Práctica 4: Certificados digitales

> Ángel Gómez Martín
>
> agomezm@correo.ugr.es
>
> Seguridad y Protección de Sistemas Informáticos
>
> UGR 2018-19

Tareas

> Para determinar la sintaxis de las ordenes a utilizar me he basado en el manual de OpenSSL.
>
> Otras referencias:
>
> - https://blog.guillen.io/2018/09/29/crear-autoridad-certificadora-ca-y-certificados-autofirmados-en-linux/
> - http://www.juanluramirez.com/crear-autoridad-certificadora-ssl/
> - https://www.bdat.net/documentos/certificados_digitales/x309.html
> - https://www.question-defense.com/2009/09/22/use-openssl-to-verify-the-contents-of-a-csr-before-submitting-for-a-ssl-certificate

1

En primer lugar preparo el directorio que voy a usar para la entidad certificadora:

```
# Creo el directorio principal donde se almacenará la CA.
mkdir CA
cd CA

# Creo los directorios necesarios.
mkdir certs crl newcerts private
chmod 700 private

# Creo los archivos necesarios para la BD de la CA.
touch index.txt
echo 1000 > serial
```

Tras esto creo el archivo *openssl.cnf* y configuro los parámetros para la CA:

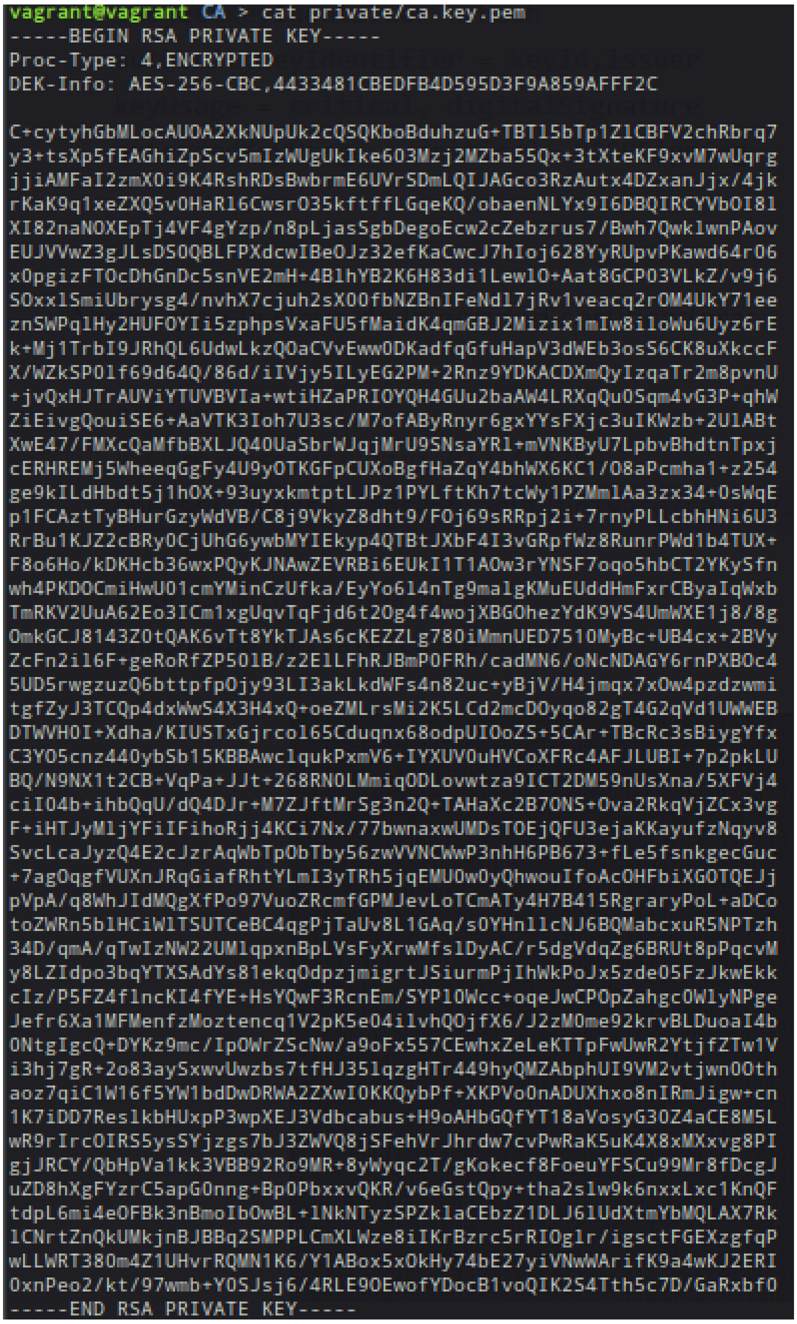
```
# Copio el archivo.
touch openssl.cnf
```

```
# Configuro los parámetros del archivo para que quede de la siguiente forma:
[ ca ]
default_ca = CA_default

[ CA_default ]
dir               = .
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/ca.key.pem
certificate       = $dir/certs/ca.cert.pem

crlnumber         = $dir/crlnumber
crl               = $dir/crl/ca.crl.pem
crl_extensions    = crl_ext
default_crl_days  = 30

default_md        = sha256

name_opt          = ca_default
cert_opt          = ca_default
default_days      = 375
preserve          = no
policy            = policy_strict

[ policy_strict ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ policy_loose ]
countryName             = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ req ]
default_bits        = 2048
distinguished_name  = req_distinguished_name
string_mask         = utf8only

default_md          = sha256
```

```
x509_extensions     = v3_ca

[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
stateOrProvinceName             = State or Province Name
localityName                    = Locality Name
0.organizationName              = Organization Name
organizationalUnitName          = Organizational Unit Name
commonName                      = Common Name
emailAddress                    = Email Address

[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ v3_intermediate_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ usr_cert ]
basicConstraints = CA:FALSE
nsCertType = client, email
nsComment = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection

[ server_cert ]
basicConstraints = CA:FALSE
nsCertType = server
nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth

[ crl_ext ]
authorityKeyIdentifier=keyid:always

[ ocsp ]
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, digitalSignature
extendedKeyUsage = critical, OCSPSigning
```

Ahora creo la clave de la entidad certificadora:

```
# Genero clave.
# Como pass utilizo: 0123456789
openssl genrsa -aes256 -out private/ca.key.pem 4096

# Le cambio los permisos
chmod 400 private/ca.key.pem
```



