CERTIFICADOS DIGITALES

Práctica 4

Índice

Errores

Cuando he creado la Autoridad certificadora subordinada, la creé dentro de la autoridad certificadora raíz. Esto no es lo más correcto, por lo que llegado a un punto de la práctica que se especificará más adelante, lo cambié y la saqué fuera.

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ mv ca/subordinada/ .
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ ls
ca  certificados.pdf  client  subordinada
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ subl subordinada/openssl.cnf
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ cat subordinada/openssl.cnf | grep dir
    =
grep: =: No such file or directory
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ cat subordinada/openssl.cnf | grep dir

# Localización de ficheros y directorios
dir               = /home/pedro/Documents/git/inform-4-SPSI/p4/subordinada
certs             = $dir/certs
crl_dir           = $dir/crl
new_certs_dir     = $dir/newcerts
database          = $dir/index.txt
serial            = $dir/serial
RANDFILE          = $dir/private/.rand
private_key       = $dir/private/subordinada.key.pem
certificate       = $dir/certs/subordinada.cert.pem
crlnumber         = $dir/crlnumber
crl               = $dir/crl/subordinada.crl.pem
#       - El país, la provincia y el nombre de la organización, deben coincidir
#       - El ON debe coincidir con la Autoridad Certificadora Intermedia
# Extensión a añadir cuando se usa la opción -x509
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$
```

Crear una autoridad certificadora

1. Creamos la estructura de directorios

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ mkdir -p ca/{certs,crl,csr,newcerts,private}
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ chmod 700 ca/private
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ touch ca/index.txt
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ echo 1000 > ca/serial
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ ls -la ca/
total 32
drwxr-xr-x 7 pedro pedro 4096 Nov 24 05:17 .
drwxr-xr-x 3 pedro pedro 4096 Nov 24 05:14 ..
drwxr-xr-x 2 pedro pedro 4096 Nov 24 05:14 certs
drwxr-xr-x 2 pedro pedro 4096 Nov 24 05:14 crl
drwxr-xr-x 2 pedro pedro 4096 Nov 24 05:14 csr
-rw-r--r-- 1 pedro pedro    0 Nov 24 05:16 index.txt
drwxr-xr-x 2 pedro pedro 4096 Nov 24 05:14 newcerts
drwx------ 2 pedro pedro 4096 Nov 24 05:14 private
-rw-r--r-- 1 pedro pedro    5 Nov 24 05:17 serial
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$
```

- Certs: es el directorio donde se guardarán los certificados emitidos.
- Newcerts: es el directorio donde se guardarán los nuevos certificados.
- Private: es el directorio donde se guardarán las claves privadas de la entidad.
- Csr: Es el directorio donde se guardarán las peticiones de firma de certificado. (Certificate Signing Request)

Además, se han recado los archivos:

- Index.txt: Es índice de la base de datos de los certificados.
- Serial: se guarda el número del siguiente certificado firmado.

2. Preparamos el fichero de configuración ca/openssl.cnf

```
[ CA_default ]
# Localización de ficheros y directorios
dir               = /home/pedro/Documents/git/inform-4-SPSI/p4/ca
certs             = $dir/certs
crl_dir           = $dir/crl
new_certs_dir     = $dir/newcerts
database          = $dir/index.txt
serial            = $dir/serial
RANDFILE          = $dir/private/.rand
```

```
# Opcionalmente se pueden especificar algunos valores por defecto
countryName_default             = ES
stateOrProvinceName_default     = Granada
localityName_default            = Granada
0.organizationName_default      = SPSI
organizationalUnitName_default  = utoridad Certificadora de SPSI
emailAddress_default            = plfuertes@correo.ugr.es
```

```
# Estas extensiones se aplican cuando se firman certificados
# hay que pasar `-extensions v3_ca` para aplicar esta opciones
[ v3_ca ]
# Extensiones para una típica CA (`man x509v3_config`).
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always,issuer
basicConstraints        = critical, CA:true
keyUsage                = critical, digitalSignature, cRLSign, keyCertSign
```

3. Creamos la nueva clave raíz en ca/private

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ openssl genrsa -aes256 -out private/ca.key.pem 4096
Generating RSA private key, 4096 bit long modulus
.....................................................................................................
...++
.....................................................................................................
.....................................++
e is 65537 (0x10001)
Enter pass phrase for private/ca.key.pem:
Verifying - Enter pass phrase for private/ca.key.pem:
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ chmod 400 private/ca.key.pem
```

4. Creamos el certificado raíz

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ openssl req -config openssl.cnf \
>         -key private/ca.key.pem \
>         -new -x509 -days 7300 -extensions v3_ca \
>         -out certs/ca.cert.pem
Enter pass phrase for private/ca.key.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.
-----
Nombre del país (Código de 2 letras) [ES]:
Provincia o Estado [Granada]:
Nombre de la localidad [Granada]:
Nombre de la organización [SPSI]:
Nombre de la unidad organizativa [utoridad Certificadora de SPSI]:
Nombre Común []:SPSI Autoridad Raiz
Correo electrónico [plfuertes@correo.ugr.es]:
```

- Openssl req: permite solicitar certificaciones. Las solicitudes se pueden crear con claves previamente creadas o crearlas en el momento.
- - config: permite utilizar un archivo de configuración alternativo, en este caso, el creado previamente en el punto 2. Por eso algunos puntos ya nos salían rellenos.

- -key: indica la clave privada con la que firmar las solicitudes
- -new: crea una nueva solicitud de certificado
- -x509: para que el cetificado que se cree esté autofirmado
- -days: el número de días en los que expirará el certificado. (20 años en este caso)
- -extensions: Indica la extensión del certificado que se agregará al emitir cada certificado, en este caso v3_ca como se ha especificado en el archivo openssl.cnf
- -out: indica dónde se almacenará el certificado que permitirá firmar otras solicitudes de certificado como verificar la identidad de los solicitantes.

5. Archivos generados

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ ls -lsR
.:
total 32
4 drwxr-xr-x 2 pedro pedro 4096 Nov 24 05:35 certs
4 drwxr-xr-x 2 pedro pedro 4096 Nov 24 05:14 crl
4 drwxr-xr-x 2 pedro pedro 4096 Nov 24 05:14 csr
0 -rw-r--r-- 1 pedro pedro    0 Nov 24 05:16 index.txt
4 drwxr-xr-x 2 pedro pedro 4096 Nov 24 05:14 newcerts
8 -rw-r--r-- 1 pedro pedro 6106 Nov 24 05:27 openssl.cnf
4 drwx------ 2 pedro pedro 4096 Nov 24 05:31 private
4 -rw-r--r-- 1 pedro pedro    5 Nov 24 05:17 serial

