de certificado que define al servidor como propietario. (Desde el servidor)

```
root@turbomachine:/home/martin/repos/ssl/4practica# openssl req -new -subj "/DC=root.com/OU=com/CN=root" -key serv-priv.pem -passin pass:clave -out petic-certificado-se
rv.pem
root@turbomachine:/home/martin/repos/ssl/4practica# cat petic-certificado-serv.pem
-----BEGIN CERTIFICATE REQUEST-----
MIICfDCCAQwCAQAwNzEYMBYCCg5JontB1xkARKkH3vb3QuY29tMQwwCgYDVQQL
DANjY20xDTALBgNVBAMMBHJ3b3QwggE1MA0GCSqGSIb3DQEBAAQAA4IBDwAwggEK
AoIBAQCC4VU9ftFny2wRvU7MM5U8E7G0H8Mx/U8CFD0nOULBxAQdT/PtaqNESbNAC
tj3ZgXKCLm6xsJ0wN7pZ8IYwVr9zgTArU5pwvFXK5+TZzonfJxafJ3LrSYEOJ3W
k82HAHL9JMMwjxgtAKg8XoN+szqwsEHRsANT0BU9BSvaysvE0Fs/aY03wEKZ0P2
R/oh2Bwzm+JA7ZGeN+PCv1EFEUvt+yXsdwCqEH+RzNWLh42aUoWixjXMTzyiF30
+WC0FKL1S9KLZJU1dF4uu5b2S0k09Ryxj296PykZnj5P3BMJ81gEzzR2ooQUQ2f
Ey+jVJLn1bBPS/L3s+Uau6JUF7j7rAgHBAAGGADANBgkqhkiG9w0BAQsFAAOCAQEA
Aho3UKZS9UZEj65m34PuSB3NDN6ACW9s4TSmg8E/8UY5K4nhVqd1QuIyV4c9c7Q3
MoEpBy6W7DLXp/xPhSBAHm1lBReCrnMJL92LQMyP/+MhxwVzFNKnZWAESNFAH14
52Fw63vn8I2LwLFUBuyY3KsVnhfFwFagLpgWbVnH39LHU5K0C13uU7JHrC81C
0jy4LEQH8w7xxHqj/Xm3z4BIZHRM37CedRQERLNCz3d3vz84LuSka09eacY9Q
06pXUJtkW/0IYjYe7H0eHn0ePtMZzE89pJ3qfbzy9eyWhgdb7mMH0DWTGE5DQU
8AkWJ618uJwjr01V7F9470=
-----END CERTIFICATE REQUEST-----
root@turbomachine:/home/martin/repos/ssl/4practica#
```