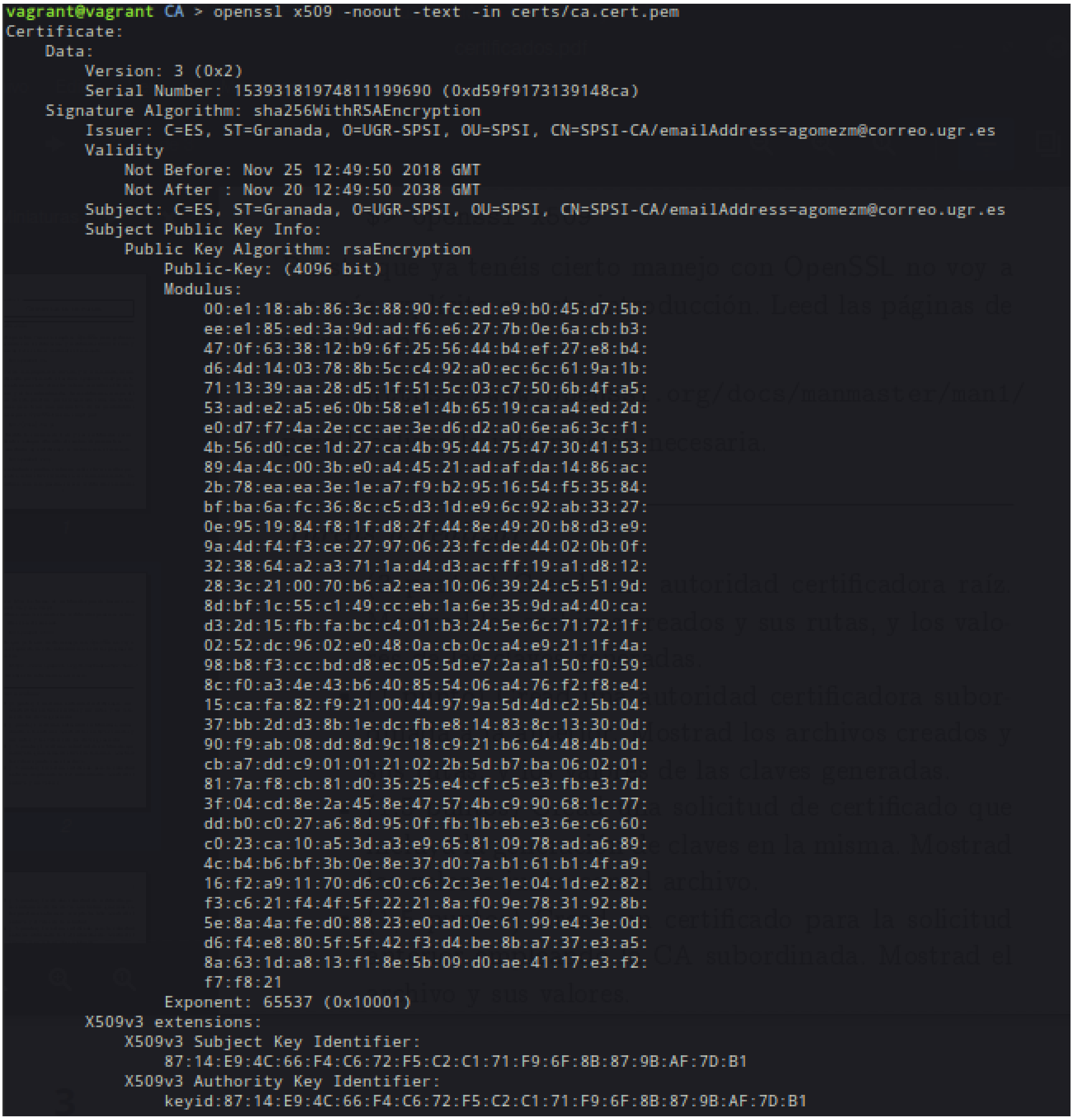
```
vagrant@vagrant CA > cat private/ca.key.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,4433481CBEDFB4D595D3F9A859AFFF2C

C+cytyhGbMLocAUOA2XkNUpUk2cQSQKboBduhzuG+TBT15bTp1Z1CBFV2chRbrq7
y3+tsXp5fEAGhiZpScv5mIzWUgUkIke603Mzj2MZba55Qx+3tXteKF9xvM7wUqrg
jjiAMFaI2zmX0i9K4RshRDsBwbrmE6UVrSDmLQIJAGco3RzAutx4DZxanJjx/4jk
rKaK9q1xeZXQ5v0HaR16Cwsr035kftffLGqeKQ/obaenNLYx9I6DBQIRCYVbOI8l
XI82naNOXEpTj4VF4gYzp/n8pLjasSgbDegoEcw2cZebzrus7/Bwh7Qwk1wnPAov
EUJVVwZ3gJLsDS0QBLFPXdcwIBeOJz32efKaCwcJ7hIoj628YyRUpvPKawd64r06
x0pgizFTOcDhGnDc5snVE2mH+4B1hYB2K6H83di1Lew1O+Aat8GCP03VLkZ/v9j6
SOxx1SmiUbrysg4/nvhX7cjuh2sX00fbNZBnIFeNd17jRv1veacq2rOM4UkY71ee
znSWPq1Hy2HUFOYIi5zphpsVxaFU5fMaidK4qmGBJ2Mizix1mIw8iloWu6Uyz6rE
k+Mj1TrbI9JRhQL6UdwLkzQOaCVvEwwODKadfqGfuHapV3dWEb3osS6CK8uXkccF
X/WZkSP01f69d64Q/86d/iIVjy5ILyEG2PM+2Rnz9YDKACDXmQyIzqaTr2m8pvnU
+jvQxHJTrAUViYTUVBVIa+wtiHZaPRIOYQH4GUu2baAW4LRXqQu0Sqm4vG3P+qhW
ZiEivgQouiSE6+AaVTK3Ioh7U3sc/M7ofAByRnyr6gxYYsFXjc3uIKWzb+2U1ABt
XwE47/FMXcQaMfbBXLJQ40UaSbrWJqjMrU9SNsaYR1+mVNKByU7LpbvBhdtnTpxj
cERHREMj5WheeqGgFy4U9yOTKGFpCUXoBgfHaZqY4bhWX6KC1/O8aPcmha1+z254
ge9kILdHbdt5j1hOX+93uyxkmtptLJPz1PYLftKh7tcWy1PZMml1Aa3zx34+OsWqE
p1FCAztTyBHurGzyWdVB/C8j9VkyZ8dht9/FOj69sRRpj2i+7rnyPLLcbhHNi6U3
RrBu1KJZ2cBRyOCjUhG6ywbMYIEkyp4QTBtJXbF4I3vGRpfWz8RunrPWd1b4TUX+
F8o6Ho/kDKHcb36wxPQyKJNAwZEVRBi6EUkI1T1AOw3rYNSF7oqo5hbCT2YKySfn
wh4PKDOCmiHwU01cmYMinCzUfka/EyYo614nTg9ma1gKMuEUddHmFxrCByaIqWxb
TmRKV2UuA62Eo3ICm1xgUqvTqFjd6t2Og4f4wojXBGOhezYdK9VS4UmWXE1j8/8g
OmkGCJ8143Z0tQAK6vTt8YkTJAs6cKEZZLg780iMmnUED7510MyBc+UB4cx+2BVy
ZcFn2il6F+geRoRfZP501B/z2E1LFhRJBmP0FRh/cadMN6/oNcNDAGY6rnPXBOc4
5UD5rwgzuzQ6bttpfpOjy93LI3akLkdWFs4n82uc+yBjV/H4jmqx7xOw4pzdzwmi
tgfZyJ3TCQp4dxWwS4X3H4xQ+oeZMLrsMi2K5LCd2mcDOyqo82gT4G2qVd1UWWEB
DTWVHOI+Xdha/KIUSTxGjrco165Cduqnx68odpUIOoZS+5CAr+TBcRc3sBiygYfx
C3YO5cnz44OybSb15KBBAwclqukPxmV6+IYXUVOuHVCoXFRc4AFJLUBI+7p2pkLU
BQ/N9NX1t2CB+VqPa+JJt+268RNOLMmiqODLovwtza9ICT2DM59nUsXna/5XFVj4
ciI04b+ihbQqU/dQ4DJr+M7ZJftMrSg3n2Q+TAHaXc2B7ONS+Ova2RkqVjZCx3vg
F+iHTJyM1jYFiIFihoRjj4KCi7Nx/77bwnaxwUMDsTOEjQFU3ejaKKayufzNqyv8
SvcLcaJyzQ4E2cJzrAqWbTpObTby56zwVVNCWwP3nhH6PB673+fLe5fsnkgecGuc
+7agOqgfVUXnJRqGiafRhtYLmI3yTRh5jqEMUOwOyQhwouIfoAcOHFbiXGOTQEJj
pVpA/q8WhJIdMQgXfPo97VuoZRcmfGPMJevLoTCmATy4H7B415RgraryPoL+aDCo
toZWRn5b1HCiW1TSUTCeBC4qgPjTaUv8L1GAq/sOYHn11cNJ6BQMabcxuR5NPTzh
34D/qmA/qTwIzNW22UM1qpxnBpLVsFyXrwMfs1DyAC/r5dgVdqZg6BRUt8pPqcvM
y8LZIdpo3bqYTXSAdYs81ekqOdpzjmigrtJSiurmPjIhWkPoJx5zde05FzJkwEkk
cIz/P5FZ4f1ncKI4fYE+HsYQwF3RcnEm/SYP10Wcc+oqeJwCPOpZahgcOW1yNPge
Jefr6Xa1MFMenfzMoztencq1V2pK5e04i1vhQOjfX6/J2zMOme92krvBLDuoaI4b
ONtgIgcQ+DYKz9mc/IpOWrZScNw/a9oFx557CEwhxZeLeKTTpFwUwR2YtjfZTw1V
i3hj7gR+2o83aySxwvUwzbs7tfHJ35lqzgHTr449hyQMZAbphUI9VM2vtjwnOOth
aoz7qiC1W16f5YW1bdDwDRWA2ZXwIOKKQybPf+XKPVoOnADUXhxo8nIRmJigw+cn
1K7iDD7Res1kbHUxpP3wpXEJ3Vdbcabus+H9oAHbGQfYT18aVosyG30Z4aCE8M5L
wR9rIrcOIRS5ysSYjzgs7bJ3ZWVQ8jSFehVrJhrdw7cvPwRaK5uK4X8xMXxvg8PI
gjJRCY/QbHpVa1kk3VBB92Ro9MR+8yWyqc2T/gKokecf8FoeuYFSCu99Mr8fDcgJ
uZD8hXgFYzrC5apGOnng+BpOPbxxvQKR/v6eGstQpy+tha2s1w9k6nxxLxc1KnQF
tdpL6mi4eOFBk3nBmoIbOwBL+1NkNTyzSPZk1aCEbzZ1DLJ61UdXtmYbMQLAX7Rk
lCNrtZnQkUMkjnBJBBq2SMPPLCmXLWze8iIKrBzrc5rRIOglr/igsctFGEXzgfqP
wLLWRT380m4Z1UHvrRQMN1K6/Y1ABox5xOkHy74bE27yiVNwWArifK9a4wKJ2ERI
OxnPeo2/kt/97wmb+YOSJsj6/4RLE9OEwofYDocB1voQIK2S4Tth5c7D/GaRxbfO
-----END RSA PRIVATE KEY-----
```