./certs:
total 4
4 -rw-r--r-- 1 pedro pedro 2244 Nov 24 05:35 ca.cert.pem

./crl:
total 0

./csr:
total 0

./newcerts:
total 0

./private:
total 4
4 -r-------- 1 pedro pedro 3326 Nov 24 05:31 ca.key.pem
```

Aquí puede verse como a parte de los ficheros generados, en el punto 1, se ha creado una clave privada llamada ca.key.pem (Punto 3) en la carpeta ca/private, así como un certificado autofirmado en /ca/certs llamado de la misma forma (Punto 4).

6. Valor de las claves generadas

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ openssl rsa -text -in private/ca.key.pem
Enter pass phrase for private/ca.key.pem:
Private-Key: (4096 bit)
modulus:
    00:c1:a5:1a:b2:b6:38:fd:53:83:c6:9a:71:c3:9f:
    a2:29:ed:a3:c8:87:92:eb:84:b2:d9:a9:22:64:fd:
    a9:b2:01:f4:75:96:32:89:5a:bd:b0:05:b8:cf:07:
    ba:3a:a9:d2:5e:03:c5:c2:d6:45:82:75:64:cb:cf:
    e6:77:f6:24:ab:dc:04:4b:72:85:81:6f:c8:0b:0e:
    38:6d:9e:ab:5b:47:2c:d5:48:2b:52:c1:75:fd:6f:
    e2:b9:a5:83:57:22:b8:75:67:4f:01:d8:f1:d2:e2:
    86:a0:ff:14:32:9b:77:56:c8:70:50:ec:d7:c7:3c:
    3d:61:96:e3:cc:45:6c:46:ba:68:8f:10:66:0e:22:
    a3:69:67:20:3e:99:42:92:03:3b:40:e7:93:b8:61:
    81:33:63:4c:d7:4b:b0:b6:91:2b:78:fa:56:d5:4c:
    42:d0:bb:67:61:8c:3e:71:80:90:e5:68:68:c9:f0:
    0c:8e:6c:8f:41:e4:a6:45:25:a5:f1:aa:68:f3:48:
    06:cd:32:a7:65:d3:f4:ec:c6:4b:2c:75:8f:da:a5:
    38:6d:86:27:9e:ac:27:b3:3e:04:9a:85:40:90:7e:
    aa:c4:28:91:83:ce:04:1c:fd:fa:98:d4:53:b8:ed:
    1c:77:fc:34:45:d3:e5:89:e1:a4:ad:1d:16:89:28:
    33:9e:69:bd:47:6b:65:34:14:c0:40:4f:f8:1e:2f:
    a8:16:a8:7c:93:b7:40:e9:a1:e9:1c:d1:e7:96:19:
    a5:a4:ac:7a:97:dd:cd:cf:ca:8a:d4:5c:11:ec:79:
    0c:09:62:9f:87:31:e2:06:0d:3b:62:75:c5:a4:7a:
    f9:e4:5a:01:95:fb:e3:32:18:59:71:0e:3d:18:0c:
    fb:f0:d7:83:8d:9c:bf:0e:fc:6a:d4:96:ad:1d:77:
    e4:25:32:8a:32:e0:4c:31:f6:52:5d:3c:fb:e2:e2:
    70:71:aa:2b:10:b6:75:65:eb:dc:67:ef:12:7e:51:
    0b:0b:01:6b:17:ce:c9:81:18:61:9a:02:9d:f4:44:
    1c:09:e0:0f:0a:b3:9a:78:69:4d:02:bd:8f:f8:f8:
    6a:e2:d7:e8:b0:3a:d1:31:8a:b0:5b:ab:ff:e3:57:
    6e:78:4b:d1:f3:db:d5:16:ba:aa:86:8c:e9:9a:7e:
    04:b4:89:4d:3d:e2:7b:45:6e:71:ed:71:9b:1c:3a:
    b3:b9:59:41:39:36:a3:1c:c8:88:dc:99:49:d9:09:
    62:ba:87:07:a7:6e:2e:ff:4c:e1:a3:94:82:5f:6a:
    00:4e:e0:cf:92:9d:28:8b:66:e7:f8:ca:e9:b5:20:
    75:e7:04:87:37:6e:f8:60:1d:63:89:99:de:b9:fa:
    27:74:29
publicExponent: 65537 (0x10001)
privateExponent:
    02:ad:4f:a3:2c:d5:b8:da:d0:b5:8c:29:0a:75:48:
    7e:9f:e4:65:bf:4a:0e:ab:74:f5:81:5b:12:5e:57:
    5c:38:9e:b2:89:73:05:67:15:bc:3b:38:04:d4:ac:
    84:67:18:9b:68:1d:f1:c5:98:8c:67:27:0f:92:3e:
    33:66:59:b7:6e:81:38:b1:ca:9a:b1:7a:e8:7c:37:
    d7:7c:1c:0e:54:fb:8f:af:41:ba:11:26:9a:6c:53:
    8c:11:77:b1:5a:af:86:1f:f9:7d:a3:0c:24:c8:30:
    e8:44:de:78:9c:a1:97:b7:89:a5:f4:c0:3e:e6:dc:
    4a:5f:15:a3:1b:4a:95:e7:b9:ce:50:81:b8:ac:4d:
    ea:05:1c:f3:00:97:65:01:5a:6e:59:45:37:85:51:
    8d:ee:4f:7f:a2:72:3c:f3:e0:cf:f9:55:fd:f8:e1:
    eb:94:cb:a7:13:93:41:6a:6f:96:5c:4d:26:8d:84:
    fe:eb:0d:47:f1:eb:42:85:74:b7:d4:8d:42:df:ba:
    08:58:2c:ec:41:73:df:5a:16:6b:f4:ec:1a:2f:b2:
    8a:01:12:c7:24:c6:1f:ba:39:c2:11:19:85:65:da:
    e2:7f:55:13:a7:63:73:2b:27:ad:b9:31:b7:1a:c0:
    0c:00:96:90:68:8f:81:ca:76:c6:55:e2:9b:de:cc:
    67:dc:12:11:e1:c4:25:48:6b:7f:28:5f:94:de:1f:
    e8:89:31:01:64:04:25:36:58:5f:b6:3b:4f:c1:91:
    9e:f3:4f:43:5f:e7:76:15:ac:d9:7f:a5:53:a6:79:
    3e:a3:0d:ae:19:7e:b2:10:00:fa:30:8e:c6:56:94:
    40:02:06:cb:9f:e1:24:3f:95:33:37:c1:49:d4:42:
    69:ef:36:6d:b4:a2:5e:af:d1:c7:67:7e:52:47:f0:
    a4:9e:ed:28:a8:4f:2b:4c:bb:97:85:c4:37:69:16:
    ce:5c:f6:fc:ee:9e:48:14:49:d6:1b:12:8f:50:e0:
    c9:bf:53:ca:05:dd:5c:81:f0:94:d6:03:46:1c:9b:
    29:65:9f:7a:54:2f:e8:72:76:7b:25:12:02:ec:e9:
    24:f4:40:b5:a9:16:e0:51:19:fd:4e:3a:23:64:e8:
    be:1e:40:67:1a:ef:04:a6:c4:ad:86:6c:0a:b3:ba:
    54:ce:54:59:e9:e9:ad:b0:f4:5d:94:ee:3c:7b:e3:
    3a:69:8b:8d:0b:2d:fc:27:88:f7:74:40:ee:32:8a:
    3f:a0:84:0b:8e:e1:b9:1c:a5:0a:3f:96:7f:32:8f:
    9d:3a:bc:ad:c0:0d:37:60:99:21:5e:99:5a:39:de:
    c9:0e:ad:ca:ef:01:20:6b:f5:44:cd:7a:d6:50:ef:
    fc:49
prime1:
    00:e3:57:f4:b7:ff:59:3a:ff:2f:33:34:35:5e:36:
    2f:84:d9:b3:c7:3a:c9:c0:9c:6e:1d:f9:7f:f4:c9:
    a0:af:86:83:c3:61:11:b2:be:ae:36:42:e0:32:21:
    10:3c:e2:c0:7f:ae:24:5e:6d:20:c4:cc:aa:2f:dc:
    7e:65:b8:49:67:07:ee:00:33:b8:e0:74:b0:8d:8b:
    74:43:03:08:57:54:3d:88:cb:55:56:8e:f7:80:16:
    dd:aa:7e:7b:12:e3:06:f3:6b:0f:fe:60:b6:47:ae:
    f5:dc:65:11:a3:1e:8b:34:8a:d2:65:c8:1b:a4:18:
    df:2a:18:b2:8b:fb:24:12:1c:04:83:c9:e6:1f:27:
    2c:51:9a:86:a5:c8:ee:eb:ee:14:68:09:44:c7:dd:
    36:87:dc:ce:e5:a6:a0:f5:e8:60:21:17:86:d5:49:
    55:3e:e4:fc:fb:22:6a:a4:62:02:68:3c:26:5d:fa:
    40:7d:f1:67:6d:da:a9:c5:61:ab:51:47:be:3c:b4:
    6e:77:68:2c:6b:38:3b:71:d5:11:62:c6:5e:66:f5:
    17:1b:6b:79:82:4c:4a:ab:85:b0:46:90:77:c8:23:
    9d:dc:85:7e:97:9b:36:60:c9:2e:34:76:1f:47:fc:
    d4:5f:bf:aa:5d:ee:47:85:26:08:37:e1:c0:19:7b:
    37:0f
prime2:
    00:da:0d:be:1e:c3:5e:5d:35:09:3c:c4:b0:63:97:
    94:52:1b:14:c5:34:ae:b7:98:f5:2c:02:ff:db:01:
    2a:b7:f2:c1:44:01:f0:11:51:2f:9d:61:9d:01:27:
    b1:4a:f2:23:0b:44:65:28:93:fe:92:bf:a5:b5:31:
    02:fa:d7:3e:43:43:36:53:a4:14:96:c0:9c:2e:8e:
    f2:cb:c8:08:14:3a:f9:85:93:48:a3:a8:1a:06:cc:
    8e:4b:13:2e:a0:d0:b2:1a:62:fd:be:65:b8:62:bf:
    60:be:22:23:eb:70:16:75:39:2c:2a:ba:2b:73:d6:
    de:63:09:ad:b1:be:6f:4e:4c:b6:1a:c5:53:b0:2e:
    81:c8:fb:07:41:be:24:cb:18:66:d4:ea:bb:46:92:
    cc:21:3c:81:51:9f:b6:73:5a:3b:e7:be:a6:3e:4a:
    b5:b3:7d:40:87:f0:63:3f:29:5a:03:75:30:60:2c:
    35:b1:be:19:a1:63:1f:27:a2:79:24:55:3a:5a:c2:
    2c:b6:58:09:32:8b:47:c2:e3:8c:b4:6d:4f:d5:ba:
    72:9a:9b:97:e7:00:a8:a8:a9:af:4f:fe:ae:41:8f:
    e4:e8:9f:d6:c8:3e:f1:0c:c2:1e:de:04:96:a1:5e:
    d0:ad:04:20:e7:34:13:c4:68:3d:5b:4e:f9:f0:f9:
    e1:47
```

```
exponent1:
    00:ba:1d:83:86:2e:51:4a:6f:26:a0:f0:98:d0:2b:
    e3:f3:0a:96:96:ff:95:b3:4d:5d:08:c4:fc:ef:d5:
    30:eb:01:60:55:4e:de:42:4a:c0:2c:43:cb:6e:be:
    8a:a0:8d:b1:b1:d5:4a:88:d3:26:04:76:d8:cc:9d:
    e2:0c:3c:36:3b:56:ce:8c:f3:ca:e2:56:25:43:7b:
    6b:0e:81:29:0e:f5:33:fb:0d:1b:2b:e5:96:d1:11:
    e7:1e:70:b5:28:dd:1b:0f:a4:12:4f:d9:b4:e0:32:
    67:ac:aa:41:2a:1d:13:31:4c:84:ba:36:7c:0a:77:
    22:1b:40:64:cb:1c:2a:87:78:d0:69:63:9c:34:dc:
    c8:f7:75:5d:cd:d3:15:65:a8:5e:a4:5d:12:25:dc:
    ff:8b:72:45:1e:d4:ae:e9:21:f7:b0:9f:a6:0e:6e:
    1e:8f:82:bf:68:88:e0:6c:fa:9f:a5:dd:b8:3b:2f:
    68:24:b2:c0:4d:ba:b9:49:91:8f:c2:d6:cc:f2:bd:
    73:c1:e5:52:97:e4:4d:25:ff:9c:60:14:ad:ab:f3:
    f1:9a:cc:fd:88:a2:14:6f:1e:df:14:a5:a8:a9:fc:
    1e:7c:2d:fd:58:f8:04:28:70:0a:97:80:2c:53:ae:
    b3:de:3e:f6:a6:37:2f:ed:dd:18:d5:46:c7:11:15:
    42:19
exponent2:
    00:bd:02:bc:92:1d:f7:66:03:db:05:f9:d8:8b:fb:
    90:6d:bb:5b:bd:b5:74:dd:60:90:e4:9d:94:fa:59:
    80:96:02:ae:d4:2c:79:d4:08:f3:a5:10:3f:f0:08:
    5f:fd:fe:f5:b1:86:8f:c9:24:bf:be:a4:b1:16:e6:
    6d:16:d2:0c:fe:70:fc:5e:74:14:04:b8:e0:a8:da:
    f0:4b:04:11:3c:b8:02:22:6f:10:c0:0b:ae:c3:c5:
    fc:71:c7:26:db:ef:0a:f3:24:6b:9e:e6:bd:75:9b:
    3e:58:91:6f:61:5d:bf:99:cc:fd:23:ec:4c:4e:15:
    2a:9f:de:7b:d9:5e:a1:4c:d5:e1:e4:42:b7:d0:37:
    ff:f8:1e:e0:a3:74:16:a0:95:7e:4d:81:4a:e4:59:
    ca:e7:e4:72:94:36:45:08:a8:66:d4:f2:c5:57:a9:
    9a:e7:02:e3:34:f2:82:94:f5:5b:39:34:13:c2:c9:
    8f:a1:8a:8e:dc:fd:f6:bb:7c:72:55:b4:2a:e9:10:
    f7:80:f7:be:c1:39:49:f2:fd:1b:b2:2a:2e:d1:ac:
    d4:3a:80:34:a3:e0:46:52:2d:03:f1:eb:69:51:1b:
    51:e8:f2:e4:52:9f:7c:82:fa:a1:97:01:93:30:3d:
    e7:d4:91:87:93:e1:e8:60:8f:9a:df:d3:0d:84:7c:
    95:71
coefficient:
    28:05:4a:58:44:79:0a:e2:82:9e:ee:77:16:d9:19:
    cc:c7:65:f8:7c:95:e6:e6:e4:8d:36:5d:08:79:57:
    9b:38:18:cf:65:25:bb:a8:c6:47:8c:3b:7c:11:45:
    d3:65:d7:12:23:2a:ef:05:f9:eb:ef:87:b0:45:20:
    64:91:3f:7b:fe:f5:e3:33:e9:6d:a3:36:4d:33:d8:
    2e:ed:21:a8:c3:5a:bf:53:9f:c2:b7:9e:ab:2e:d7:
    ab:43:fa:b2:ab:a1:97:35:72:e5:83:ca:02:21:8b:
    c1:cb:a5:9a:46:35:62:8f:aa:12:44:5d:c1:26:ae:
    0c:a6:b3:b9:66:6a:b1:ed:20:fd:d7:f4:36:f5:f2:
    19:87:25:f8:fa:e1:32:15:3c:38:97:16:45:cd:61:
    dc:fb:ef:4e:94:1e:9c:34:0d:9f:19:f2:d5:36:c4:
    32:fa:de:01:c1:df:68:1e:4e:53:c3:17:e5:1e:a2:
    fe:4b:14:71:41:58:c1:f3:0e:e0:9b:c8:d5:7d:58:
    62:d7:7e:0e:5e:9f:e2:cc:95:5f:23:74:f3:bd:24:
    3b:7d:e0:5f:60:55:f7:34:6f:ad:f9:63:4c:b6:e8:
    99:36:a6:6d:52:fc:a3:1f:5d:2a:be:19:36:a4:8f:
    e1:77:b5:a6:5c:c2:dc:ed:95:bb:9d:dc:36:b2:06:
    97
writing RSA key
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKQIBAAKCAgEAwaUasrY4/VODxppxw5+iKe2jyIeS64Sy2akiZP2psgH0dZYy
iVq9sAW4zwe6OqnSXgPFwtZFgnVky8/md/Ykq9wES3KFgW/ICw44bZ6rW0cs1Ugr
UsF1/W/iuaWDVyK4dWdPAdjx0uKGoP8UMpt3VshwUOzXxzw9YZbjzEVsRrpojxBm
DiKjaWcgPplCkgM7QOeTuGGBM2NM10uwtpErePpW1UxC0LtnYYw+cYCQ5WhoyfAM
jmyPQeSmRSWl8apo80gGzTKnZdP07MZLLHWP2qU4bYYnnqwnsz4EmoVAkH6qxCiR
g84EHP36mNRTuO0cd/w0RdPlieGkrR0WiSgznmm9R2tlNBTAQE/4Hi+oFqh8k7dA
6aHpHNHnlhmlpKx6l93Nz8qK1FwR7HkMCWKfhzHiBg07YnXFpHr55FoBlfvjMhhZ
cQ49GAz78NeDjZy/Dvxq1JatHXfkJTKKMuBMMfZSXTz74uJwcaorELZ1ZevcZ+8S
flELCwFrF87JgRhhmgKd9EQcCeAPCrOaeGlNAr2P+Phq4tfosDrRMYqwW6v/41du
eEvR89vVFrqqhozpmn4EtIlNPeJ7RW5x7XGbHDqzuVlBOTajHMiI3JlJ2QliuocH
p24u/0zho5SCX2oATuDPkp0oi2bn+MrptSB15wSHN274YB1jiZneufondCkCAwEA
AQKCAgACrU+jLNW42tC1jCkKdUh+n+Rlv0oOq3T1gVsSXldcOJ6yiXMFZxW8OzgE
1KyEZxibaB3xxZiMZycPkj4zZlm3boE4scqasXrofDfXfBwOVPuPr0G6ESaabFOM
EXexWq+GH/l9owwkyDDoRN54nKGXt4ml9MA+5txKXxWjG0qV57nOUIG4rE3qBRzz
AJdlAVpuWUU3hVGN7k9/onI88+DP+VX9+OHrlMunE5NBam+WXE0mjYT+6w1H8etC
hXS31I1C37oIWCzsQXPfWhZr9OwaL7KKARLHJMYfujnCERmFZdrif1UTp2NzKyet
uTG3GsAMAJaQaI+BynbGVeKb3sxn3BIR4cQlSGt/KF+U3h/oiTEBZAQlNlhftjtP
wZGe809DX+d2FazZf6VTpnk+ow2uGX6yEAD6MI7GVpRAAgbLn+EkP5UzN8FJ1EJp
7zZttKJer9HHZ35SR/Cknu0oqE8rTLuXhcQ3aRbOXPb87p5IFEnWGxKPUODJv1PK
Bd1cgfCU1gNGHJspZZ96VC/ocnZ7JRIC7Okk9EC1qRbgURn9TjojZOi+HkBnGu8E
psSthmwKs7pUzlRZ6emtsPRdlO48e+M6aYuNCy38J4j3dEDuMoo/oIQLjuG5HKUK
P5Z/Mo+dOrytwA03YJkhXplaOd7JDq3K7wEga/VEzXrWUO/8SQKCAQEA41f0t/9Z
Ov8vMzQ1XjYvhNmzxzrJwJxuHfl/9Mmgr4aDw2ERsr6uNkLgMiEQPOLAf64kXm0g
xMyqL9x+ZbhJZwfuADO44HSwjYt0QwMIV1Q9iMtVVo73gBbdqn57EuMG82sP/mC2
R6713GURox6LNIrSZcgbpBjfKhiyi/skEhwEg8nmHycsUZqGpcju6+4UaAlEx902
h9zO5aag9ehgIReG1UlVPuT8+yJqpGICaDwmXfpAffFnbdqpxWGrUUe+PLRud2gs
azg7cdURYsZeZvUXG2t5gkxKq4WwRpB3yCOd3IV+l5s2YMkuNHYfR/zUX7+qXe5H
hSYIN+HAGXs3DwKCAQEA2g2+HsNeXTUJPMSwY5eUUhsUxTSut5j1LAL/2wEqt/LB
RAHwEVEvnWGdASexSvIjC0RlKJP+kr+ltTEC+tc+Q0M2U6QUlsCcLo7yy8gIFDr5
hZNIo6gaBsyOSxMuoNCyGmL9vmW4Yr9gviIj63AWdTksKrorc9beYwmtsb5vTky2
GsVTsC6ByPsHQb4kyxhm1Oq7RpLMITyBUZ+2c1o7576mPkq1s31Ah/BjPylaA3Uw
YCw1sb4ZoWMfJ6J5JFU6WsIstlgJMotHwuOMtG1P1bpympuX5wCoqKmvT/6uQY/k
6J/WyD7xDMIe3gSWoV7QrQQg5zQTxGg9W0758PnhRwKCAQEAuh2Dhi5RSm8moPCY
0Cvj8wqWlv+Vs01dCMT879Uw6wFgVU7eQkrALEPLbr6KoI2xsdVKiNMmBHbYzJ3i
DDw2O1bOjPPK4lYlQ3trDoEpDvUz+w0bK+WW0RHnHnC1KN0bD6QST9m04DJnrKpB
Kh0TMUyEujZ8CnciG0Bkyxwqh3jQaWOcNNzI93VdzdMVZahepF0SJdz/i3JFHtSu
6SH3sJ+mDm4ej4K/aIjgbPqfpd24Oy9oJLLATbq5SZGPwtbM8r1zweVSl+RNJf+c
YBStq/Pxmsz9iKIUbx7fFKWoqfwefC39WPgEKHAKl4AsU66z3j72pjcv7d0Y1UbH
ERVCGQKCAQEAvQK8kh33ZgPbBfnYi/uQbbtbvbV03WCQ5J2U+lmAlgKu1Cx51AjZ
pRA/8Ahf/f71sYaPySS/vqSxFuZtFtIM/nD8XnQUBLjgqNrwSwQRPLgCIm8QwAuu
w8X8cccm2+8K8yRrnua9dZs+WJFvYV2/mcz9I+xMThUqn9572V6hTNXh5EK30Df/
+B7go3QWoJV+TYFK5FnK5+RylDZFCKhm1PLFV6ma5wLjNPKClPVbOTQTwsmPoYqO
3P32u3xyVbQq6RD3gPe+wTlJ8v0bsiou0azUOoA0o+BGUi0D8etpURtR6PLkUp98
gvqhlwGTMD3n1JGHk+HoYI+a39MNhHyVcQKCAQAoBUpYRHkK4oKe7ncW2RnMx2X4
fJXm5uSNNl0IeVebOBjPZSW7qMZHjDt8EUXTZdcSIyrvBfnr74ewRSBkkT97/vXj
M+ltozZNM9gu7SGow1q/U5/Ct56rLterQ/qyq6GXNXLlg8oCIYvBy6WaRjVij6oS
RF3BJq4MprO5Zmqx7SD91/Q29fIZhyX4+uEyFTw4lxZFzWHc++9OlB6cNA2fGfLV
NsQy+t4Bwd9oHk5TwxflHqL+SxRxQVjB8w7gm8jVfVhi134OXp/izJVfI3TzvSQ7
feBfYFX3NG+t+WNMtuiZNqZtUvyjH10qvhk2pI/hd7WmXMLc7ZW7ndw2sgaX
-----END RSA PRIVATE KEY-----
```