Con esa petición, la CA emite el certificado del servidor usando el certificado de la CA y la clave privada de la CA.

```

certificados git:(master) ✗ sudo openssl x509 -CA CAcert.pem -CAkey CAkey.pem -
req -in petic-certificado-serv.pem -days 15 -extfile config1.txt -sha1 -CAcreatese
rial -out servidor-cert.pem
[sudo] password for martin:
Signature ok
subject=DC = root.com, OU = com, CN = root
Getting CA Private Key
Enter pass phrase for CAkey.pem:
certificados git:(master) ✗ cat servidor-cert.pem
-----BEGIN CERTIFICATE-----
MIIDazCCAlOgAwIBAgIJAPZ4qCvLXrOrMA0GCSqGSIb3DQEBBQUAMIGLMQswCQYD
VQQGEwJFUzERMA8GA1UECAwIVGVuZlZpZmUxEjAQBgNVBAcMCUxhIEExhZ3VvYTEM
MAoGA1UECgwDVUxMMQ0wCwYDVQQQLDAREcHRvMQ8wDQYDVQQDDAZNYXJ0aW4xJzAl
BgkqhkiG9w0BCQEWGfSdTAXMDA4MzIyMTFAdWxsLmVkdS5lczAeFw0xODExMDkx
MzUxNTRAFw0xODExMjQxMzUxNTRAMDCxGDAWBgoJkiaJk/IsZAEZFghyb290LmNv
bTEMAoGA1UECwwDY29tMQ0wCwYDVQQDDARyb290MIIBIjANBgkqhkiG9w0BAQEFA
AOCAQ8AMIIBCgKCAQEAzrGrJPfCNaRhJMuvzEirtRQQPSQfY6womlB02EyQGmx2
BPtrxjZUWDmtAva7iAXG2l0Vh5GDGBF1VQnE4tRFHFU/NQu6kPZbkfol/J56pVLO
TcdZ4Q02ZZDQLGpiUJwDFbjXP5xFsgRgB+dKPyYmigAzamycUgOsaKiIDxQLV5+P
eXpO6UVU40SuAqO+FTEM9lyeD2hPzgdwv/sAObtUnzsxONWbKdAz5W9IhDDGALmn
ABFZBHo7MPIdC95Ac5wHFLLEXyVSiP0BLPBd1isbGT24kLUMbbwBNf5drw22qXFm
OmHV0J7YUTeIIa/I/iZJD5cii0bjaB90g4jt1odnMQIDAQABoyUwIzAMBgNVHRMB
Af8EAJAAMBGA1UdJQMMAoGCCSGAQUFBwMBMA0GCSqGSIb3DQEBBQUAA4IBAQAAL
kBBfMr/KvXJ3Hzoss9d8rQvcefCglPVqS0tJrA09xFao3Wu43YNLSdI1ZzPwZj7sg
5fKHUqZR8oIt1s1XE413YF5x2egzj2REoTCD/0LzkpSDj/PJzUsjIkfJSNRhaJu0
4kLOxf6VjfmI8YGxrwYOC/FidQR9GLtQtS4qNFgGtz7mkZUJ/D6Ijpze++avyfil
CfqomhikvgDXpLL590EJNimdjtDfYbJp3on9v5PwuiEjcwAHn+dBa813qzcAYEMw
8JI87k2dbDFYnDuHgV9Qs9tN/kkwmU1icZf58js8LMWxiZ4s6GwCCqnhSx/wbUHV
btbRP0n10/Aq0Jg+txw4
-----END CERTIFICATE-----
certificados git:(master) ✗ █

```

1.3 Generación de los certificados de los clientes

En este paso se simula la transacción entre un cliente y la CA para que el cliente obtenga un certificado que pueda usar en internet.

Se crea la clave privada del cliente (en el cliente).

```

root@turbomachine:/home/martin/repos/ssi/4practica/certificados# openssl genrsa -d
es3 -passout pass:clave -out client-priv.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x010001)
root@turbomachine:/home/martin/repos/ssi/4practica/certificados# █

```

Con esa clave privada se crea una petición para obtener un certificado de la CA

```

root@turbomachine:/home/martin/repos/ssi/4practica/certificados# openssl req -new
-key client-priv.pem -passin pass:clave -subj "/DC=localhost/OU=com/CN=Fsv" -out p
etic-cert-client.pem
root@turbomachine:/home/martin/repos/ssi/4practica/certificados# ls
CAcert.pem  client-priv.pem      petic-certificado-serv.pem
CAcert.srl  config1.txt          serv-cert.pem
CAkey.pem   petic-cert-client.pem serv-priv.pem
root@turbomachine:/home/martin/repos/ssi/4practica/certificados# cat petic-cert
cat: petic-cert: No such file or directory
root@turbomachine:/home/martin/repos/ssi/4practica/certificados# cat petic-cert-cl
ient.pem
-----BEGIN CERTIFICATE REQUEST-----
MIICfDCCAWQCAQAwNzEZMBcGCgmSJomT8ixkARkWCWxvY2FsaG9zdDEMMAoGA1UE
CwwDY29tMQwwCgYDVQQDDANGc3YwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDGG6n32Jgi1wxvZVcdht+DHILYW7oV9bfx8iI++BTs7mDLAE3l0ZEr01CcZ
xWttMTY1oYcb5XxJ7a7ncHkE8xXBD+QTL609mil50MJPnH+LM0M1qX5QUE2qmkyu
2VCM60Uug6ogXd961jW1HLBUfxkpG5sWY2kqyl/cKvIsv8SVhhEM0b10owD4mXqz9
vmMEY1/7rglknmbJUS4wBUZu2k/aR+vu4iZLLh+1uBxku6GX6HpAp2mXSfwAXV05
mrD+6V//ukeRmNyDjtIfU8g005E0M0UdqWsRQDBKjccwWVaFwWrr6Tm6sgrsub0s
yJvbL+0H4lRj4tXCWSg1YstAhbNTAgMBAAGgADANBgkqhkiG9w0BAQsFAA0CAQEA
fjbl/et2MAx8JJISPje16KgV8PJ0eG6R/6C3rLimmw1fleXZfyeONnH509XnLv7L
sGHLhDrTDt+SToc+/kT4ntRttbAW1UTalODu887inqp64RitskCEWIMY9gTbU4PD
Zom7IkhFrL+wfpGt9ViPifnVenli796hGEjpfKhV49VdWl01ADp6iizJo/Yw0y+t
3Lb+sLNZ8G+04WGvcDagYQUjDlyJ7Jg8LQhbNCL+J0nWdZOAD35EVxPnTVV1lr8+
1BsnT6/s50NEttUHFf99YYbmgBH/kPDjiD/oEmwYco7Xq1nYxjdAPd0NhOrjTP8
QDC6cINxuVtodIvMQ8Nh/Q==
-----END CERTIFICATE REQUEST-----
root@turbomachine:/home/martin/repos/ssi/4practica/certificados#