Creo ahora el certificado de la entidad certificadora:

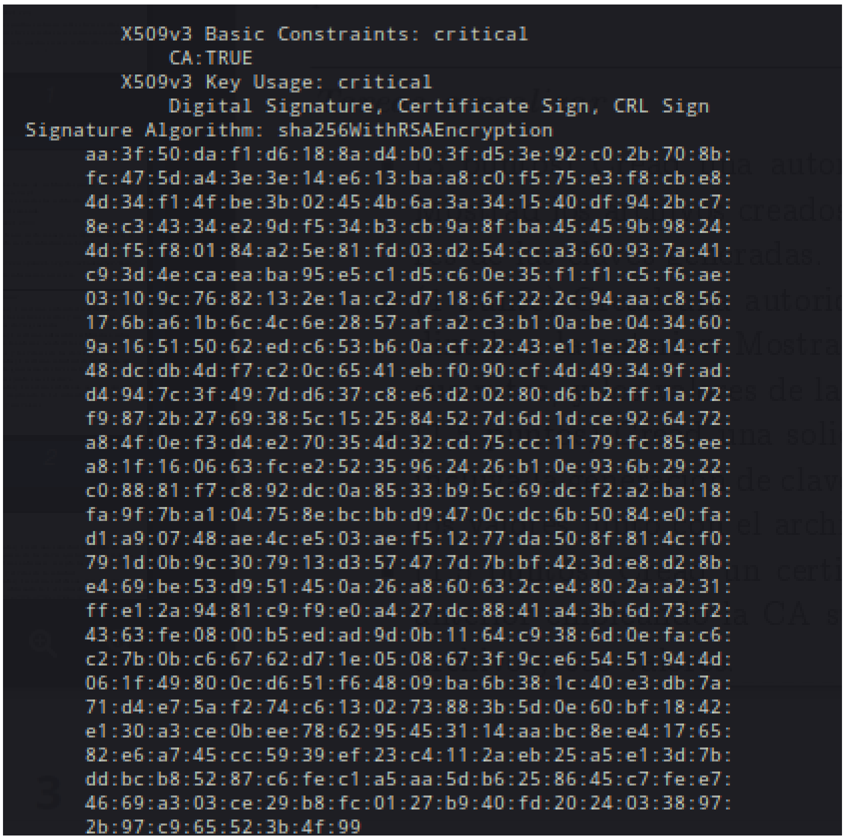
```
# Creo certificado:
openssl req -config openssl.cnf -key private/ca.key.pem -new -x509 -days 7300 -sha256 -
extensions v3_ca -out certs/ca.cert.pem

# Cambio permisos del certificado:
chmod 444 certs/ca.cert.pem
```