7. Valor de los certificados generados

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ cat certs/ca.cert.pem
-----BEGIN CERTIFICATE-----
MIIGTDCCBDSgAwIBAgIJALnYFu3932FAMA0GCSqGSIb3DQEBCwUAMIGyMQswCQYD
VQQGEwJFUzEQMA4GA1UECAwHR3JhbmFkYTEQMA4GA1UEBwwHR3JhbmFkYTENMAsG
A1UECgwEU1BTSTEnMCUGA1UECwwedXRvcmlkYWQgQ2VydGlmaWNhZG9yYSBkZSBT
UFNJMR8wHQYDVQQDDBZTUFNJIEF1dG9yaWRhZCBSYcODwq16MSYwJAYJKoIhvcN
AQkBFhdwbGZ1ZXJ0ZXNAY29ycmVvLnVnci5lczAeFw0xODExMjQxMzM1MDZaFw0z
ODExMTkxMzM1MDZaMIGyMQswCQYDVQQGEwJFUzEQMA4GA1UECAwHR3JhbmFkYTEQ
MA4GA1UEBwwHR3JhbmFkYTENMAsGA1UECgwEU1BTSTEnMCUGA1UECwwedXRvcmlk
YWQgQ2VydGlmaWNhZG9yYSBkZSBTUFNJMR8wHQYDVQQDDBZTUFNJIEF1dG9yaWRh
ZCBSYcODwq16MSYwJAYJKoIhvcNAQkBFhdwbGZ1ZXJ0ZXNAY29ycmVvLnVnci5l
czCCAiIwDQYJKoIhvcNAQEBBQADggIPADCCAgoCggIBAMGlGrK2OP1Tg8aaccOf
ointo8iHkuuEstmpImT9qbIB9HWWMolavbAFuM8Hujqp0l4DxcLWRYJ1ZMvP5nf2
JKvcBEtyhYFvyAsOOG2eq1tHLNVIK1LBdf1v4rmlg1ciuHVnTwHY8dLihqD/FDKb
d1bIcFDs18c8PWGW48xFbEa6aI8QZg4io2lnID6ZQpIDO0Dnk7hhgTNjTNdLsLaR
K3j6VtVMQtC7Z2GMPnGAkOVoaMnwDI5sj0HkpkUlpfGqaPNIBs0yp2XT9OzGSyx1
j9qlOG2GJ56sJ7M+BJqFQJB+qsQokYPOBBz9+pjUU7jtHHf8NEXT5YnhpK0dFoko
M55pvUdrZTQUwEBP+B4vqBaofJO3QOmh6RzR55YZpaSsepfdzc/KitRcEex5DAli
n4cx4gYNO2J1xaR6+eRaAZX74zIYWXEOPRgM+/DXg42cvw78atSWrR135CUyijLg
TDH2Ul08++LicHGqKxC2dWXr3GfvEn5RCwsBaxfOyYEYYZoCnfREHAngDwqzmnhp
TQK9j/j4auLX6LA60TGKsFur/+NXbnhL0fPb1Ra6qoaM6Zp+BLSJTT3ie0Vuce1x
mxw6s7lZQTk2oxzIiNyZSdkJYrqHB6duLv9M4aOUgl9qAE7gzSKdKItm5/jK6bUg
decEhzdu+GAdY4mZ3rn6J3QpAgMBAAGjYzBhMB0GA1UdDgQWBBTVaqahIjchnLaQ
Xa31kg2U0G2xUzAfBgNVHSMEGDAWgBTVaqahIjchnLaQXa31kg2U0G2xUzAPBgNV
HRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjANBgkqhkiG9w0BAQsFAAOCAgEA
l97kOXCNNpl3CVnOw81/gJwpgx/93fubPfKFxHAQcD4kbviwhvgpHxw4urVIGQ3o
XhRMDJfXQagJRBuEG/sYeXra8QNZJ4SIVXfcS70jXnrM3K9xtQG2/VYzgRx9nv0G
596oFpEw7/lggikcWBBn1Hz1VAOKPSS247hvIvlqWlNqVdJd5U8q0Faqx1rP/GjP
ft8298IPJzJKfP7OMuuZG/oDhufObbRQ+QnmdVTo7mQ3SCnGgjjg/SHTs8sISX6b
UZl4PvMZRVvaPeL/uNKfvsyPlREKDZHnGLuSjfXbuosgJ+1PvuE6a+CAeu6ZvE1+
KeKM1F+7sCg0N16SitkE73+U/T0ur0GS3pHpzCGgzYYMQRThFyyBWcwPNxbAcbjt
BOf3/0VMBKpk2FZD9R4wIoeCexTMRsqkJavX2PCX0eaEIcVo6H+jOdrORfbO39lV
JMNUJK1M0hvykRzLBYaq5XhYmNK9qKHJvji8egXggaMhBKHsuY7qan/TnPGiWJNq
WXZMzRHzLJp31IJtXt8LjrLpr7+acKfoyoj1vm5bybUD993UvpMgJBdUe78vomL6
C2otPOHcFQwohxOOF+rYVc1O7rDrXqyVvdSIvCgdBjzmm1SMeex0jfdtUuiG5Aa3
Xe3lZ3ekMdt8O90Zf35H5eBU3fGElqkQQGGsqCZKb9U=
-----END CERTIFICATE-----
```

Cread una autoridad certificadora subordinada a la anterior.

1. Creamos la estructura de directorios

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ mkdir -p ca/subordinada/{certs,crl,csr,newcerts,privat
e}
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ ls
ca  certificados.pdf
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ cd ca
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ ls
certs  crl  csr  index.txt  newcerts  openssl.cnf  private  serial  subordinada
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ cd subordinada/
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca/subordinada$ chmod 700 private
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca/subordinada$ touch index.txt
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca/subordinada$ echo 1000 > serial
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca/subordinada$ echo 1000 > crlnumber
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca/subordinada$ ls -lsR
.:
total 28
4 drwxr-xr-x 2 pedro pedro 4096 Nov 24 08:00 certs
4 drwxr-xr-x 2 pedro pedro 4096 Nov 24 08:00 crl
4 -rw-r--r-- 1 pedro pedro    5 Nov 24 08:03 crlnumber
4 drwxr-xr-x 2 pedro pedro 4096 Nov 24 08:00 csr
0 -rw-r--r-- 1 pedro pedro    0 Nov 24 08:02 index.txt
4 drwxr-xr-x 2 pedro pedro 4096 Nov 24 08:00 newcerts
4 drwx------ 2 pedro pedro 4096 Nov 24 08:00 private
4 -rw-r--r-- 1 pedro pedro    5 Nov 24 08:02 serial

./certs:
total 0

./crl:
total 0

./csr:
total 0

./newcerts:
total 0

./private:
total 0
```

El sistema de archivos es similar salvo por que ha creado el fichero crlnumber donde se almacena el número de serie de las listas de revocación de certificados.

2. Modificamos el archivo de configuración de la CA subordinada

Debemos modificar los siguientes parámetros

/ca/openssl.cnf	/ca/subordinada/openssl.cnf
Dir = /home/pedro/Documents/git/inform-4-SPSI/p4/ca	dir = /home/pedro/Documents/git/inform-4-SPSI/p4/**ca/subordinada**
private_key = $dir/private/ca.key.pem	private_key = $dir/private/**subordinada**.key.pem
certificate = $dir/certs/ca.cert.pem	certificate = $dir/certs/**subordinada**.cert.pem
crl = $dir/crl/ca.crl.pem	crl = $dir/crl/**subordinada**.crl.pem
Policy = policy_strict	policy = policy_**loose**
	copy_extensions = copy

3. Creamos la clave privada de la CA subordinada

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ openssl genrsa -aes256 \
>        -out subordinada/private/subordinada.key.pem 4096
Generating RSA private key, 4096 bit long modulus
.....................................................................................++
..............++
e is 65537 (0x10001)
Enter pass phrase for subordinada/private/subordinada.key.pem:
Verifying - Enter pass phrase for subordinada/private/subordinada.key.pem:
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ chmod 400 subordinada/private/subordinada.key.pem
```

Cambiamos los permisos con chmod para que sólo se pueda leer y siendo superusuario.

4. Creamos el certificado de la CA subordinada

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ openssl req -config subordinada/openssl.cnf -new \
> -key subordinada/private/subordinada.key.pem -out subordinada/csr/subordinada.csr.pem
Enter pass phrase for subordinada/private/subordinada.key.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.
-----
Nombre del país (Código de 2 letras) [ES]:
Provincia o Estado [Granada]:
Nombre de la localidad [Granada]:
Nombre de la organización [SPSI]:
Nombre de la unidad organizativa [utoridad Certificadora de SPSI]:
Nombre Común []:SPSI Autoridad Certificadora Intermedia
Correo electrónico [plfuertes@correo.ugr.es]:
```

En este caso, como puede verse, cambia dónde se encuentra la clave privada de la CA .

Además, en este caso, la CA primaria tendrá que autorizar a la intermedia, por lo que se crea una CSR y se guarda en ../ca/subordinada/csr/subordinada.csr.pem

5. Firmamos la autoridad de la CA subordinada con la autoridad raíz

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ openssl ca -config openssl.cnf -extensions v3_ca -d
ays 3650 -notext -in subordinada/csr/subordinada.csr.pem -out subordinada/certs/subordinada.cert.pem
Using configuration from openssl.cnf
Enter pass phrase for /home/pedro/Documents/git/inform-4-SPSI/p4/ca/private/ca.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Nov 24 17:37:38 2018 GMT
            Not After : Nov 21 17:37:38 2028 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = Granada
            organizationName          = SPSI
            organizationalUnitName    = utoridad Certificadora de SPSI
            commonName                = SPSI Autoridad Certificadora Intermedia
            emailAddress              = plfuertes@correo.ugr.es
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                CA:B8:92:72:6B:11:32:E5:D7:35:7A:D2:E7:49:08:2C:4E:00:26:45
            X509v3 Authority Key Identifier:
                keyid:D5:6A:A6:A1:22:37:21:9C:B6:90:5D:AD:F5:92:0D:94:D0:6D:B1:53

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Nov 21 17:37:38 2028 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

- - config: usamos el archivos de configuración de la CA raíz.
- -extensions: La extensión será v3_ca como se ha especificado en el archivo openssl.cnf
- -days: el número de días en los que expirará el certificado. 10 años en este caso, como se puede ver en el recuadro azul
- -in: indica la CSR que se quiere firmar.
- -out: indica dónde se guardará el certificado

También se puede ver como se ha cogido el nombre común introducido en el punto 1 de esta sección.

Finalmente, si hacemos un cat del index o del serial podemos ver como en index se ha almacenado el certificado el certificado firmado y como el serial se ha incrementado en uno.

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ cat index.txt
V       281121173738Z           1000    unknown /C=ES/ST=Granada/O=SPSI/OU=utoridad Certificadora de
SPSI/CN=SPSI Autoridad Certificadora Intermedia/emailAddress=plfuertes@correo.ugr.es
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ cat serial
1001
```

6. Archivos creados

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ ls -laR subordinada/
subordinada/:
total 44
drwxr-xr-x 7 pedro pedro 4096 Nov 24 08:55 .
drwxr-xr-x 8 pedro pedro 4096 Nov 24 09:37 ..
drwxr-xr-x 2 pedro pedro 4096 Nov 24 09:36 certs
drwxr-xr-x 2 pedro pedro 4096 Nov 24 08:00 crl
-rw-r--r-- 1 pedro pedro    5 Nov 24 08:03 crlnumber
drwxr-xr-x 2 pedro pedro 4096 Nov 24 09:22 csr
-rw-r--r-- 1 pedro pedro    0 Nov 24 08:02 index.txt
drwxr-xr-x 2 pedro pedro 4096 Nov 24 08:00 newcerts
-rw-r--r-- 1 pedro pedro 6167 Nov 24 08:59 openssl.cnf
drwx------ 2 pedro pedro 4096 Nov 24 09:13 private
-rw-r--r-- 1 pedro pedro    5 Nov 24 08:02 serial

subordinada/certs:
total 12
drwxr-xr-x 2 pedro pedro 4096 Nov 24 09:36 .
drwxr-xr-x 7 pedro pedro 4096 Nov 24 08:55 ..
-rw-r--r-- 1 pedro pedro 2232 Nov 24 09:37 subordinada.cert.pem

subordinada/crl:
total 8
drwxr-xr-x 2 pedro pedro 4096 Nov 24 08:00 .
drwxr-xr-x 7 pedro pedro 4096 Nov 24 08:55 ..

subordinada/csr:
total 12
drwxr-xr-x 2 pedro pedro 4096 Nov 24 09:22 .
drwxr-xr-x 7 pedro pedro 4096 Nov 24 08:55 ..
-rw-r--r-- 1 pedro pedro 1821 Nov 24 09:22 subordinada.csr.pem

subordinada/newcerts:
total 8
drwxr-xr-x 2 pedro pedro 4096 Nov 24 08:00 .
drwxr-xr-x 7 pedro pedro 4096 Nov 24 08:55 ..

subordinada/private:
total 12
drwx------ 2 pedro pedro 4096 Nov 24 09:13 .
drwxr-xr-x 7 pedro pedro 4096 Nov 24 08:55 ..
-r-------- 1 pedro pedro 3326 Nov 24 09:14 subordinada.key.pem
```

Se puede ver como a parte de la estructura de archivos creado en el punto 1 de esta sección, se ha creado una clave privada de la CA subordinada, así como una CSR en la carpeta csr de la CA subordinada y finalmente el certificado firmado por la CA raíz en la carpeta certs de la CA subordinada.

7. Valor de las claves generadas

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4/ca$ openssl rsa -text -in subordinada/private/subordina
da.key.pem
Enter pass phrase for subordinada/private/subordinada.key.pem:
Private-Key: (4096 bit)
modulus:
    00:b7:09:c1:94:09:e4:7a:2c:e5:4d:75:42:d7:89:
    34:5c:4e:95:9d:98:c6:ba:88:ff:6f:86:36:03:41:
    4c:c1:e8:19:57:f8:b5:d9:31:2b:8c:e9:dd:6a:d4:
    2c:f4:06:e5:3a:90:89:81:ae:85:0e:a4:1c:6b:71:
    a9:f9:0c:fe:a8:cd:bc:b5:a6:56:22:49:7f:07:f4:
    cb:6d:37:7b:ec:1d:1b:96:30:7e:7f:6c:c1:e7:c7:
    3c:05:cf:04:5e:10:7a:89:7b:d3:6b:46:a8:89:f2:
    05:d7:66:9f:40:29:a2:8b:72:e2:67:bd:53:df:73:
    eb:34:56:66:23:3b:7e:13:45:13:f0:69:ca:7d:81:
    44:92:75:92:2c:af:e4:90:59:da:ae:96:02:6d:37:
    e9:a8:cb:92:34:ca:de:75:3f:01:7e:b9:7d:30:5d:
    c4:06:70:a2:7b:98:c7:d7:f1:7d:bc:68:d2:bd:cd:
    4f:0a:f6:73:19:42:5b:43:c0:68:01:ed:d9:a3:cb:
    5d:68:06:d3:9a:46:fc:b9:f4:1b:0c:85:21:b6:1e:
    88:86:85:1c:0d:bc:a9:68:24:c2:b8:25:8a:0d:4a:
    d6:b5:fc:50:89:8a:10:05:19:21:bb:8f:eb:05:c4:
    d3:51:14:02:ec:e1:48:9a:f2:88:e3:2f:97:07:eb:
    f5:a6:e4:1e:5e:72:6e:f5:7f:57:00:9c:62:aa:60:
    b2:ac:8d:56:21:43:06:b7:7d:ea:90:52:bd:e7:91:
    37:cc:36:8e:b2:7e:c3:ba:68:bc:4d:79:a1:16:5d:
    71:84:11:b5:d6:7e:e5:8c:7d:66:33:fa:60:a4:c7:
    81:70:d3:0d:43:06:bd:34:26:04:c1:22:ea:21:e1:
    fd:ab:63:f7:72:b5:ee:6a:98:36:f0:a1:a9:81:9b:
    b8:b5:8c:6d:9e:71:9a:78:61:a3:e5:23:7f:50:46:
    2a:a0:d1:07:4e:c9:a1:12:8e:74:e2:cb:79:6d:53:
    cf:31:dc:9c:b8:5f:43:5b:4f:60:20:b6:4e:10:54:
    3f:a5:8b:9a:77:af:ef:d5:76:a0:e1:a9:5b:08:1f:
    89:90:53:98:f9:05:f8:bf:1c:4d:51:dc:d8:b2:99:
    94:8f:e5:47:0d:7a:85:b0:14:38:22:28:fa:cb:77:
    05:16:bd:3c:ed:be:9e:c8:3c:a9:09:30:e8:37:03:
    40:45:be:da:84:44:21:28:e2:2e:e3:39:12:f1:09:
    ff:ad:47:84:d0:c7:77:bf:5a:eb:75:e7:18:1b:73:
    73:d4:81:25:1c:23:19:e7:3f:80:1a:ae:c9:8c:89:
    65:4b:5a:d0:bb:32:1d:f5:3e:8d:97:97:8f:e5:11:
    a3:ea:87
publicExponent: 65537 (0x10001)
```