```

Con la petición, la CA usa su certificado y su clave privada para crear el certificado del cliente mediante el comando

```

openssl x509 -CA CAcert.pem -CAkey CAkey.pem -req -in
petic-cert-client.pem -set_serial 3 -days 15 -extfile config2.txt
-out client-cert.pem

```

1.4 Exportando los certificados de los clientes

Se exporta a un formato estándar que el navegador entiende: pkcs12.

Este paso se dará en el lado del cliente.

Con el certificado del cliente, la clave privada del cliente y el certificado de la autoridad certificadora se genera un fichero que es el que el cliente debe instalar en su navegador.

```

root@turbomachine:/home/martin/repos/ssl/4practica/certificados# openssl pkcs12 -e
xport -in client-cert.pem -inkey client-priv.pem -certfile CACert.pem -out cert-pc
k12.p12
Enter pass phrase for client-priv.pem:
Enter Export Password:
Verifying - Enter Export Password:
root@turbomachine:/home/martin/repos/ssl/4practica/certificados# ls
CACert.pem  cert-pck12.p12  config1.txt      petic-certificado-serv.pem
CACert.srl  client-cert.pem config2.txt      serv-cert.pem
CAkey.pem   client-priv.pem petic-cert-client.pem serv-priv.pem
root@turbomachine:/home/martin/repos/ssl/4practica/certificados# cat cert-pck12.p1
2
00000000 *H
00000000 I$00000000VG0V00@300x0*000n0eb00:v)0M000~fE\00000000F00<00)g0y0pJ=&00-V{0_0jp+00
0RR00E00q\ : *80u00it70 00k00hk0`050006q;X!0000
                                $D0=0]0"0 _sC0J00
                                )N0Wr0Z0x0%000000
00K.00X00!:9o\mu)"0b00.@P0&00F00h00N00)0Et0I0000?0j0;
**0l0^'.0000
\0q.Km0'@000h000B000000070'00R0F^0:0ie50L0
                                000>00<0_0R/a0&G0qVLYy+0D00B00M00000a0100
000nbd.00,n00y070 000T0000d000M%00@dd0 0J00x00000000t06=06
-my000V0<u0gC 0E02Y,0
P00 bNoA?0{0d:0N00%
0F0-00U000ic4^0U000J000000V00Uj00}00X00L00Y
$0000
0#L00Q0BC000#V00W00 K+iU00lk000*^Y000y00800
                                /0m000h.U00h>h-W-#zb00-0070j0
00700U?FD000
00B'0y<KT000000$000_0?00$000i000:05I0\p00g0T0r000em00M00 0000uS&00Y000w0-J0.=00ü
000^00005)00 30 0l00X0h0000w00'H-0