Verifico el certificado:

```
openssl x509 -noout -text -in certs/ca.cert.pem
```



```
vagrant@vagrant CA > openssl x509 -noout -text -in certs/ca.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 15393181974811199690 (0xd59f9173139148ca)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, ST=Granada, O=UGR-SPSI, OU=SPSI, CN=SPSI-CA/emailAddress=agomezm@correo.ugr.es
        Validity
            Not Before: Nov 25 12:49:50 2018 GMT
            Not After : Nov 20 12:49:50 2038 GMT
        Subject: C=ES, ST=Granada, O=UGR-SPSI, OU=SPSI, CN=SPSI-CA/emailAddress=agomezm@correo.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:e1:18:ab:86:3c:88:90:fc:ed:e9:b0:45:d7:5b:
                    ee:e1:85:ed:3a:9d:ad:f6:e6:27:7b:0e:6a:cb:b3:
                    47:0f:63:38:12:b9:6f:25:56:44:b4:ef:27:e8:b4:
                    d6:4d:14:03:78:8b:5c:c4:92:a0:ec:6c:61:9a:1b:
                    71:13:39:aa:28:d5:1f:51:5c:03:c7:50:6b:4f:a5:
                    53:ad:e2:a5:e6:0b:58:e1:4b:65:19:ca:a4:ed:2d:
                    e0:d7:f7:4a:2e:cc:ae:3e:d6:d2:a0:6e:a6:3c:f1:
                    4b:56:d0:ce:1d:27:ca:4b:95:44:75:47:30:41:53:
                    89:4a:4c:00:3b:e0:a4:45:21:ad:af:da:14:86:ac:
                    2b:78:ea:ea:3e:1e:a7:f9:b2:95:16:54:f5:35:84:
                    bf:ba:6a:fc:36:8c:c5:d3:1d:e9:6c:92:ab:33:27:
                    0e:95:19:84:f8:1f:d8:2f:44:8e:49:20:b8:d3:e9:
                    9a:4d:f4:f3:ce:27:97:06:23:fc:de:44:02:0b:0f:
                    32:38:64:a2:a3:71:1a:d4:d3:ac:ff:19:a1:d8:12:
                    28:3c:21:00:70:b6:a2:ea:10:06:39:24:c5:51:9d:
                    8d:bf:1c:55:c1:49:cc:eb:1a:6e:35:9d:a4:40:ca:
                    d3:2d:15:fb:fa:bc:c4:01:b3:24:5e:6c:71:72:1f:
                    02:52:dc:96:02:e0:48:0a:cb:0c:a4:e9:21:1f:4a:
                    98:b8:f3:cc:bd:d8:ec:05:5d:e7:2a:a1:50:f0:59:
                    8c:f0:a3:4e:43:b6:40:85:54:06:a4:76:f2:f8:e4:
                    15:ca:fa:82:f9:21:00:44:97:9a:5d:4d:c2:5b:04:
                    37:bb:2d:d3:8b:1e:dc:fb:e8:14:83:8c:13:30:0d:
                    90:f9:ab:08:dd:8d:9c:18:c9:21:b6:64:48:4b:0d:
                    cb:a7:dd:c9:01:01:21:02:2b:5d:b7:ba:06:02:01:
                    81:7a:f8:cb:81:d0:35:25:e4:cf:c5:e3:fb:e3:7d:
                    3f:04:cd:8e:2a:45:8e:47:57:4b:c9:90:68:1c:77:
                    dd:b0:c0:27:a6:8d:95:0f:fb:1b:eb:e3:6e:c6:60:
                    c0:23:ca:10:a5:3d:a3:e9:65:81:09:78:ad:a6:89:
                    4c:b4:b6:bf:3b:0e:8e:37:d0:7a:b1:61:b1:4f:a9:
                    16:f2:a9:11:70:d6:c0:c6:2c:3e:1e:04:1d:e2:82:
                    f3:c6:21:f4:4f:5f:22:21:8a:f0:9e:78:31:92:8b:
                    5e:8a:4a:fe:d0:88:23:e0:ad:0e:61:99:e4:3e:0d:
                    d6:f4:e8:80:5f:5f:42:f3:d4:be:8b:a7:37:e3:a5:
                    8a:63:1d:a8:13:f1:8e:5b:09:d0:ae:41:17:e3:f2:
                    f7:f8:21
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                87:14:E9:4C:66:F4:C6:72:F5:C2:C1:71:F9:6F:8B:87:9B:AF:7D:B1
            X509v3 Authority Key Identifier:
                keyid:87:14:E9:4C:66:F4:C6:72:F5:C2:C1:71:F9:6F:8B:87:9B:AF:7D:B1
```



```
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
         aa:3f:50:da:f1:d6:18:8a:d4:b0:3f:d5:3e:92:c0:2b:70:8b:
         fc:47:5d:a4:3e:3e:14:e6:13:ba:a8:c0:f5:75:e3:f8:cb:e8:
         4d:34:f1:4f:be:3b:02:45:4b:6a:3a:34:15:40:df:94:2b:c7:
         8e:c3:43:34:e2:9d:f5:34:b3:cb:9a:8f:ba:45:45:9b:98:24:
         4d:f5:f8:01:84:a2:5e:81:fd:03:d2:54:cc:a3:60:93:7a:41:
         c9:3d:4e:ca:ea:ba:95:e5:c1:d5:c6:0e:35:f1:f1:c5:f6:ae:
         03:10:9c:76:82:13:2e:1a:c2:d7:18:6f:22:2c:94:aa:c8:56:
         17:6b:a6:1b:6c:4c:6e:28:57:af:a2:c3:b1:0a:be:04:34:60:
         9a:16:51:50:62:ed:c6:53:b6:0a:cf:22:43:e1:1e:28:14:cf:
         48:dc:db:4d:f7:c2:0c:65:41:eb:f0:90:cf:4d:49:34:9f:ad:
         d4:94:7c:3f:49:7d:d6:37:c8:e6:d2:02:80:d6:b2:ff:1a:72:
         f9:87:2b:27:69:38:5c:15:25:84:52:7d:6d:1d:ce:92:64:72:
         a8:4f:0e:f3:d4:e2:70:35:4d:32:cd:75:cc:11:79:fc:85:ee:
         a8:1f:16:06:63:fc:e2:52:35:96:24:26:b1:0e:93:6b:29:22:
         c0:88:81:f7:c8:92:dc:0a:85:33:b9:5c:69:dc:f2:a2:ba:18:
         fa:9f:7b:a1:04:75:8e:bc:bb:d9:47:0c:dc:6b:50:84:e0:fa:
         d1:a9:07:48:ae:4c:e5:03:ae:f5:12:77:da:50:8f:81:4c:f0:
         79:1d:0b:9c:30:79:13:d3:57:47:7d:7b:bf:42:3d:e8:d2:8b:
         e4:69:be:53:d9:51:45:0a:26:a8:60:63:2c:e4:80:2a:a2:31:
         ff:e1:2a:94:81:c9:f9:e0:a4:27:dc:88:41:a4:3b:6d:73:f2:
         43:63:fe:08:00:b5:ed:ad:9d:0b:11:64:c9:38:6d:0e:fa:c6:
         c2:7b:0b:c6:67:62:d7:1e:05:08:67:3f:9c:e6:54:51:94:4d:
         06:1f:49:80:0c:d6:51:f6:48:09:ba:6b:38:1c:40:e3:db:7a:
         71:d4:e7:5a:f2:74:c6:13:02:73:88:3b:5d:0e:60:bf:18:42:
         e1:30:a3:ce:0b:ee:78:62:95:45:31:14:aa:bc:8e:e4:17:65:
         82:e6:a7:45:cc:59:39:ef:23:c4:11:2a:eb:25:a5:e1:3d:7b:
         dd:bc:b8:52:87:c6:fe:c1:a5:aa:5d:b6:25:86:45:c7:fe:e7:
         46:69:a3:03:ce:29:b8:fc:01:27:b9:40:fd:20:24:03:38:97:
         2b:97:c9:65:52:3b:4f:99
```