```
privateExponent:
    7d:b8:2f:c3:d4:bf:9f:c3:32:84:6f:64:47:d2:af:
    aa:2f:37:c8:95:64:fa:3e:9a:e4:29:14:f4:4b:67:
    c3:4f:fe:08:54:85:e2:f6:48:e9:72:c0:68:5d:ef:
    ba:74:fa:01:ad:c1:24:d7:90:00:ac:6b:f0:c8:93:
    6c:c2:a6:2f:9f:90:5c:5c:31:91:3f:56:07:4a:f6:
    66:bf:d3:58:2b:ee:04:cc:ae:36:2b:a7:4b:e1:a6:
    b2:7e:ac:8b:47:5a:43:10:4f:f8:c1:01:86:2e:3c:
    20:e5:15:c0:e6:58:04:dc:15:f2:17:32:82:aa:86:
    04:de:cb:2c:ab:f2:3e:9e:15:c1:ed:87:ed:88:5a:
    67:16:66:1e:57:79:f0:44:27:55:ff:27:0f:89:75:
    ee:40:54:dd:f9:f1:ae:2a:66:86:7a:35:28:81:5e:
    e0:e5:80:54:d0:6d:83:3f:15:93:d1:93:de:56:24:
    52:6d:50:45:2b:34:b0:66:79:89:c9:aa:d1:3c:1f:
    9e:12:02:49:57:34:c3:2c:8d:5f:9e:19:b7:93:65:
    46:b0:2a:c2:ac:b0:d7:1d:58:b9:4e:df:71:9d:d3:
    b8:0f:e3:e9:74:70:e8:6f:88:a1:e1:8a:15:de:49:
    1e:c9:55:f1:0a:13:ea:89:67:c8:53:a9:b3:01:39:
    2a:0c:a2:e9:99:98:37:8b:84:9f:c5:56:12:47:fa:
    51:89:76:59:ca:96:7b:28:a0:03:d9:9d:72:40:ad:
    2d:b9:ad:03:78:ce:d5:ea:1d:5a:28:c4:ea:b9:fc:
    0e:c4:15:b2:a2:20:bf:b3:aa:b7:d0:cd:dc:e7:c9:
    42:9b:25:e7:3a:ff:17:ff:94:5f:3b:bd:23:a0:dc:
    97:12:f8:aa:cb:39:87:9a:b6:54:ea:bc:72:32:76:
    a3:7c:19:fc:86:14:40:dd:75:65:7d:87:4c:2d:e6:
    8b:e8:fc:74:7f:56:84:d2:65:cd:a4:39:5d:11:9e:
    ad:a1:f6:dc:e8:7c:eb:4c:42:48:db:3a:ad:d0:1d:
    98:75:9a:46:54:49:b1:14:42:c9:a7:a2:76:79:d6:
    e5:9f:65:66:49:48:2e:c5:88:e9:d4:7f:4e:e7:e7:
    61:b2:46:b2:f4:70:f4:72:68:42:77:d1:ca:01:1f:
    30:03:37:a6:62:a3:f7:6c:04:a6:f9:11:88:ea:eb:
    ba:85:ce:f7:3d:00:b1:69:13:b5:9a:e6:71:c7:ac:
    45:c4:db:ba:df:f6:9f:a1:de:81:b1:67:7f:8e:68:
    24:8f:46:b6:b7:31:5b:02:eb:d0:78:40:f3:27:89:
    39:73:88:cb:88:e8:34:17:b9:9b:54:e7:bf:e0:22:
    0c:f1
```

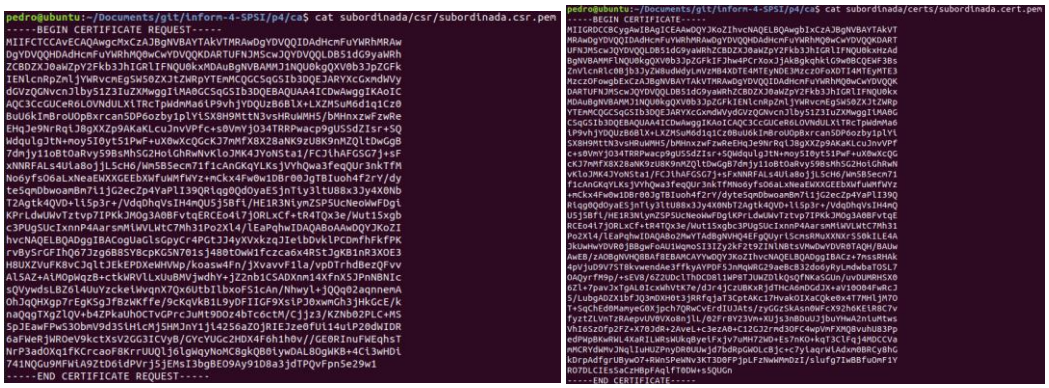
```
prime1:
    00:e2:2d:40:2a:2d:48:9c:18:6a:d7:45:52:ea:97:
    a7:a7:1f:68:11:c7:4c:48:9c:93:eb:13:d1:89:d9:
    d8:fe:da:a0:b9:d8:b4:68:50:0c:00:50:7a:a4:0b:
    06:55:39:fc:03:7f:5c:af:65:dc:45:12:a5:02:f9:
    a5:4f:c1:3e:81:ec:39:ba:97:96:34:a8:4f:5d:87:
    07:93:33:73:b0:f5:9f:5e:38:c1:fb:00:87:17:a1:
    01:f5:33:04:46:a8:be:73:f3:fc:08:59:40:4b:04:
    a6:e7:74:50:4b:1a:52:ac:d7:33:96:e1:58:f3:5d:
    1d:05:fc:0d:82:41:02:5b:df:a5:b9:1f:f4:31:5d:
    56:20:ec:11:6e:f6:e3:de:36:19:6b:df:bc:f6:b0:
    ac:d3:32:ac:d8:cf:fc:41:2a:62:1d:70:61:cd:dc:
    c2:e3:bb:91:fb:c4:cf:f5:fd:0d:7b:a3:22:45:35:
    74:57:cd:99:93:d4:0a:f5:ee:8d:5a:7b:25:69:d4:
    e6:47:63:ff:a7:c2:b4:2a:c5:e7:ad:2c:09:e1:07:
    87:05:42:df:70:38:09:3c:f6:e0:75:b2:8f:bd:6a:
    3e:ce:55:15:9e:be:78:36:3b:4d:f6:d9:24:9a:42:
    54:00:ed:b7:85:13:3e:47:4d:31:51:87:7e:92:86:
    37:9b
prime2:
    00:cf:2c:54:cb:cc:f8:1b:65:eb:d3:e4:01:9b:ba:
    65:d2:06:6e:c1:07:26:e0:7a:f2:14:48:aa:9c:19:
    8b:09:3c:44:f7:36:94:12:65:f9:c2:34:cd:18:3b:
    fb:3a:39:2f:58:a1:b2:9e:11:62:58:89:c8:a3:85:
    7e:c1:d7:4b:05:c9:77:2e:09:9d:a0:bd:53:d1:dd:
    28:02:67:7d:a6:41:b8:83:b8:98:c4:3f:82:e6:39:
    8a:49:62:fa:2a:7c:1f:66:52:22:cd:63:d0:98:d3:
    46:73:ca:b8:2e:0c:3f:81:a5:df:a5:ee:c1:5c:a8:
    d1:88:8a:67:30:b6:92:d1:0d:3a:f4:6c:b2:48:77:
    c6:9c:a7:cd:81:85:68:66:4a:a6:83:5d:40:eb:c8:
    51:c8:d6:18:c5:b8:1f:2b:c2:45:3d:64:b9:88:c4:
    7f:29:a5:ee:8f:d3:a0:64:50:98:89:c8:fb:c4:30:
    d5:08:33:c0:b5:b9:ed:89:8a:51:cf:b6:5d:4a:d1:
    db:a4:50:82:be:e0:f9:14:6c:18:63:5a:3e:c9:58:
    86:cc:03:8b:90:dc:bc:2d:3a:ef:98:7e:99:04:fc:
    dc:e4:a5:b3:b3:a3:b4:59:68:2d:51:cd:3d:7e:7b:
    e5:51:92:20:45:c0:fe:19:c9:13:e5:fe:74:71:29:
    05:85
```

```
exponent1:
    50:1f:f9:b8:37:5c:9e:b7:e3:b9:a9:7c:6b:51:18:
    7a:93:1c:ba:17:a1:85:a3:ba:9f:2f:e1:2e:75:b7:
    72:e9:9e:c0:d7:ed:69:7a:da:15:8e:6d:34:0a:17:
    cf:3f:80:70:f8:c0:ab:fe:68:df:2b:70:bb:b2:17:
    07:3f:0d:56:d7:89:c7:f9:85:a3:d7:f0:6d:d0:b5:
    35:47:a7:f7:8b:bc:4e:93:ca:dc:91:de:49:d7:a7:
    2a:e7:4c:df:7f:4e:21:23:d1:28:5f:fd:ef:d5:91:
    0f:33:dc:72:0e:bc:35:30:f3:bc:c2:ce:51:40:ae:
    54:7d:6b:87:b6:62:10:8c:15:58:94:e2:5c:4e:95:
    81:8a:3f:ce:d0:b5:fe:f5:a9:61:d6:dc:49:84:63:
    65:5a:71:73:49:93:32:be:c2:0d:6d:cf:a8:2f:49:
    f7:85:6e:7d:03:c7:2c:7c:de:36:eb:9e:eb:67:b9:
    74:95:88:8f:9f:31:d6:d8:10:c9:7a:10:d2:02:33:
    26:1d:5d:e7:5f:89:96:11:90:36:80:00:6b:f0:cf:
    bb:64:6a:65:85:e4:77:ed:79:ad:18:79:e5:7f:6b:
    0a:8b:87:e2:39:d5:ba:58:9e:11:11:f1:ee:98:0a:
    cc:5d:6a:83:41:42:f1:dd:7d:d8:45:28:e8:dd:95:
    7b
exponent2:
    62:31:f9:f3:2b:30:c2:13:ba:06:91:c0:ad:66:59:
    12:86:58:02:87:f8:46:58:1f:db:bb:61:9a:61:85:
    04:18:9b:fb:ac:d3:dc:30:97:84:14:70:cd:b6:c8:
    6a:1d:66:b2:94:d9:cb:90:23:d4:21:62:87:17:24:
    30:8e:72:11:c9:1f:03:24:2d:a1:5d:7b:98:32:41:
    df:79:dc:15:6c:7b:1f:7b:e4:74:c8:41:ac:0b:c3:
    de:ea:d9:f6:3f:24:c6:e3:d1:79:16:81:6d:9e:5e:
    7b:4d:af:a4:ab:cb:82:10:f4:03:7b:3a:0d:48:3b:
    20:83:b1:4b:66:8e:0a:26:42:36:4e:3a:e6:9c:56:
    f8:33:94:f5:7a:1d:34:b6:d7:5b:d6:5c:8a:25:45:
    96:72:dc:05:03:33:4b:13:66:ac:25:cc:c6:e5:93:
    fc:52:98:d3:75:14:45:d7:e9:a5:0d:2d:40:1d:81:
    2b:c5:13:e7:4e:bc:26:ff:f7:ad:03:1c:0e:f5:8f:
    2c:bf:b8:68:ee:cb:40:81:c7:c1:77:a9:e0:d7:63:
    f4:d9:0d:52:d9:3d:1c:17:1e:2f:62:79:f6:e2:3f:
    74:e4:91:5b:69:11:77:7b:28:57:e8:76:e8:37:a3:
    46:d9:83:10:6c:dc:43:ae:8a:0e:ee:5f:94:af:43:
    dd
```