```

1.5 Definiendo la lista de revocación

El archivo que define los certificados revocados se encuentra en /etc/ssl/index.txt

Se configura correctamente /etc/ssl/openssl.cnf

```

#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName

# This really needs to be in place for it to be a proxy certificate.
proxyCertInfo=critical,language:id-ppl-anyLanguage,pathlen:3,policy:foo

#####
[ tsa ]

default_tsa = tsa_config1      # the default TSA section

[ tsa_config1 ]

# These are used by the TSA reply generation only.
dir           = ./demoCA      # TSA root directory
serial        = $dir/tsaserial  # The current serial number (mandatory)
crypto_device = builtin       # OpenSSL engine to use for signing
signer_cert   = $dir/tsacert.pem # The TSA signing certificate
                                # (optional)
certs         = $dir/CAcert.pem # Certificate chain to include in reply
                                # (optional)
signer_key     = $dir/private/tsakey.pem # The TSA private key (optional)
signer_digest  = sha256        # Signing digest to use. (Optional)
default_policy = tsa_policy1    # Policy if request did not specify it
                                # (optional)
other_policies = tsa_policy2, tsa_policy3 # acceptable policies (optional)
digests        = sha1, sha256, sha384, sha512 # Acceptable message digests (mandatory)
accuracy       = secs:1, millisecs:500, microsecs:100 # (optional)
clock_precision_digits = 0      # number of digits after dot. (optional)
ordering       = yes          # Is ordering defined for timestamps?
                                # (optional, default: no)
tsa_name       = yes          # Must the TSA name be included in the reply?
                                # (optional, default: no)
ess_cert_id_chain = no        # Must the ESS cert id chain be included?
                                # (optional, default: no)

"openssl.cnf" 346L, 10774C                                     338,8      Final

```

En este fichero de configuración se ha especificado que el directorio donde van a estar el certificado, la clave privada y el número de serie de la CA es /etc/ssl/demoCA, la estructura de este directorio es la siguiente

```

root@turbomachine:/etc/ssl# tree demoCA/
demoCA/
├── CAcert.pem
├── CAcert.srl
├── index.txt
├── index.txt.attr
└── private
    └── CAkey.pem

1 directory, 5 files

```

Se crea un fichero crl y pem que representa la lista de revocación mediante el comando

```
openssl ca -gencrl -out listarev.pem
```



```
openssl ca -gencrl -out listarev.crl
```

```
root@turbomachine:/etc/ssl# cat listarev.crl
-----BEGIN X509 CRL-----
MIIB0jCBuzANBgkqhkiG9w0BAQsFADCBizELMAkGA1UEBhMCrVMxETAPBgNVBAGM
CFRlbmVyaWZlMRIwEAYDVQQHDAIMYSBMYWd1bmExDDAKBgNVBAoMA1VMTDENMA
A1UECwwERHB0bzEPMA0GA1UEAwGTWFydGluMScwJQYJKoZIhvcNAQkBFhhhhbHUw
MTAwODMyMjExQHVsbC5lZHUuZXMxDTE4MTEwOTEzNDA0MFOxDTE4MTIwOTEzNDA0
MFowDQYJKoZIhvcNAQELBQADggEBAJ6wuV+h9lFKAZm72UAhmJ8kSj1TQFKIMg+g
ELpl80E1870vFM9mr4sTS02cg01zly3a8bdATrUGLxB2k8+UP1ROGArhRWD0VmtY
FgImkDYZRHjLqkyi9LUVu2h8ns983RsojofWs/YnOXnRY/1qnWTOrdPEPGNv3/nn
t02uha6gvzDEs1Dh+9LNx8rh7/MWTgUhSqA5CDI5fI1HGcRc3yup7KRvPLmoPxNe
+s8Gwv/+yeb8RW5PLPQU9K0VXPKKsPzVI58rz4PTJSqjm9c8MbME1QR3J3XHc8ER
us0isGrr02aOCVAL900hz/Nkji6xS+zjyJZwqX9wPK9M8JH4hrY=
-----END X509 CRL-----
```