Habiendo comprobado que la verificación es correcta sabemos que la entidad certificadora está creada correctamente.

2

Para crear una entidad subordinada primero preparo el entorno:

```
# Directorio para la CA subordinada
mkdir SUB

mkdir certs crl csr newcerts private
chmod 700 private
touch index.txt
echo 1000 > serial
```

Ahora creo el archivo de configuración, que tiene la siguiente forma:

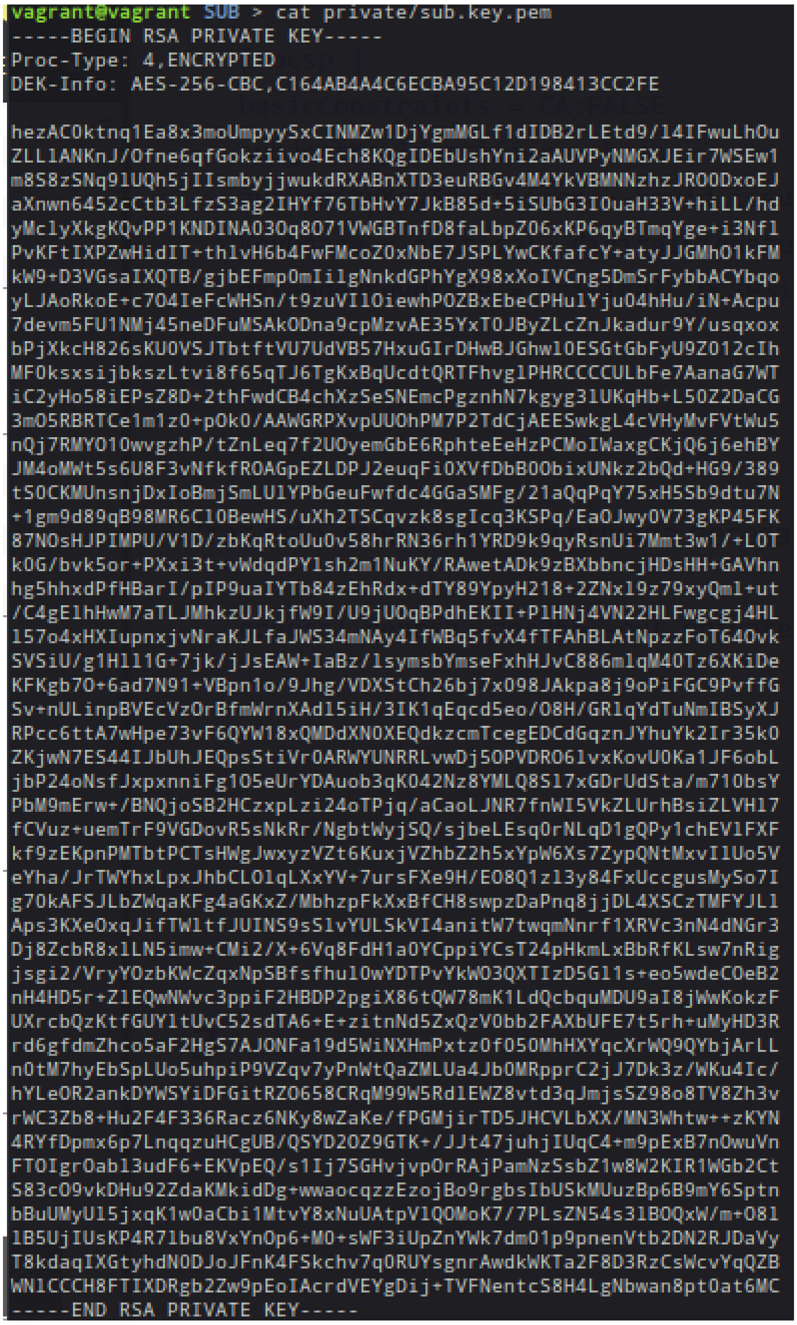
```
[ ca ]
default_ca = CA_default
```

```
[ CA_default ]
dir               = .
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/sub.key.pem
certificate       = $dir/certs/sub.cert.pem

crlnumber         = $dir/crlnumber
crl               = $dir/crl/sub.crl.pem
crl_extensions    = crl_ext
default_crl_days  = 30

default_md        = sha256

name_opt          = ca_default
cert_opt          = ca_default
default_days      = 375
preserve          = no
policy            = policy_loose

[ policy_strict ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ policy_loose ]
countryName             = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ req ]
default_bits        = 2048
distinguished_name  = req_distinguished_name
string_mask         = utf8only

default_md          = sha256

x509_extensions     = v3_ca

[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
```

```
stateOrProvinceName             = State or Province Name
localityName                    = Locality Name
0.organizationName              = Organization Name
organizationalUnitName          = Organizational Unit Name
commonName                      = Common Name
emailAddress                    = Email Address


[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ v3_intermediate_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ usr_cert ]
basicConstraints = CA:FALSE
nsCertType = client, email
nsComment = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection

[ server_cert ]
basicConstraints = CA:FALSE
nsCertType = server
nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth

[ crl_ext ]
authorityKeyIdentifier=keyid:always

[ ocsp ]
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, digitalSignature
extendedKeyUsage = critical, OCSPSigning
```

Tras esto, creo el la clave privada necesaria:

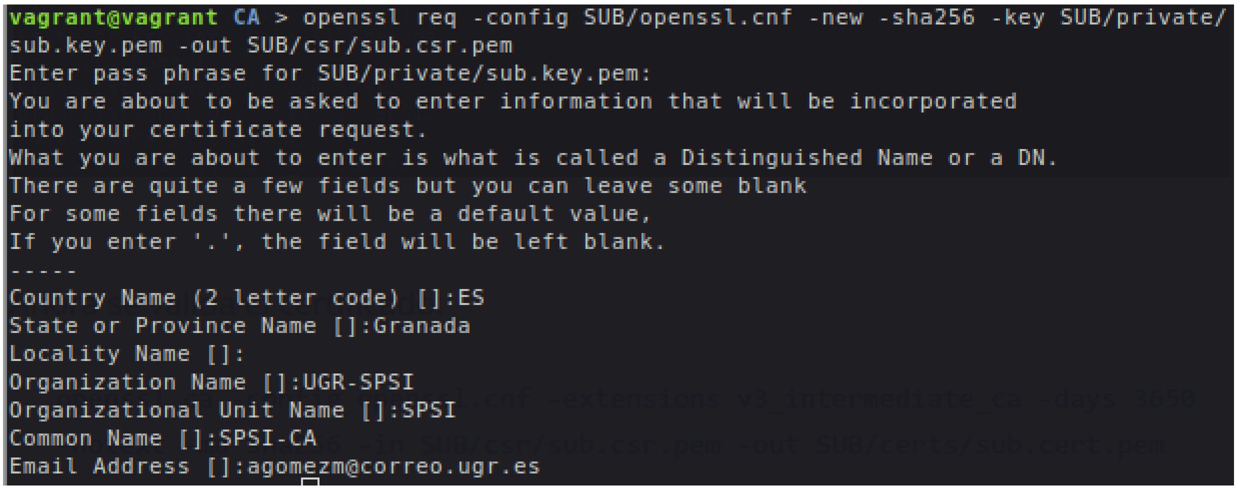
```
openssl genrsa -aes256 -out private/sub.key.pem 4096

# Modifico sus permisos
chmod 400 private/sub.key.pem
```



```
vagrant@vagrant SUB > cat private/sub.key.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,C164AB4A4C6ECBA95C12D198413CC2FE

hezAC0ktnq1Ea8x3moUmpyySxCINMZw1DjYgmMGLf1dIDB2rLEtd9/14IFwuLh0u
ZLL1ANKnJ/0fne6qfGokziivo4Ech8KQgIDEbUshYni2aAUVPyNMGXJEir7WSEw1
m8S8zSNq91UQh5jIIsmbyjjwukdRXABnXTD3euRBGv4M4YkVBMNNzhzJROODxoEJ
aXnwn6452cCtb3LfzS3ag2IHYf76TbHvY7JkB85d+5iSUbG3I0uaH33V+hiLL/hd
yMclyXkgKQvPP1KNDINA03Oq8071VWGBTnfD8faLbpZ06xKP6qyBTmqYge+i3Nfl
PvKFtIXPZwHidIT+thlvH6b4FwFMcoZ0xNbE7JSPLYwCKfafcY+atyJJGMh01kFM
kW9+D3VGsaIXQTB/gjbEFmp0mIilgNnkdGPhYgX98xXoIVCng5DmSrFybbACYbqo
yLJAoRkoE+c704IeFcWHSn/t9zuVIl0iewhPOZBxEbeCPHulYju04hHu/iN+Acpu
7devm5FU1NMj45neDFuMSAkODna9cpMzvAE35YxT0JByZLcZnJkadur9Y/usqxox
bPjXkcH826sKU0VSJTbtftVU7UdVB57HxuGIrDHwBJGhwl0ESGtGbFyU9Z012cIh
MF0ksxsijbkszLtvi8f65qTJ6TgKxBqUcdtQRTFhvglPHRCCCCULbFe7AanaG7WT
iC2yHo58iEPsZ8D+2thFwdCB4chXzSeSNEmcPgznhN7kgyg31UKqHb+L50Z2DaCG
3mO5RBRTCe1m1z0+pOk0/AAWGRPXvpUUOhPM7P2TdCjAEESwkgL4cVHyMvFVtWu5
nQj7RMYO10wvgzhP/tZnLeq7f2UOyemGbE6RphteEeHzPCMoIWaxgCKjQ6j6ehBY
JM4oMWt5s6U8F3vNfkfROAGpEZLDPJ2euqFi0XVfDbBOObixUNkz2bQd+HG9/389
tSOCKMUnsnjDxIoBmjSmLU1YPbGeuFwfdc4GGaSMFg/21aQqPqY75xH5Sb9dtu7N
+1gm9d89qB98MR6C10BewHS/uXh2TSCqvzk8sgIcq3KSPq/EaOJwy0V73gKP45FK
87NOsHJPIMPU/V1D/zbKqRtoUu0v58hrRN36rh1YRD9k9qyRsnUi7Mmt3w1/+LOT
kOG/bvk5or+PXxi3t+vWdqdPYlsh2m1NuKY/RAwetADk9zBXbbncjHDsHH+GAVhn
hg5hhxdPfHBarI/pIP9uaIYTb84zEhRdx+dTY89YpyH218+2ZNxl9z79xyQml+ut
/C4gElhHwM7aTLJMhkzUJkjfW9I/U9jUOqBPdhEKII+PlHNj4VN22HLFwgcgj4HL
l57o4xHXIupnxjvNraKJLfaJWS34mNAy4IfWBq5fvX4fTFAhBLAtNpzzFoT64Ovk
SVSiU/g1Hl11G+7jk/jJsEAW+IaBz/lsymsbYmseFxhHJvC886mlqM40Tz6XKiDe
KFKgb7O+6ad7N91+VBpn1o/9Jhg/VDXStCh26bj7x098JAkpa8j9oPiFGC9PvffG
Sv+nULinpBVEcVzOrBfmWrnXAdl5iH/3IK1qEqcd5eo/O8H/GR1qYdTuNmIBSyXJ
RPcc6ttA7wHpe73vF6QYW18xQMDdXN0XEQdkzcmTcegEDCdGqznJYhuYk2Ir35kO
ZKjwN7ES44IJbUhJEQpsStiVr0ARWYUNRRLvwDj5OPVDRO6lvxKovU0Ka1JF6obL
jbP24oNsfJxpxnniFg105eUrYDAuob3qK042Nz8YWLQ8Sl7xGDrUdSta/m710bsY
PbM9mErw+/BNQjoSB2HCzxpLzi24oTPjq/aCaoLJNR7fnWI5VkZLUrhBsiZLVH17
fCVuz+uemTrF9VGDovR5sNkRr/NgbtWyjSQ/sjbeLEsq0rNLqD1gQPy1chEV1FXF
kf9zEKpnPMTbtPCTsHWgJwxyzVZt6KuxjVZhbZ2h5xYpW6Xs7ZypQNtMxvIlUo5V
eYha/JrTWYhxLpxJhbCLO1qLXxYV+7ursFXe9H/EO8Q1zl3y84FxUccgusMySo7I
g70kAFSJLbZWqaKFg4aGKxZ/MbhzpFkXxBfCH8swpzDaPnq8jjDL4XSCzTMFYJLl
Aps3KXeOxqJifTWltfJUINS9sSlvYULSkVI4anitW7twqmNnrf1XRVc3nN4dNGr3
Dj8ZcbR8xlLN5imw+CMi2/X+6Vq8FdH1a0YCppiYCsT24pHkmLxBbRfKLsw7nRig
jsgi2/VryYOzbKWcZqxNpSBfsfhul0wYDTPvYkWO3QXTIzD5G11s+eo5wdeCOeB2
nH4HD5r+Z1EQwNWvc3ppiF2HBDP2pgiX86tQW78mK1LdQcbquMDU9aI8jWwKokzF
UXrcbQzKtfGUY1tUvC52sdTA6+E+zitnNd5ZxQzV0bb2FAXbUFE7t5rh+uMyHD3R
rd6gfdmZhco5aF2HgS7AJONFa19d5WiNXHmPxtz0f050MhHXYqcXrWQ9QYbjArLL
n0tM7hyEbSpLUo5uhpiP9VZqv7yPnWtQaZMLUa4Jb0MRpprC2jJ7Dk3z/WKu4Ic/
hYLeOR2ankDYWSYiDFGitRZO658CRqM99W5Rd1EWZ8vtd3qJmjsSZ98o8TV8Zh3v
rWC3Zb8+Hu2F4F336Racz6NKy8wZaKe/fPGMjirTD5JHCVLbXX/MN3Whtw++zKYN
4RYfDpmx6p7LnqqzuHCgUB/QSYD2OZ9GTK+/JJt47juhjIUqC4+m9pExB7nOwuVn
FTOIgrOabl3udF6+EKVpEQ/s1Ij7SGHvjvpOrRAjPamNzSsbZ1w8W2KIR1WGb2Ct
S83cO9vkDHu92ZdaKMkidDg+wwaocqzzEzojBo9rgbsIbUSkMUuzBp6B9mY6Sptn
bBuUMyU15jxqK1w0aCbi1MtvY8xNuUAtpV1QOMoK7/7PLsZN54s31BOQxW/m+O81
1B5UjIUsKP4R71bu8VxYnOp6+MO+sWF3iUpZnYWk7dm01p9pnenVtb2DN2RJDaVy
T8kdaqIXGtyhdNODJoJFnK4FSkchv7q0RUYsgnrAwdkWKTa2F8D3RzCsWcvYqQZB
WN1CCCH8FTIXDRgb2Zw9pEoIAcrdVEYgDij+TVFNentcS8H4LgNbwan8pt0at6MC
-----END RSA PRIVATE KEY-----
```