```
coefficient:
    78:7a:62:10:20:b9:0d:a0:e1:fa:d8:2e:24:c0:c7:
    8c:dc:72:34:b5:76:cc:25:e5:c2:3a:e7:41:db:4b:
    95:e8:dd:87:f1:55:94:42:78:be:0e:c6:45:45:40:
    9c:41:cd:69:8c:f4:7c:a0:7d:84:9b:4b:f8:e5:05:
    a0:95:f2:93:fc:23:a3:e4:8a:66:b4:34:91:ea:27:
    8f:0d:1c:38:f6:e3:26:c2:ca:36:eb:e8:b2:1f:43:
    39:c3:95:d4:a7:74:5d:14:1c:71:6d:ee:8e:cd:75:
    82:d4:d7:36:a0:3a:d7:d6:61:77:df:83:43:a7:76:
    d5:b2:74:0d:77:68:77:42:40:aa:9d:bf:03:d1:0a:
    27:65:93:1f:0d:87:07:1e:0a:9a:b3:74:ba:93:97:
    2c:4b:d8:cf:b1:b4:fa:e2:1c:17:71:f5:02:9c:b3:
    c4:11:74:af:d6:1f:ab:a4:fa:71:46:10:42:31:bc:
    ca:dd:28:a6:31:8b:46:d5:18:e8:9f:f4:84:d5:d9:
    72:6c:5d:31:2b:48:14:fe:a9:73:90:4e:12:e2:20:
    ee:8e:7c:e8:c0:50:4d:96:8e:34:dd:5f:e0:4f:3c:
    4c:ec:31:24:1a:34:39:6d:83:ec:18:08:e6:f9:d7:
    81:46:a6:b6:1b:af:37:6e:2d:37:00:fd:c8:cb:15:
    b4
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIJJwIBAAKCAgEAtwnBlAnkeizlTXVC14k0XE6VnZjGuoj/b4Y2A0FMwegZV/i1
2TErjOndatQs9AblOpCJga6FDqQca3Gp+Qz+qM28taZWIkl/B/TLbTd77B0bljB+
f2zB58c8Bc8EXhB6iXvTa0aoifIF12afQCmii3LiZ71T33PrNFZmIzt+E0UT8GnK
fYFEknWSLK/kkFnarpYCbTfpqMuSNMredT8Bfrl9MF3EBnCie5jH1/F9vGjSvc1P
CvZzGUJbQ8BoAe3Zo8tdaAbTmkb8ufQbDIUhth6IhoUcDbypaCTCuCWKDUrWtfxQ
iYoQBRkhu4/rBcTTURQC7OFImvKI4y+XB+v1puQeXnJu9X9XAJxiqmCyrI1WIUMG
t33qkFK955E3zDaOsn7Dumi8TXmhFl1xhBG11n7ljH1mM/pgpMeBcNMNQwa9NCYE
wSLqIeH9q2P3crXuapg28KGpgZu4tYxtnnGaeGGj5SN/UEYqoNEHTsmhEo504st5
bVPPMdycuF9DW09gILZOEFQ/pYuad6/v1Xag4albCB+JkFOY+QX4vxxNUdzYspmU
j+VHDXqFsBQ4Iij6y3cFFr087b6eyDypCTDoNwNARb7ahEQhKOIu4zkS8Qn/rUeE
0Md3v1rrdecYG3Nz1IElHCMZ5z+AGq7JjIllS1rQuzId9T6Nl5eP5RGj6ocCAwEA
AQKCAgB9uC/D1L+fwzKEb2RH0q+qLzfIlWT6PprkKRT0S2fDT/4IVIXi9kjpcsBo
Xe+6dPoBrcEk15AArGvwyJNswqYvn5BcXDGRP1YHSvZmv9NYK+4EzK42K6dL4aay
fqyLR1pDEE/4wQGGLjwg5RXA5lgE3BXyFzKCqoYE3sssq/I+nhXB7YftiFpnFmYe
V3nwRCdV/ycPiXXuQFTd+fGuKmaGejUogV7g5YBU0G2DPxWT0ZPeViRSbVBFKzSw
ZnmJyarRPB+eEgJJVzTDLI1fnhm3k2VGsCrCrLDXHVi5Tt9xndO4D+PpdHDob4ih
4YoV3kkeyVXxChPqiWfIU6mzATkqDKLpmZg3i4SfxVYSR/pRiXZZypZ7KKAD2Z1y
QK0tua0DeM7V6h1aKMTqufwOxBWyoiC/s6q30M3c58lCmyXnOv8X/5RfO70joNyX
EviqyzmHmrZU6rxyMnajfBn8hhRA3XVlfYdMLeaL6Px0f1aE0mXNpDldEZ6tofbc
6HzrTEJI2zqt0B2YdZpGVEmxFELJp6J2edbln2VmSUguxYjp1H9O5+dhskay9HD0
cmhCd9HKAR8wAzemYqP3bASm+RGI6uu6hc73PQCxaRO1muZxx6xFxNu63/afod6B
sWd/jmgkj0a2tzFbAuvQeEDzJ4k5c4jLiOg0F7mbVOe/4CIM8QKCAQEA4i1AKi1I
nBhq10VS6penpx9oEcdMSJyT6xPRidnY/tqgudi0aFAMAFB6pAsGVTn8A39cr2Xc
RRKlAvmlT8E+gew5upeWNKhPXYcHkzNzsPWfXjjB+wCHF6EB9TMERqi+c/P8CFlA
SwSm53RQSxpSrNczluFY810dBfwNgkECW9+luR/0MV1WIOwRbvbj3jYZa9+89rCs
0zKs2M/8QSpiHXBhzdzC47uR+8TP9f0Ne6MiRTV0V82Zk9QK9e6NWnsladTmR2P/
p8K0KsXnrSwJ4QeHBULfcDgJPPbgdbKPvWo+zlUVnr54NjtN9tkkmkJUAO23hRM+
R00xUYd+koY3mwKCAQEAzyxUy8z4G2Xr0+QBm7pl0gZuwQcm4HryFEiqnBmLCTxE
9zaUEmX5wjTNGDv7OjkvWKGynhFiWInIo4V+wddLBcl3LgmdoL1T0d0oAmd9pkG4
g7iYxD+C5jmKSWL6KnwfZlIizWPQmNNGc8q4Lgw/gaXfpe7BXKjRiIpnMLaS0Q06
9GyySHfGnKfNgYVoZkqmg11A68hRyNYYxbgfK8JFPWS5iMR/KaXuj9OgZFCYicj7
xDDVCDPAtbntiYpRz7ZdStHbpFCCvuD5FGwYY1o+yViGzAOLkNy8LTrvmH6ZBPzc
5KWzs6O0WWgtUc09fnvlUZIgRcD+GckT5f50cSkFhQKCAQBQH/m4N1yet+O5qXXr
URh6kxy6F6GFo7qfL+Eudbdy6Z7A1+1petoVjm00ChfPP4Bw+MCr/mjfK3C7shcH
Pw1W14nH+YWj1/Bt0LU1R6f3i7xOk8rckd5J16cq50zff04hI9EoX/3v1ZEPM9xy
Drw1MPO8ws5RQK5UfWuHtmIQjBVYlOJcTpWBij/O0LX+9alh1txJhGNlWnFzSZMy
vsINbc+oL0n3hW59A8csfN42657rZ7l0lYiPnzHW2BDJehDSAjMmHV3nX4mWEZA2
gABr8M+7ZGplheR37XmtGHnlf2sKi4fiOdW6WJ4REfHumArMXWqDQULx3X3YRSjo
3ZV7AoIBAGIx+fMrMMITugaRwK1mWRKGWAKH+EZYH9u7YZphhQQYm/us09wwl4QU
cM22yGodZrKU2cuQI9QhYocXJDCOchHJHwMkLaFde5gyQd953BVsex975HTIQawL
w97q2fY/JMbj0XkWgW2eXntNr6Sry4IQ9AN7Og1IOyCDsUtmjgomQjZOOuacVvgz
lPV6HTS211vWXIolRZZy3AUDM0sTZqwlzMblk/xSmNN1FEXX6aUNLUAdgSvFE+dO
vCb/960DHA71jyy/uGjuy0CBx8F3qeDXY/TZDVLZPRwXHi9iefbiP3TkkVtpEXd7
KFfodug3o0bZgxBs3EOuig7uX5SvQ90CggEAeHpiECC5DaDh+tguJMDHjNxyNLV2
zCXlwjrnQdtLlejdh/FVlEJ4vg7GRUVAnEHNaYz0fKB9hJtL+OUFoJXyk/wjo+SK
ZrQ0keonjw0cOPbjJsLKNuvosh9DOcOV1Kd0XRQccW3ujs11gtTXNqA619Zhd9+D
Q6d21bJ0DXdod0JAqp2/A9EKJ2WTHW2HBx4KmrN0upOXLEvYz7G0+uIcF3H1Apyz
xBF0r9Yfq6T6cUYQQjG8yt0opjGLRtUY6J/0hNXZcmxdMStIFP6pc5BOEuIg7o58
6MBQTZaONN1f4E88TOwxJBo0OW2D7BgI5vnXgUamthuvN24tNwD9yMsVtA==
-----END RSA PRIVATE KEY-----
```

8. Valor de los certificados generados



Crear una solicitud de certificado que incluya la generación de claves en la misma

1. Creación de la solicitud

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ mkdir -p client/{csr,private}
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ openssl req -newkey rsa:2048 -keyout client/private/cl
ient.key.prm -out client/csr/client.csr.pem -config ca/openssl.cnf
Generating a 2048 bit RSA private key
.....................................+++
.................+++
writing new private key to 'client/private/client.key.prm'
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.
-----
Nombre del país (Código de 2 letras) [ES]:
Provincia o Estado [Granada]:
Nombre de la localidad [Granada]:
Nombre de la organización [SPSI]:
Nombre de la unidad organizativa [utoridad Certificadora de SPSI]:
Nombre Común []:Cliente
Correo electrónico [plfuertes@correo.ugr.es]:
```

- Openssl req: para indicar que voy a hacer una solicitud
- -newkey: crea una nueva clave privada para esta solicitud, en este caso rsa de 2048 bits.
- -keyout: indica dónde se va a guardar la clave privada que se acaba de generar.
- -out: indica dónde se va a guardar la solicitud
- - config: indica que configuración se va a coger, en este caso la de la CA raíz.

2. Archivos generados

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ ls -laR client/
client/:
total 16
drwxr-xr-x 4 pedro pedro 4096 Nov 24 10:27 .
drwxr-xr-x 4 pedro pedro 4096 Nov 24 10:27 ..
drwxr-xr-x 2 pedro pedro 4096 Nov 24 10:27 csr
drwxr-xr-x 2 pedro pedro 4096 Nov 24 10:27 private

client/csr:
total 12
drwxr-xr-x 2 pedro pedro 4096 Nov 24 10:27 .
drwxr-xr-x 4 pedro pedro 4096 Nov 24 10:27 ..
-rw-r--r-- 1 pedro pedro 1086 Nov 24 10:27 client.csr.pem

client/private:
total 12
drwxr-xr-x 2 pedro pedro 4096 Nov 24 10:27 .
drwxr-xr-x 4 pedro pedro 4096 Nov 24 10:27 ..
-rw-r--r-- 1 pedro pedro 1858 Nov 24 10:27 client.key.prm
```

Como se puede ver, se han generado dos archivos, el de la solicitud del certificado en csr y la clave privada en private.

3. Valor de la clave privada

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ openssl rsa -text -in client/private/client.key.prm
Enter pass phrase for client/private/client.key.prm:
Private-Key: (2048 bit)
modulus:
    00:ac:75:97:f2:49:49:ad:32:c9:83:70:03:c9:f2:
    e1:e3:86:21:78:9e:20:c0:d0:fe:be:5f:53:58:53:
    d0:92:ba:7e:43:63:ca:62:74:74:57:fb:bd:a4:be:
    99:c8:16:cf:7e:56:3c:48:52:dd:af:6e:eb:f4:f7:
    c6:b1:42:e0:6c:6a:02:78:86:6e:d5:51:5d:c2:d6:
    b6:24:e0:63:b8:fc:d5:ea:f2:07:f2:3c:5b:fb:46:
    df:97:f3:ec:06:a7:5d:43:16:8c:01:44:73:5b:db:
    e0:0b:89:b3:73:d6:8d:09:e2:29:3c:b1:a4:90:6c:
    58:a6:51:9a:59:15:32:19:e2:10:6a:1e:78:6e:cd:
    9f:2b:ca:b9:93:e4:f0:e0:1e:77:ef:11:2a:78:54:
    28:04:98:5c:7f:57:c0:8a:43:f8:14:73:46:55:2f:
    4e:3e:72:46:1c:ef:6b:e6:cc:c9:2f:9d:0a:f4:72:
    a1:0c:f1:fa:11:7f:6d:d5:e5:d2:34:0b:9f:bc:63:
    14:46:1a:46:bd:98:ad:dd:ed:b1:be:20:36:05:38:
    5f:6d:74:1b:4f:7c:55:8d:54:5f:62:a0:87:82:d0:
    a9:5c:f5:97:90:66:59:de:31:9f:7a:d5:66:62:63:
    88:35:9b:df:3d:e6:5f:bf:59:51:24:e1:08:ae:f9:
    85:9b
publicExponent: 65537 (0x10001)
privateExponent:
    2d:6c:b3:de:ff:6a:c6:91:ef:fe:0c:cd:12:ae:44:
    cd:57:11:0d:e2:28:a2:60:ea:18:5e:a7:67:46:7c:
    53:89:87:a4:5c:6e:7c:4c:4c:30:b8:80:15:1a:97:
    0a:da:e7:40:51:9a:83:3a:40:65:eb:03:7f:7c:9b:
    fb:28:b0:50:1e:04:14:96:e4:2e:8f:c5:f0:81:f9:
    6b:f1:26:93:1d:15:83:52:c8:c1:07:20:fb:28:89:
    d0:4e:51:46:d7:62:7b:3f:3f:15:3e:60:5c:3b:a7:
    e1:a2:1d:80:4f:6c:ca:c3:a5:34:f5:5d:71:24:f8:
    9c:a6:35:cf:6d:03:cb:49:0f:5d:d2:96:0c:f8:6a:
    cd:de:da:61:ec:ee:1d:72:0b:a7:85:50:88:72:f9:
    e2:02:15:2a:a7:ec:07:74:b7:e9:33:56:8a:0f:12:
    87:83:a9:2a:75:29:01:c8:c3:de:27:e3:73:23:a7:
    b9:de:3a:15:8d:f6:ae:d7:c3:a1:2a:57:e4:bb:38:
    4b:5e:1a:ba:bd:aa:73:f8:36:f8:88:22:a2:fa:dd:
    93:d6:26:a7:97:b3:d7:29:37:57:a7:28:43:ba:0e:
    a8:70:88:1e:e3:60:b3:85:5e:96:49:bb:12:9c:45:
    51:f9:f5:ff:75:d6:e7:55:e8:f9:fe:f9:f9:7d:d4:
    51
```

```
prime1:
    00:da:dc:a7:bb:82:15:2e:ed:47:a7:98:58:fe:bc:
    94:d7:22:c8:00:65:c0:85:93:42:ee:73:d4:e9:c2:
    7d:9c:c5:b6:14:aa:be:63:0a:9a:0f:67:b4:4a:15:
    74:b6:3b:f0:b4:83:13:68:6b:5f:b4:e0:a0:3c:21:
    de:6c:d6:e3:51:b0:f7:6d:f8:2c:5f:10:98:dc:e1:
    6a:3d:e8:35:93:15:3a:23:b1:81:3c:f9:35:43:99:
    39:c6:16:21:bf:f7:c8:3b:58:c2:d0:d9:33:43:ef:
    25:df:1f:90:04:40:cb:61:cf:14:fa:23:c0:89:b7:
    e1:ca:9a:57:86:3e:a8:70:55
prime2:
    00:c9:b9:36:bb:81:ef:85:7a:13:4e:3d:c2:57:b8:
    75:f2:66:89:2b:c4:47:ba:74:00:f0:73:8b:48:36:
    21:6c:83:0a:ab:d1:18:32:05:ed:61:98:65:68:02:
    9d:11:cf:a3:a7:29:df:ab:09:f2:8c:8e:af:f8:98:
    42:8f:cb:58:c1:24:24:10:45:d3:79:dc:27:56:0c:
    85:30:42:03:44:5c:f9:27:32:dc:9d:a6:b6:2f:d6:
    aa:3c:be:bd:7b:a8:8a:56:4f:6d:f0:d0:00:d1:32:
    6e:fe:70:eb:22:c5:72:e5:bc:a4:60:bc:5d:16:95:
    2c:3e:14:f6:a9:23:87:4e:2f
exponent1:
    00:a3:0d:4a:e5:16:27:a3:fb:60:ab:ca:83:5a:dc:
    b1:e2:89:66:09:6d:c4:fd:7e:d5:99:82:b0:37:ab:
    0f:1c:11:eb:f1:ff:b6:b1:60:bf:a0:04:79:bb:cb:
    ba:54:dd:d9:19:12:a2:0d:e4:18:bc:4f:b0:f0:bb:
    a6:d2:dd:51:23:96:3c:f0:2f:b9:16:e5:ed:8c:79:
    5f:46:59:ce:38:12:d3:6a:ae:1e:83:87:82:18:27:
    7a:74:4a:1e:c0:be:df:ec:de:d6:dc:f3:44:0f:33:
    86:ba:70:f0:41:4a:e8:7a:a8:e5:8e:e9:bd:d2:9c:
    2c:da:5d:1c:21:c6:62:84:b5
exponent2:
    00:96:2f:70:21:70:5e:fc:d8:63:71:38:27:ee:19:
    66:ae:ff:4a:17:2c:be:5e:82:29:84:db:f1:91:e4:
    c3:43:bf:d8:7d:0d:62:df:33:6c:85:e1:e9:75:e3:
    a4:3f:73:81:1b:5e:e0:a8:bd:f2:38:55:af:8b:fd:
    08:69:78:72:ee:f1:52:6c:4f:20:60:b4:d9:10:86:
    a7:ce:c3:07:1d:a9:be:d2:41:5a:e1:81:12:59:51:
    90:53:43:8b:5d:7a:a0:ec:1b:9c:f5:d2:57:19:69:
    5c:1b:d1:c4:2e:92:24:b6:08:99:b5:6f:e8:3a:7c:
    fb:80:89:29:0f:ca:64:dd:7f
coefficient:
    46:a4:90:9e:8b:0d:92:34:e0:f3:a5:01:bd:fd:ed:
    15:b5:6b:6e:c4:b0:63:1c:ea:4b:48:dd:fa:08:9c:
    c8:04:e6:81:92:37:18:b4:65:60:14:79:6a:cf:04:
    f9:c9:45:e2:4d:58:16:93:08:86:ed:63:17:1d:01:
    3a:14:62:64:3f:d2:23:1c:13:57:4b:3b:2a:e6:12:
    d8:e6:74:e7:ae:65:70:bc:de:21:f9:42:34:4d:d9:
    12:19:16:74:dd:9f:a5:dd:b1:32:65:2f:0e:f0:8a:
    86:e4:a5:eb:9a:fc:a2:82:fb:e5:1e:f5:64:08:3d:
    42:66:82:75:1b:f6:56:20
```

```
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEArHWX8klJrTLJg3ADyfLh44YheJ4gwND+vl9TWFPQkrp+Q2PK
YnR0V/u9pL6ZyBbPflY8SFLdr27r9PfGsULgbGoCeIZu1VFdwta2JOBjuPzV6vIH
8jxb+0bfl/PsBqddQxaMAURzW9vgC4mzc9aNCeIpPLGkkGxYplGaWRUyGeIQah54
bs2fK8q5k+Tw4B537xEqeFQoBJhcf1fAikP4FHNGVS9OPnJGHO9r5szJL50K9HKh
DPH6EX9t1eXSNAufvGMURhpGvZit3e2xviA2BThfbXQbT3xVjVRfYqCHgtCpXPWX
kGZZ3jGfetVmYmOINZvfPeZfv1lRJOEIrvmFmwIDAQABAoIBAC1ss97/asaR7/4M
zRKuRM1XEQ3iKKJg6hhep2dGfFOJh6RcbnxMTDC4gBUalwra50BRmoM6QGXrA398
m/sosFAeBBSW5C6PxfCB+WvxJpMdFYNSyMEHIPsoidBOUUbXYns/PxU+YFw7p+Gi
HYBPbMrDpTT1XXEk+JymNc9tA8tJD13Slgz4as3e2mHs7h1yC6eFUIhy+eICFSqn
7Ad0t+kzVooPEoeDqSp1KQHIw94n43Mjp7neOhWN9q7Xw6EqV+S7OEteGrq9qnP4
NviIIqL63ZPWJqeXs9cpN1enKEO6DqhwiB7jYLOFXpZJuxKcRVH59f911udV6Pn+
+fl91FECgYEA2tynu4IVLu1Hp5hY/ryU1yLIAGXAhZNC7nPU6cJ9nMW2FKq+Ywqa
D2e0ShV0tjvwtIMTaGtftOCgPCHebNbjUbD3bfgsXxCY3OFqPeg1kxU6I7GBPPk1
Q5k5xhYhv/fIO1jC0NkzQ+8l3x+QBEDLYc8U+iPAibfhyppXhj6ocFUCgYEAybk2
u4HvhXoTTj3CV7h18maJK8RHunQA8HOLSDYhbIMKq9EYMgXtYZhlaAKdEc+jpynf
qwnyjI6v+JhCj8tYwSQkEEXTedwnVgyFMEIDRFz5JzLcnaa2L9aqPL69e6iKVk9t
8NAA0TJu/nDrIsVy5bykYLxdFpUsPhT2qSOHTi8CgYEAow1K5RYno/tgq8qDWtyx
4olmCW3E/X7VmYKwN6sPHBHr8f+2sWC/oAR5u8u6VN3ZGRKiDeQYvE+w8Lum0t1R
I5Y88C+5FuXtjHlfRlnOOBLTaq4eg4eCGCd6dEoewL7f7N7W3PNEDzOGunDwQUro
eqjljum90pws2l0cIcZihLUCgYEAli9wIXBe/NhjcTgn7hlmrv9KFyy+XoIphNvx
keTDQ7/YfQ1i3zNsheHpdeOkP3OBG17gqL3yOFWvi/0IaXhy7vFSbE8gYLTZEIan
zsMHHam+0kFa4YESWVGQU0OLXXqg7Buc9dJXGWlcG9HELpIktgiZtW/oOnz7gIkp
O8pk3X8CgYBGpJCeiw2SNODzpQG9/e0VtWtuxLBjHOpLSN36CJzIBOaBkjcYtGVg
FHlqzwT5yUXiTVgWkwiG7WMXHQE6FGJkP9IjHBNXSzsq5hLY5nTnrmVwvN4h+UI0
TdkSGRZ03Z+l3bEyZS8O8IqG5KXrmvyigvvlHvVkCD1CZoJ1G/ZWIA==
-----END RSA PRIVATE KEY-----
```

4. Valor del certificado

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ cat client/csr/client.csr.pem
-----BEGIN CERTIFICATE REQUEST-----
MIIC6TCCAdECAQAwgaMxCzAJBgNVBAYTAkVTMRAwDgYDVQQIDAdHcmFuYWRhMRAw
DgYDVQQHDAdHcmFuYWRhMQ0wCwYDVQQKDARTUFNJMScwJQYDVQQLDB51dG9yaWRh
ZCBDZXJ0aWZpY2Fkb3JhIGRlIFNQU0kxEDAOBgNVBAMMB0NsaWVudGUxJjAkBgkq
hkiG9w0BCQEWF3BsZnVlcnRlc0Bjb3JyZW8udWdyLmVzMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEArHWX8klJrTLJg3ADyfLh44YheJ4gwND+vl9TWFPQ
krp+Q2PKYnR0V/u9pL6ZyBbPflY8SFLdr27r9PfGsULgbGoCeIZu1VFdwta2JOBj
uPzV6vIH8jxb+0bfl/PsBqddQxaMAURzW9vgC4mzc9aNCeIpPLGkkGxYplGaWRUy
GeIQah54bs2fK8q5k+Tw4B537xEqeFQoBJhcf1fAikP4FHNGVS9OPnJGHO9r5szJ
L50K9HKhDPH6EX9t1eXSNAufvGMURhpGvZit3e2xviA2BThfbXQbT3xVjVRfYqCH
gtCpXPWXkGZZ3jGfetVmYmOINZvfPeZfv1lRJOEIrvmFmwIDAQABoAAwDQYJKoZI
hvcNAQELBQADggEBAJRiLB3I67lav07ls2vSFP6uQhOP6Xr/GM9Woz4kAnKbgGaN
EiX+NOGI7qJjl+PQON3ctYPaD4rNbHGWIiW8wWdN1RMkVLTDCECOpueep4asEhIt
dPi7E9NzoBaQw84kU+UxjUv3phVfVlxsjbgiPZz/1boNO40R+Dh5MYRvFw2wpzmN
PnlxYZCU3HSl4hE+jyxzl5CwfU2JuQDTt4H2aOXwk2QVtgHSMALG4E/MZ2VnJ2jW
JNqxDxFO3EBVzwDWa5q+inhNa1kWWLX0whCpXw7L2rhTidn6/sAxMSSHjfsNQqDq
++zlsS+sZhB9CuPi9nc14FBqzORNFA9Wtk9AmYA=
-----END CERTIFICATE REQUEST-----
```

Cread un certificado para la solicitud anterior empleando la CA subordinada.

1. Firmamos la petición

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ openssl ca -config ca/subordinad
a/openssl.cnf -in client/csr/client.csr.pem -out client/certs/client.cert.pem
Using configuration from ca/subordinada/openssl.cnf
Enter pass phrase for /home/pedro/Documents/git/inform-4-SPSI/p4/ca/subordinada
/private/subordinada.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Nov 26 10:00:00 2018 GMT
            Not After : Nov 26 10:00:00 2019 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = Granada
            localityName              = Granada
            organizationName          = SPSI
            organizationalUnitName    = utoridad Certificadora de SPSI
            commonName                = Cliente
            emailAddress              = plfuertes@correo.ugr.es
Certificate is to be certified until Nov 26 10:00:00 2019 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
```

- -config: indica la configuración que se usará.
- -in: indica dónde está la solicitud a firmar
- -out: indica dónde se guardará el certificado

* Como se puede ver, no se especifica dónde está la privada de la CA subordinada. Esto es debido que se obtiene del archivo de configuración openssl.cnf

2. Mostramos los valores

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ cat client/certs/client.cert.pem
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 4097 (0x1001)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, ST=Granada, O=SPSI, OU=utoridad Certificadora de SPSI, CN=SPSI Autoridad C
ertificadora Intermedia/emailAddress=plfuertes@correo.ugr.es
        Validity
            Not Before: Nov 26 10:00:00 2018 GMT
            Not After : Nov 26 10:00:00 2019 GMT
        Subject: C=ES, ST=Granada, L=Granada, O=SPSI, OU=utoridad Certificadora de SPSI, CN=Clie
nte/emailAddress=plfuertes@correo.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ac:75:97:f2:49:49:ad:32:c9:83:70:03:c9:f2:
                    e1:e3:86:21:78:9e:20:c0:d0:fe:be:5f:53:58:53:
                    d0:92:ba:7e:43:63:ca:62:74:74:57:fb:bd:a4:be:
                    99:c8:16:cf:7e:56:3c:48:52:dd:af:6e:eb:f4:f7:
                    c6:b1:42:e0:6c:6a:02:78:86:6e:d5:51:5d:c2:d6:
                    b6:24:e0:63:b8:fc:d5:ea:f2:07:f2:3c:5b:fb:46:
                    df:97:f3:ec:06:a7:5d:43:16:8c:01:44:73:5b:db:
                    e0:0b:89:b3:73:d6:8d:09:e2:29:3c:b1:a4:90:6c:
                    58:a6:51:9a:59:15:32:19:e2:10:6a:1e:78:6e:cd:
                    9f:2b:ca:b9:93:e4:f0:e0:1e:77:ef:11:2a:78:54:
                    28:04:98:5c:7f:57:c0:8a:43:f8:14:73:46:55:2f:
                    4e:3e:72:46:1c:ef:6b:e6:cc:c9:2f:9d:0a:f4:72:
                    a1:0c:f1:fa:11:7f:6d:d5:e5:d2:34:0b:9f:bc:63:
                    14:46:1a:46:bd:98:ad:dd:ed:b1:be:20:36:05:38:
                    5f:6d:74:1b:4f:7c:55:8d:54:5f:62:a0:87:82:d0:
                    a9:5c:f5:97:90:66:59:de:31:9f:7a:d5:66:62:63:
                    88:35:9b:df:3d:e6:5f:bf:59:51:24:e1:08:ae:f9:
                    85:9b
                Exponent: 65537 (0x10001)
```

```
Signature Algorithm: sha256WithRSAEncryption
     70:f7:f3:97:2b:51:b7:10:64:39:2d:cc:57:8f:b8:79:27:55:
     66:a8:f4:1a:b9:c2:93:79:cf:7b:c8:b3:b6:79:c3:ba:75:d1:
     0a:e7:f6:52:93:80:b1:87:e7:2a:33:e8:d3:ef:12:18:67:6e:
     2c:b7:3b:d6:64:53:0c:27:6b:04:0c:ea:6c:ff:c0:f8:f0:e4:
     86:19:fc:9a:6a:f7:b5:e2:a9:e5:6a:d1:7c:bd:2f:e4:3e:17:
     bd:61:2b:b0:b1:6c:1d:d5:35:71:77:f2:ae:86:cc:ad:9d:63:
     20:34:2b:1e:f8:5d:68:45:b2:fc:7b:90:d1:81:3e:50:36:0f:
     94:9b:d1:bc:ca:ec:f8:6b:b5:84:67:fb:2d:cc:c3:19:5c:7c:
     7a:8c:d9:ab:27:3d:c5:ec:b5:63:16:b6:dd:1f:b7:88:c4:13:
     8e:8a:83:89:cc:a2:ea:c0:80:0b:f8:59:e4:06:9c:19:f2:6d:
     23:d3:38:c7:24:5c:27:c2:af:8d:f4:2a:f7:21:ea:4a:f6:92:
     8d:51:99:ae:1e:28:ac:e1:05:dd:0b:7c:18:a8:cf:58:b3:ac:
     3d:1b:ea:e9:86:85:60:31:63:fc:63:d3:62:2a:13:d5:49:30:
     3a:96:3b:d1:97:29:1a:42:84:b1:9e:fa:b4:66:da:dd:d9:3d:
     94:ac:55:10:9b:de:27:e6:43:9d:fb:85:e2:05:bb:c0:a5:67:
     33:8c:61:09:16:30:a9:b9:64:a2:6b:b1:c7:26:f0:16:06:56:
     37:0a:79:8a:88:03:f9:49:08:b2:81:dd:f7:ce:77:d2:1c:e4:
     47:2c:bb:de:68:dd:81:9a:d4:45:d3:45:17:48:16:55:38:00:
     f6:78:9f:92:c9:10:72:fc:55:ab:51:3e:07:34:97:61:ff:4d:
     7a:92:f6:f0:d2:38:b5:b0:d8:a8:f0:c4:53:87:7f:2e:7d:d8:
     bb:f0:77:c5:f0:fe:f5:1e:65:d7:7a:27:c3:be:4e:a6:82:6c:
     80:c4:af:78:4d:d0:2a:86:68:27:dc:e5:a5:8f:bc:9b:7e:6a:
     86:ea:54:15:40:31:e4:58:bc:a5:38:90:7d:f8:de:98:c3:7a:
     8d:d5:29:76:1b:2c:26:71:51:e8:93:ab:60:d7:4f:d9:fa:32:
     66:c2:23:22:0c:c6:61:8a:a4:98:ba:cf:75:d9:ca:80:65:11:
     67:7d:53:25:8b:ef:69:c4:b2:71:1e:f2:fe:77:83:7d:60:4a:
     c4:2a:cb:85:02:14:03:71:43:a3:76:1f:d7:e0:19:15:a4:1c:
     30:c9:0c:b4:45:a2:8a:d8:8c:3a:62:43:93:13:9c:91:63:c8:
     e1:0a:3e:9f:1b:de:8d:25
```

```
-----BEGIN CERTIFICATE-----
MIIEyzCCArMCAhABMA0GCSqGSIb3DQEBCwUAMIGxMQswCQYDVQQGEwJFUzEQMA4G
A1UECAwHR3JhbmFkYTENMAsGA1UECgwEU1BTSTEnMCUGA1UECwwedXRvcmlkYWQg
Q2VydGlmaWNhZG9yYSBkZSBTUFNJMTAwLgYDVQQDDCdTUFNJIEF1dG9yaWRhZCBD
ZXJ0aWZpY2Fkb3JhIEludGVybWVkaWExJjAkBgkqhkiG9w0BCQEWF3BsZnVlcnRl
c0Bjb3JyZW8udWdyLmVzMB4XDTE4MTEyNjEwMDAwMFoXDTE5MTEyNjEwMDAwMFow
gaMxCzAJBgNVBAYTAkVTMRAwDgYDVQQIDAdHcmFuYWRhMRAwDgYDVQQHDAdHcmFu
YWRhMQ0wCwYDVQQKDARTUFNJMScwJQYDVQQLDB51dG9yaWRhZCBDZXJ0aWZpY2Fk
b3JhIGRlIFNQU0kxEDAOBgNVBAMMB0NsaWVudGUxJjAkBgkqhkiG9w0BCQEWF3Bs
ZnVlcnRlc0Bjb3JyZW8udWdyLmVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArHWX8klJrTLJg3ADyfLh44YheJ4gwND+vl9TWFPQkrp+Q2PKYnR0V/u9
pL6ZyBbPflY8SFLdr27r9PfGsULgbGoCeIZu1VFdwta2JOBjuPzV6vIH8jxb+0bf
l/PsBqddQxaMAURzW9vgC4mzc9aNCeIpPLGkkGxYplGaWRUyGeIQah54bs2fK8q5
k+Tw4B537xEqeFQoBJhcf1fAikP4FHNGVS9OPnJGHO9r5szJL50K9HKhDPH6EX9t
1eXSNAufvGMURhpGvZit3e2xviA2BThfbXQbT3xVjVRfYqCHgtCpXPWXkGZZ3jGf
etVmYmOINZvfPeZfv1lRJOEIrvmFmwIDAQABMA0GCSqGSIb3DQEBCwUAA4ICAQBw
9/OXK1G3EGQ5LcxXj7h5J1VmqPQaucKTec97yLO2ecO6ddEK5/ZSk4Cxh+cqM+jT
7xIYZ24stzvWZFMMJ2sEDOps/8D48OSGGfyaave14qnlatF8vS/kPhe9YSuwsWwd
1TVxd/KuhsytnWMgNCse+F1oRbL8e5DRgT5QNg+Um9G8yuz4a7WEZ/stzMMZXHx6
jNmrJz3F7LVjFrbdH7eIxBOOioOJzKLqwIAL+FnkBpwZ8m0j0zjHJFwnwq+N9Cr3
IepK9pKNUZmuHiis4QXdC3wYqM9Ys6w9G+rphoVgMWP8Y9NiKhPVSTA6ljvRlyka
QoSxnvq0Ztrd2T2UrFUQm94n5kOd+4XiBbvApWczjGEJFjCpuWSia7HHJvAWBlY3
CnmKiAP5SQiygd33znfSHORHLLveaN2BmtRF00UXSBZVOAD2eJ+SyRBy/FWrUT4H
NJdh/016kvbw0ji1sNio8MRTh38ufdi78HfF8P71HmXXeifDvk6mgmyAxK94TdAq
hmgn3OWlj7ybfmqG6lQVQDHkWLylOJB9+N6Yw3qN1Sl2GywmcVHok6tg10/Z+jJm
wiMiDMZhiqSYus912cqAZRFnfVMli+9pxLJxHvL+d4N9YErEKsuFAhQDcUOjdh/X
4BkVpBwwyQy0RaKK2Iw6YkOTE5yRY8jhCj6fG96NJQ==
-----END CERTIFICATE-----
```

Crear una solicitud de certificado para otra clave de las generadas en prácticas anteriores

1. Creación de la solicitud

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ openssl req -new -key ../p3/pedroDSAkey.pem -out clien
t/csr/pedroDSAkey.csr.pem -config subordinada/openssl.cnf
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.
-----
Nombre del país (Código de 2 letras) [ES]:
Provincia o Estado [Granada]:
Nombre de la localidad [Granada]:
Nombre de la organización [SPSI]:
Nombre de la unidad organizativa [utoridad Certificadora de SPSI]:
Nombre Común []:Cliente con clave DSA
Correo electrónico [plfuertes@correo.ugr.es]:
```