Y ahora creo el certificado intermedio desde el directorio de la CA principal:

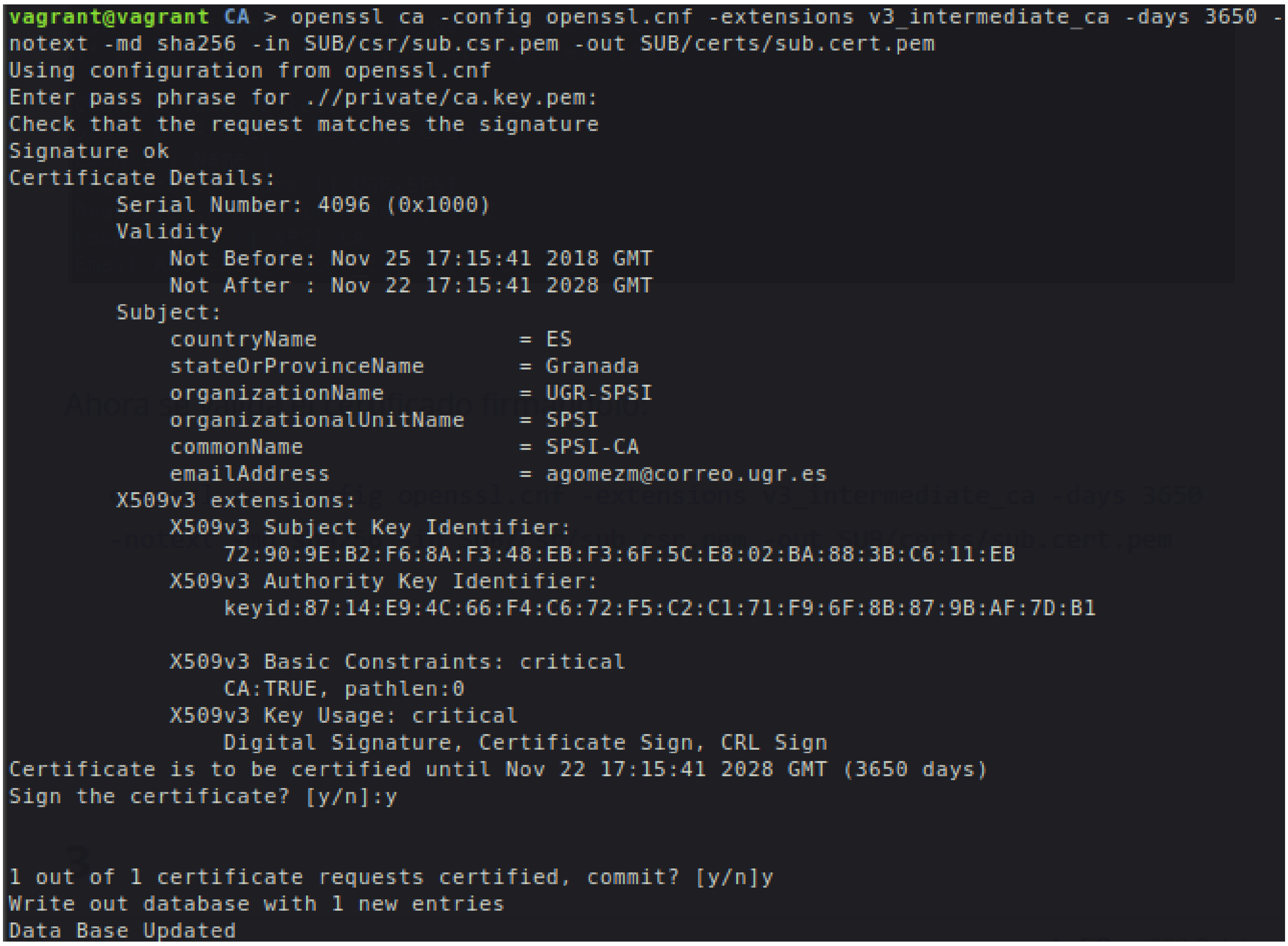
```
openssl req -config SUB/openssl.cnf -new -sha256 -key SUB/private/sub.key.pem -out
SUB/csr/sub.csr.pem
```



```
vagrant@vagrant CA > openssl req -config SUB/openssl.cnf -new -sha256 -key SUB/private/
sub.key.pem -out SUB/csr/sub.csr.pem
Enter pass phrase for SUB/private/sub.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.
-----
Country Name (2 letter code) []:ES
State or Province Name []:Granada
Locality Name []:
Organization Name []:UGR-SPSI
Organizational Unit Name []:SPSI
Common Name []:SPSI-CA
Email Address []:agomezm@correo.ugr.es
```