- Openssl req: Indica que vamos a trabajar con solicitudes de certificados
- -new: Que es una nueva solicitud
- -key: indica dónde se encuentra la clave para el certificado
- -out: dónde se va a guardar la certificación
- -config: la configuración para hacer la solicitud

2. Valor de la clave usada

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ openssl dsa -text -in ../p3/pedroDSAkey.pem
read DSA key
Private-Key: (2048 bit)
priv:
    00:8f:55:c8:4b:5e:22:77:20:e0:63:00:2b:e4:d9:
    7f:0a:c4:5e:9b:0b:2a:d0:12:8d:e1:bf:74:4a:b4:
    97:65:42
pub:
    60:74:fd:a1:0f:64:03:1a:3b:47:cb:11:e7:e9:10:
    97:4c:28:e6:ae:b9:d2:df:34:4b:57:bb:73:1f:2c:
    cf:99:23:72:b7:32:1d:2e:89:c8:df:21:4a:7c:62:
    48:6a:6e:a0:e2:c5:03:35:f8:a6:dc:d2:55:6d:3d:
    3f:93:f8:62:16:0b:3f:16:b4:bb:ec:fb:c6:61:eb:
    34:b9:ad:ca:a8:78:0f:16:81:03:81:fb:00:71:fb:
    9f:e8:bd:b3:f6:b0:c8:92:c5:d0:4a:1b:0e:e3:a3:
    06:4a:72:e2:9d:a3:1c:0c:82:91:2a:b2:f9:07:6a:
    ec:f6:12:ea:18:ea:73:a8:b6:d2:61:60:07:56:4b:
    b4:0c:21:37:52:ab:ae:2c:68:b8:f1:4a:a1:5b:5b:
    05:aa:e9:ac:14:7d:da:b2:6a:b3:80:58:2a:89:93:
    6a:11:b4:11:af:a7:d3:e8:3d:25:87:3b:d7:23:a3:
    8c:19:3d:97:bb:6b:b4:8b:82:8b:b7:6b:dc:a2:e4:
    d5:d3:84:61:13:4e:7f:69:c4:da:c8:bf:87:ad:02:
    44:cd:d7:5a:d8:8b:f3:ae:6d:7c:ea:f6:54:02:c3:
    50:1d:d2:aa:43:e0:f8:c4:bf:e7:66:d4:08:9f:70:
    9d:81:03:ca:b1:21:6c:c5:9b:91:10:82:df:9e:a6:
    99
P:
    00:c4:8d:a2:0f:3c:76:0b:a9:ca:e2:5e:2d:d5:48:
    b2:af:49:ec:fa:0a:c2:68:6d:d1:28:69:89:23:31:
    b4:fb:2c:ac:23:cc:10:c9:b4:f5:a3:e5:a3:50:bd:
    ec:8c:8e:b2:a5:ba:d9:b9:6d:15:f8:ce:f7:c2:3a:
    de:1c:d2:7a:76:b4:f7:3d:2d:21:78:7d:c3:af:bc:
    57:b1:92:52:2b:c0:b5:54:9e:09:0c:9f:65:74:d0:
    35:1a:d5:19:4d:87:76:5a:39:a4:1c:5c:52:ee:c0:
    55:81:4f:7c:23:c1:dd:d7:5f:ea:6d:06:39:4c:ec:
    a7:0a:0b:0e:34:a6:73:bb:c7:8d:ef:90:bd:80:1e:
    4e:36:6b:a4:7d:44:1d:ed:6d:85:ca:cb:64:7b:fe:
    25:d3:e0:4a:93:4e:79:f5:0e:b9:61:e3:bf:76:7c:
    64:9b:33:d4:d0:21:9e:df:7d:b5:3c:77:d3:77:2f:
    af:15:60:e1:8f:27:0b:c3:99:3e:2f:14:00:36:88:
    df:7c:45:9a:ba:65:11:93:06:c9:dd:41:31:a2:bd:
    9b:10:c7:43:e6:8c:b8:39:b0:e4:a1:9c:6d:8c:88:
    61:8e:bb:57:ea:c4:36:51:16:c7:4d:f6:35:a6:4b:
    00:ae:8e:36:64:96:73:fb:a1:51:33:df:2f:a0:57:
    a4:57
Q:
    00:e9:ba:59:ca:20:cc:a3:4f:28:19:6a:af:cf:1c:
    12:d4:60:83:4a:8d:6e:4b:24:8e:d9:b2:a6:48:0b:
    1f:b3:79
```

```
G:
    00:a6:65:f5:18:c8:94:3e:03:33:c9:1c:b3:3b:0c:
    79:e6:21:00:62:2e:f5:0e:f0:d0:07:7b:5f:67:19:
    ff:5f:41:8c:16:c7:b7:d0:9c:38:2c:e7:b6:6a:a9:
    e3:3f:79:26:4b:d8:86:8f:42:e9:4a:ab:b6:b7:0e:
    13:6c:04:8e:4d:23:35:c1:ca:68:06:9b:30:31:00:
    52:4f:be:cd:db:6a:6a:98:6c:fd:95:44:38:63:0f:
    86:34:ae:35:b5:a1:b0:03:e9:4a:51:c4:9b:26:b4:
    cf:31:15:04:31:8b:25:b6:7e:23:72:53:07:13:b0:
    d5:c9:59:ec:84:6c:a9:a2:86:47:ac:82:4c:0c:82:
    24:4f:0f:a7:15:32:84:26:bd:e1:fc:1a:69:75:07:
    dc:50:84:cc:9f:32:a9:54:6b:9e:79:b3:02:eb:a4:
    a3:6b:84:21:c5:92:12:ff:62:0b:2c:be:e5:5d:dc:
    7c:33:30:a2:0f:8d:b7:9b:b9:e4:77:7e:de:a8:e9:
    b0:ab:38:19:5b:30:2f:3f:7f:cf:49:f8:dc:9d:d5:
    b0:83:5b:da:59:66:c8:fe:5a:f0:5a:4b:e0:89:83:
    97:3f:22:1c:9e:e0:c6:94:06:a2:95:13:d2:4c:a3:
    d1:c9:bc:07:89:26:43:2f:4f:2c:55:e7:16:e1:88:
    24:42
writing DSA key
-----BEGIN DSA PRIVATE KEY-----
MIIDVwIBAAKCAQEAxI2iDzx2C6nK4l4t1Uiyr0ns+grCaG3RKGmJIzG0+yysI8wQ
ybT1o+WjUL3sjI6ypbrZuW0V+M73wjreHNJ6drT3PS0heH3Dr7xXsZJSK8C1VJ4J
DJ9ldNA1GtUZTYd2WjmkHFxS7sBVgU98I8Hd11/qbQY5TOynCgsONKZzu8eN75C9
gB5ONmukfUQd7W2Fystke/4l0+BKk0559Q65YeO/dnxkmzPU0CGe3321PHfTdy+v
FWDhjycLw5k+LxQANojffEWaumURkwbJ3UExor2bEMdD5oy4ObDkoZxtjIhhjrtX
6sQ2URbHTfY1pksAro42ZJZz+6FRM98voFekVwIhAOm6WcogzKNPKBlqr88cEtRg
g0qNbkskjtmypkgLH7N5AoIBAQCmZfUYyJQ+AzPJHLM7DHnmIQBiLvUO8NAHe19n
Gf9fQYwWx7fQnDgs57ZqqeM/eSZL2IaPQulKq7a3DhNsBI5NIzXBymgGmzAxAFJP
vs3bamqYbP2VRDhjD4Y0rjW1obAD6UpRxJsmtM8xFQQxiyW2fiNyUwcTsNXJWeyE
bKmihkesgkwMgiRPD6cVMoQmveH8Gml1B9xQhMyfMqlUa555swLrpKNrhCHFkhL/
YgssvuVd3HwzMKIPjbebueR3ft6o6bCrOBlbMC8/f89J+Nyd1bCDW9pZZsj+WvBa
S+CJg5c/Ihye4MaUBqKVE9JMo9HJvAeJJkMvTyxV5xbhiCRCAoIBAGB0/aEPZAMa
O0fLEefpEJdMKOauudLfNEtXu3MfLM+ZI3K3Mh0uicjfIUp8YkhqbqDixQM1+Kbc
0lVtPT+T+GIWCz8WtLvs+8Zh6zS5rcqoeA8WgQOB+wBx+5/ovbP2sMiSxdBKGw7j
owZKcuKdoxwMgpEqsvkHauz2EuoY6nOottJhYAdWS7QMITdSq64saLjxSqFbWwWq
6awUfdqyarOAWCqJk2oRtBGvp9PoPSWHO9cjo4wZPZe7a7SLgou3a9yi5NXThGET
Tn9pxNrIv4etAkTN11rYi/OubXzq9lQCw1Ad0qpD4PjEv+dm1AifcJ2BA8qxIWzF
m5EQgt+eppkCIQCPVchLXiJ3IOBjACvk2X8KxF6bCyrQEo3hv3RKtJdlQg==
-----END DSA PRIVATE KEY-----
```

3. Valor del certificado

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ cat client/csr/pedroDSAkey.csr.pem
-----BEGIN CERTIFICATE REQUEST-----
MIIEXzCCBAQCAQAwgbExCzAJBgNVBAYTAkVTMRAwDgYDVQQIDAdHcmFuYWRhMRAw
DgYDVQQHDAdHcmFuYWRhMQ0wCwYDVQQKDARTUFNJMScwJQYDVQQLDB51dG9yaWRh
ZCBDZXJ0aWZpY2Fkb3JhIGRlIFNQU0kxHjAcBgNVBAMMFUNsaWVudGUgY29uIGNs
YXZlIERTQTEmMCQGCSqGSIb3DQEJARYXcGxmdWVydGVzQGNvcnJlby51Z3IuZXMw
ggNHMIICOgYHKoZIzjgEATCCAi0CggEBAMSNog88dgupyuJeLdVIsq9J7PoKwmht
0ShpiSMxtPssrCPMEMm09aPlo1C97IyOsqW62bltFfjO98I63hzSena09z0tIXh9
w6+8V7GSUivAtVSeCQyfZXTQNRrVGU2Hdlo5pBxcUu7AVYFPfCPB3ddf6m0GOUzs
pwoLDjSmc7vHje+QvYAeTjZrpH1EHe1thcrLZHv+JdPgSpNOefUOuWHjv3Z8ZJsz
1NAhnt99tTx303cvrxVg4Y8nC8OZPi8UADaI33xFmrplEZMGyd1BMaK9mxDHQ+aM
uDmw5KGcbYyIYY67V+rENlEWx032NaZLAK6ONmSWc/uhUTPfL6BXpFcCIQDpulnK
IMyjTygZaq/PHBLUYINKjW5LJI7ZsqZICx+zeQKCAQEApmX1GMiUPgMzyRyzOwx5
5iEAYi71DvDQB3tfZxn/X0GMFse30Jw4LOe2aqnjP3kmS9iGj0LpSqu2tw4TbASO
TSM1wcpoBpswMQBST77N22pqmGz9lUQ4Yw+GNK41taGwA+lKUcSbJrTPMRUEMYsl
tn4jclMHE7DVyVnshGypooZHrIJMDIIkTw+nFTKEJr3h/BppdQfcUITMnzKpVGue
ebMC66Sja4QhxZIS/2ILLL7lXdx8MzCiD423m7nkd37eqOmwqzgZWzAvP3/PSfjc
ndWwg1vaWWbI/lrwWkvgiYOXPyIcnuDGlAailRPSTKPRybwHiSZDL08sVecW4Ygk
QgOCAQUAAoIBAGB0/aEPZAMaO0fLEefpEJdMKOauudLfNEtXu3MfLM+ZI3K3Mh0u
icjfIUp8YkhqbqDixQM1+Kbc0lVtPT+T+GIWCz8WtLvs+8Zh6zS5rcqoeA8WgQOB
+wBx+5/ovbP2sMiSxdBKGw7jowZKcuKdoxwMgpEqsvkHauz2EuoY6nOottJhYAdW
S7QMITdSq64saLjxSqFbWwWq6awUfdqyarOAWCqJk2oRtBGvp9PoPSWHO9cjo4wZ
PZe7a7SLgou3a9yi5NXThGETTn9pxNrIv4etAkTN11rYi/OubXzq9lQCw1Ad0qpD
4PjEv+dm1AifcJ2BA8qxIWzFm5EQgt+eppmgADALBglghkgBZQMEAwIDSAAwRQIg
TqdsIRFB5qeDr9frJwQyajGgikX9XgplQ6JShYDDaVgCIQCJcwhqZyY31DSl6b4M
kFloqhYpAfmYMsnShhmllZAphw==
-----END CERTIFICATE REQUEST-----
```

Firmamos la petición anterior con la subordinada

1. Firma de la solicitud

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ openssl ca  -in client/csr/pedroDSAkey.csr.pem -out cl
ient/certs/pedroDSAkey.cert.pem -config subordinada/openssl.cnf
Using configuration from subordinada/openssl.cnf
Enter pass phrase for /home/pedro/Documents/git/inform-4-SPSI/p4/subordinada/private/subordinada.key.
pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4098 (0x1002)
        Validity
            Not Before: Nov 27 13:08:33 2018 GMT
            Not After : Nov 27 13:08:33 2019 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = Granada
            localityName              = Granada
            organizationName          = SPSI
            organizationalUnitName    = utoridad Certificadora de SPSI
            commonName                = Cliente con clave DSA
            emailAddress              = plfuertes@correo.ugr.es
Certificate is to be certified until Nov 27 13:08:33 2019 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

2. Valor del certificado

```
pedro@ubuntu:~/Documents/git/inform-4-SPSI/p4$ cat client/certs/pedroDSAkey.cert.pem
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 4098 (0x1002)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, ST=Granada, O=SPSI, OU=utoridad Certificadora de SPSI, CN=SPSI Autoridad Certif
icadora Intermedia/emailAddress=plfuertes@correo.ugr.es
        Validity
            Not Before: Nov 27 13:08:33 2018 GMT
            Not After : Nov 27 13:08:33 2019 GMT
        Subject: C=ES, ST=Granada, L=Granada, O=SPSI, OU=utoridad Certificadora de SPSI, CN=Cliente c
on clave DSA/emailAddress=plfuertes@correo.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: dsaEncryption
                pub:
                    60:74:fd:a1:0f:64:03:1a:3b:47:cb:11:e7:e9:10:
                    97:4c:28:e6:ae:b9:d2:df:34:4b:57:bb:73:1f:2c:
                    cf:99:23:72:b7:32:1d:2e:89:c8:df:21:4a:7c:62:
                    48:6a:6e:a0:e2:c5:03:35:f8:a6:dc:d2:55:6d:3d:
                    3f:93:f8:62:16:0b:3f:16:b4:bb:ec:fb:c6:61:eb:
                    34:b9:ad:ca:a8:78:0f:16:81:03:81:fb:00:71:fb:
                    9f:e8:bd:b3:f6:b0:c8:92:c5:d0:4a:1b:0e:e3:a3:
                    06:4a:72:e2:9d:a3:1c:0c:82:91:2a:b2:f9:07:6a:
                    ec:f6:12:ea:18:ea:73:a8:b6:d2:61:60:07:56:4b:
                    b4:0c:21:37:52:ab:ae:2c:68:b8:f1:4a:a1:5b:5b:
                    05:aa:e9:ac:14:7d:da:b2:6a:b3:80:58:2a:89:93:
                    6a:11:b4:11:af:a7:d3:e8:3d:25:87:3b:d7:23:a3:
                    8c:19:3d:97:bb:6b:b4:8b:82:8b:b7:6b:dc:a2:e4:
                    d5:d3:84:61:13:4e:7f:69:c4:da:c8:bf:87:ad:02:
                    44:cd:d7:5a:d8:8b:f3:ae:6d:7c:ea:f6:54:02:c3:
                    50:1d:d2:aa:43:e0:f8:c4:bf:e7:66:d4:08:9f:70:
                    9d:81:03:ca:b1:21:6c:c5:9b:91:10:82:df:9e:a6:
                    99
```

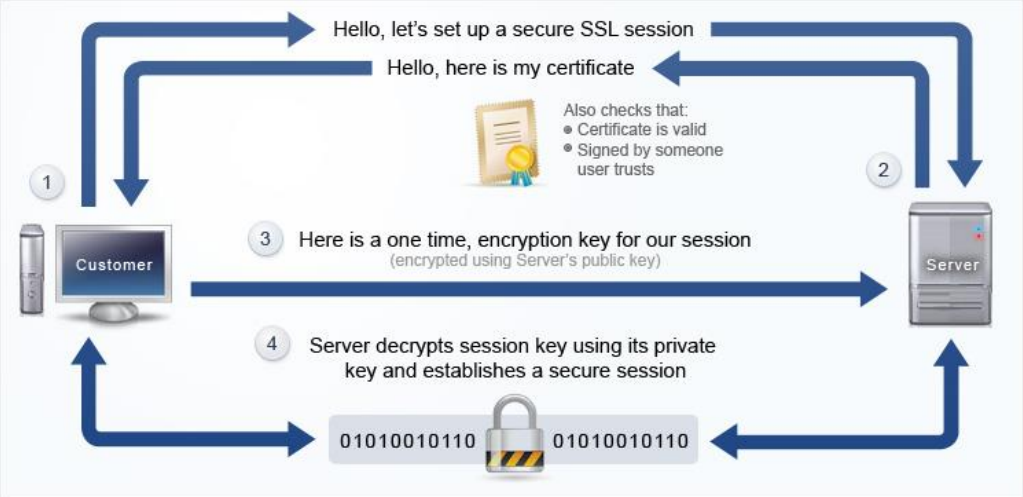
```
P:
    00:c4:8d:a2:0f:3c:76:0b:a9:ca:e2:5e:2d:d5:48:
    b2:af:49:ec:fa:0a:c2:68:6d:d1:28:69:89:23:31:
    b4:fb:2c:ac:23:cc:10:c9:b4:f5:a3:e5:a3:50:bd:
    ec:8c:8e:b2:a5:ba:d9:b9:6d:15:f8:ce:f7:c2:3a:
    de:1c:d2:7a:76:b4:f7:3d:2d:21:78:7d:c3:af:bc:
    57:b1:92:52:2b:c0:b5:54:9e:09:0c:9f:65:74:d0:
    35:1a:d5:19:4d:87:76:5a:39:a4:1c:5c:52:ee:c0:
    55:81:4f:7c:23:c1:dd:d7:5f:ea:6d:06:39:4c:ec:
    a7:0a:0b:0e:34:a6:73:bb:c7:8d:ef:90:bd:80:1e:
    4e:36:6b:a4:7d:44:1d:ed:6d:85:ca:cb:64:7b:fe:
    25:d3:e0:4a:93:4e:79:f5:0e:b9:61:e3:bf:76:7c:
    64:9b:33:d4:d0:21:9e:df:7d:b5:3c:77:d3:77:2f:
    af:15:60:e1:8f:27:0b:c3:99:3e:2f:14:00:36:88:
    df:7c:45:9a:ba:65:11:93:06:c9:dd:41:31:a2:bd:
    9b:10:c7:43:e6:8c:b8:39:b0:e4:a1:9c:6d:8c:88:
    61:8e:bb:57:ea:c4:36:51:16:c7:4d:f6:35:a6:4b:
    00:ae:8e:36:64:96:73:fb:a1:51:33:df:2f:a0:57:
    a4:57
Q:
    00:e9:ba:59:ca:20:cc:a3:4f:28:19:6a:af:cf:1c:
    12:d4:60:83:4a:8d:6e:4b:24:8e:d9:b2:a6:48:0b:
    1f:b3:79
G:
    00:a6:65:f5:18:c8:94:3e:03:33:c9:1c:b3:3b:0c:
    79:e6:21:00:62:2e:f5:0e:f0:d0:07:7b:5f:67:19:
    ff:5f:41:8c:16:c7:b7:d0:9c:38:2c:e7:b6:6a:a9:
    e3:3f:79:26:4b:d8:86:8f:42:e9:4a:ab:b6:b7:0e:
    13:6c:04:8e:4d:23:35:c1:ca:68:06:9b:30:31:00:
    52:4f:be:cd:db:6a:6a:98:6c:fd:95:44:38:63:0f:
    86:34:ae:35:b5:a1:b0:03:e9:4a:51:c4:9b:26:b4:
    cf:31:15:04:31:8b:25:b6:7e:23:72:53:07:13:b0:
    d5:c9:59:ec:84:6c:a9:a2:86:47:ac:82:4c:0c:82:
    24:4f:0f:a7:15:32:84:26:bd:e1:fc:1a:69:75:07:
    dc:50:84:cc:9f:32:a9:54:6b:9e:79:b3:02:eb:a4:
    a3:6b:84:21:c5:92:12:ff:62:0b:2c:be:e5:5d:dc:
    7c:33:30:a2:0f:8d:b7:9b:b9:e4:77:7e:de:a8:e9:
    b0:ab:38:19:5b:30:2f:3f:7f:cf:49:f8:dc:9d:d5:
    b0:83:5b:da:59:66:c8:fe:5a:f0:5a:4b:e0:89:83:
    97:3f:22:1c:9e:e0:c6:94:06:a2:95:13:d2:4c:a3:
    d1:c9:bc:07:89:26:43:2f:4f:2c:55:e7:16:e1:88:
    24:42
```

```
    Signature Algorithm: sha256WithRSAEncryption
         82:17:d0:9d:32:ba:f8:4f:46:b6:91:f5:0f:23:05:3e:55:a5:
         56:a2:7d:3e:fe:ac:82:53:35:f7:65:35:0e:0d:3e:13:6b:e1:
         76:b9:13:5d:29:2d:b3:71:7e:82:cb:2d:0c:b9:28:02:2f:ed:
         55:8c:f5:f7:3e:af:a0:ac:10:e1:54:90:e9:07:45:88:8f:88:
         3a:b0:f4:97:b4:64:71:58:31:d2:db:8d:0b:98:bf:e6:fb:38:
         e2:61:9f:e1:a5:48:22:8f:c2:98:6a:3a:d6:b1:2a:53:62:48:
         76:3f:e9:09:fd:be:1d:17:bd:40:ca:50:7c:5a:e1:9f:f6:0e:
         c5:fe:cf:44:87:47:4e:4c:58:55:e4:31:e9:be:5c:a0:81:b1:
         44:8b:0f:18:e6:37:bb:24:83:e8:1c:12:88:9b:01:bc:4b:af:
         ae:40:19:b7:81:4a:ee:7d:76:53:ed:5b:4f:20:87:ef:cd:da:
         e3:a6:0e:1c:20:f4:55:ac:bd:9d:62:de:5b:35:4a:4e:31:b0:
         7d:e7:1c:41:91:e3:48:d0:f8:dd:15:61:6c:dd:27:d5:e5:1e:
         0a:9c:68:c2:f0:9b:af:9a:cc:62:52:52:a8:fe:aa:23:87:58:
         5d:c4:42:ed:4e:33:41:19:ee:13:00:cb:9b:c1:8f:97:79:e4:
         19:35:78:85:69:14:c1:ed:70:67:b4:7e:26:f4:7e:5e:5e:28:
         64:87:50:78:38:90:9a:14:f6:48:a4:60:e0:84:75:8b:99:f1:
         22:3a:c2:31:7a:27:0f:cb:88:a8:c5:e4:9a:5c:66:14:96:24:
         b4:55:be:16:d1:3a:40:10:7a:0d:25:70:33:e5:9a:d4:8d:ff:
         4c:16:11:3e:a4:07:40:a0:87:18:9e:df:40:4e:5e:b4:d2:8e:
         09:db:5d:40:57:e7:f3:44:b8:28:df:ea:5b:fa:da:68:a4:6f:
         52:96:49:e9:16:16:7d:e1:2d:75:94:53:b2:4f:ec:95:4d:2c:
         0b:e1:33:ce:4d:87:d8:64:c3:a7:48:ef:ab:10:5c:9b:83:9e:
         2e:cb:b4:06:25:4c:b5:19:9b:a0:4a:25:49:12:cd:d6:8b:34:
         8b:42:fa:9c:fd:2e:f1:ae:d5:a0:47:d5:49:a2:35:4b:ad:65:
         cf:73:8d:3d:9c:d4:e3:bb:12:b2:cf:3c:97:d8:ac:86:bd:30:
         2d:53:15:14:64:b4:c5:fc:33:ec:45:d5:cd:6a:5d:c4:26:45:
         69:c1:c8:a6:9b:df:58:a7:e5:85:a1:61:69:e4:50:e8:5a:00:
         b2:d8:46:57:72:fa:79:60:c0:76:55:66:06:17:fd:49:31:a2:
         c1:7f:42:e4:8d:01:e5:43
-----BEGIN CERTIFICATE-----
MIIG/jCCBOYCAhACMA0GCSqGSIb3DQEBCwUAMIGxMQswCQYDVQQGEwJFUzEQMA4G
A1UECAwHR3JhbmFkYTENMAsGA1UECgwEU1BTSTEnMCUGA1UECwwedXRvcmlkYWQg
Q2VydGlmaWNhZG9yYSBkZSBTUFNJMTAwLgYDVQQDDCdTUFNJIEF1dG9yaWRhZCBD
ZXJ0aWZpY2Fkb3JhIEludGVybWVkaWExJjAkBgkqhkiG9w0BCQEWF3BsZnVlcnRl
c0Bjb3JyZW8udWdyLmVzMB4XDTE4MTEyNzEzMDgzM1oXDTE5MTEyNzEzMDgzM1ow
gbExCzAJBgNVBAYTAkVTMRAwDgYDVQQIDAdHcmFuYWRhMRAwDgYDVQQHDAdHcmFu
YWRhMQ0wCwYDVQQKDARTUFNJMScwJQYDVQQLDB51dG9yaWRhZCBDZXJ0aWZpY2Fk
b3JhIGRlIFNQU0kxHjAcBgNVBAMMFUNsaWVudGUgY29uIGNsYXZlIERTQTEmMCQG
CSqGSIb3DQEJARYXcGxmdWVydGVzQGNvcnJlby51Z3IuZXMwggNHMIICOgYHKoZI
zjgEATCCAi0CggEBAMSNog88dgupyuJeLdVIsq9J7PoKwmht0ShpiSMxtPssrCPM
EMm09aPlo1C97IyOsqW62bltFfjO98I63hzSena09z0tIXh9w6+8V7GSUivAtVSe
CQyfZXTQNRrVGU2Hdlo5pBxcUu7AVYFPfCPB3ddf6m0GOUzspwoLDjSmc7vHje+Q
vYAeTjZrpH1EHe1thcrLZHv+JdPgSpNOefUOuWHjv3Z8ZJsz1NAhnt99tTx303cv
rxVg4Y8nC8OZPi8UADaI33xFmrplEZMGyd1BMaK9mxDHQ+aMuDmw5KGcbYyIYY67
V+rENlEWx032NaZLAK6ONmSWc/uhUTPfL6BXpFcCIQDpulnKIMyjTygZaq/PHBLU
YINKjW5LJI7ZsqZICx+zeQKCAQEApmX1GMiUPgMzyRyzOwx55iEAYi71DvDQB3tf
Zxn/X0GMFse30Jw4LOe2aqnjP3kmS9iGj0LpSqu2tw4TbASOTSM1wcpoBpswMQBS
T77N22pqmGz9lUQ4Yw+GNK41taGwA+lKUcSbJrTPMRUEMYsltn4jclMHE7DVyVns
hGypooZHrIJMDIIkTw+nFTKEJr3h/BppdQfcUITMnzKpVGueebMC66Sja4QhxZIS
/2ILLL7lXdx8MzCiD423m7nkd37eqOmwqzgZWzAvP3/PSfjcndWwg1vaWWbI/lrw
WkvgiYOXPyIcnuDGlAailRPSTKPRybwHiSZDL08sVecW4YgkQgOCAQUAAoIBAGB0
/aEPZAMaO0fLEefpEJdMKOauudLfNEtXu3MfLM+ZI3K3Mh0uicjfIUp8YkhqbqDi
xQM1+Kbc0lVtPT+T+GIWCz8WtLvs+8Zh6zS5rcqoeA8WgQOB+wBx+5/ovbP2sMiS
xdBKGw7jowZKcuKdoxwMgpEqsvkHauz2EuoY6nOottJhYAdWS7QMITdSq64saLjx
SqFbWwWq6awUfdqyarOAWCqJk2oRtBGvp9PoPSWHO9cjo4wZPZe7a7SLgou3a9yi
5NXThGETTn9pxNrIv4etAkTN11rYi/OubXzq9lQCw1Ad0qpD4PjEv+dm1AifcJ2B
A8qxIWzFm5EQgt+eppkwDQYJKoZIhvcNAQELBQADggIBAIIX0J0yuvhPRraR9Q8j
BT5VpVaifT7+rIJTNfdlNQ4NPhNr4Xa5E10pLbNxfoLLLQy5KAIv7VWM9fc+r6Cs
EOFUkOkHRYiPiDqw9Je0ZHFYMdLbjQuYv+b7OOJhn+GlSCKPwphqOtaxKlNiSHY/
6Qn9vh0XvUDKUHxa4Z/2DsX+z0SHR05MWFXkMem+XKCBsUSLDxjmN7skg+gcEoib
AbxLr65AGbeBSu59dlPtW08gh+/N2uOmDhwg9FWsvZ1i3ls1Sk4xsH3nHEGR40jQ
+N0VYWzdJ9XlHgqcaMLwm6+azGJSUqj+qiOHWF3EQu1OM0EZ7hMAy5vBj5d55Bk1
eIVpFMHtcGe0fib0fl5eKGSHUHg4kJoU9kikYOCEdYuZ8SI6wjF6Jw/LiKjF5Jpc
ZhSWJLRVvhbROkAQeg0lcDPlmtSN/0wWET6kB0Cghxie30BOXrTSjgnbXUBX5/NE
uCjf6lv62mikb1KWSekWFn3hLXWUU7JP7JVNLAvhM85Nh9hkw6dI76sQXJuDni7L
tAYlTLUZm6BKJUkSzdaLNItC+pz9LvGu1aBH1UmiNUutZc9zjT2c1OO7ErLPPJfY
rIa9MC1TFRRktMX8M+xF1c1qXcQmRWnByKab31in5YWhYWnkUOhaALLYRldy+nlg
wHZVZgYX/UkxosF/QuSNAeVD
-----END CERTIFICATE-----
```

3. Conclusiones

Se puede ver como al mostrar el valor del certificado aparecen los valores públicos de la clave (DSA en este caso) usada. Esto se utiliza para poder enviar una clave de sesión cifrada con la pública del servidor y que sólo ese servidor pueda descifrarla con la pública.

El proceso es más o menos este:



* Imagen obtenida de aquí.