Ahora se valida el certificado firmándolo:

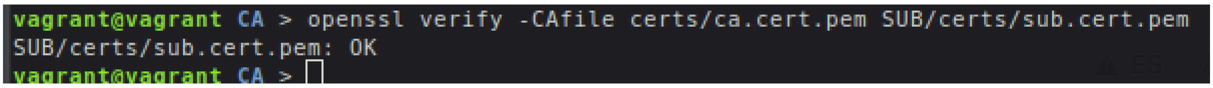
```
openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days 3650 -notext -md sha256 -in
SUB/csr/sub.csr.pem -out SUB/certs/sub.cert.pem
```



```
vagrant@vagrant CA > openssl ca -config openssl.cnf -extensions v3_intermediate_ca -days 3650 -
notext -md sha256 -in SUB/csr/sub.csr.pem -out SUB/certs/sub.cert.pem
Using configuration from openssl.cnf
Enter pass phrase for .//private/ca.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Nov 25 17:15:41 2018 GMT
            Not After : Nov 22 17:15:41 2028 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = Granada
            organizationName          = UGR-SPSI
            organizationalUnitName    = SPSI
            commonName                = SPSI-CA
            emailAddress              = agomezm@correo.ugr.es
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                72:90:9E:B2:F6:8A:F3:48:EB:F3:6F:5C:E8:02:BA:88:3B:C6:11:EB
            X509v3 Authority Key Identifier:
                keyid:87:14:E9:4C:66:F4:C6:72:F5:C2:C1:71:F9:6F:8B:87:9B:AF:7D:B1

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Nov 22 17:15:41 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
```

Compruebo la entidad subordinada:

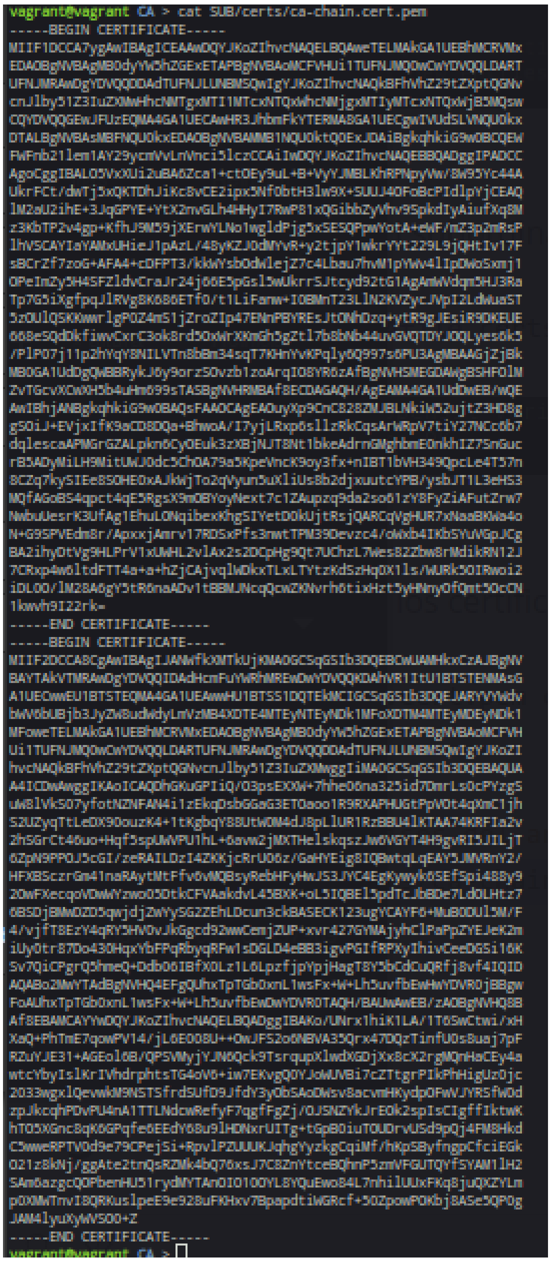
```
openssl verify -CAfile certs/ca.cert.pem SUB/certs/sub.cert.pem
```



```
vagrant@vagrant CA > openssl verify -CAfile certs/ca.cert.pem SUB/certs/sub.cert.pem
SUB/certs/sub.cert.pem: OK
vagrant@vagrant CA > 
```

Por último concateno los certificados:

```
cat SUB/certs/sub.cert.pem certs/ca.cert.pem > SUB/certs/ca-chain.cert.pem

# Cambio los permisos del archivo creado
chmod 444 SUB/certs/ca-chain.cert.pem
```



```
vagrant@vagrant CA > cat SUB/certs/ca-chain.cert.pem
-----BEGIN CERTIFICATE-----
MIIF1DCCA7ygAwIBAgICEAAwDQYJKoZIhvcNAQELBQAweTELMAkGA1UEBhMCRVMx
EDAOBgNVBAgMB0dyYW5hZGExETAPBgNVBAoMCFVHUi1TUFNJMQ0wCwYDVQQLDART
UFNJMRAwDgYDVQQDDAdTUFNJLUNBMSQwIgYJKoZIhvcNAQkBFhVhZ29tZXptQGNv
cnJlby51Z3IuZXMwHhcNMTgxMTI1MTcxNTQxWhcNMjgxMTIyMTcxNTQxWjB3MQsw
CQYDVQQGEwJFUzEQMA4GA1UECAwHR3JhbmFkYTERMA8GA1UECgwIVUdSLVNQU0kx
DTALBgNVBAsMBFNQU0kxEDAOBgNVBAMMB1NQU0ktQ0ExJDAiBgkqhkiG9w0BCQEW
FWFnb21lem1AY29ycmVvLnVnci5lczCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCC
AgoCggIBALO5VxXUi2uBA6Zca1+ctOEy9uL+B+VyYJNBLKhRPNpyVw/8W95Yc44A
UkrFCt/dWTj5xQKTDhJiKc8vCE2ipx5NfObtH3lw9X+SUUJ4OFoBcPIdlpYjCEAQ
lN2aU2ihE+3JqGPYE+YtX2nvGLh4HHyI7RwP81xQGibbZyVhv9SpkdIyAiufXq8N
z3KbTP2v4gp+KfhJ9N59jXErwYLNo1wgldPjg5xSESQPpwYotA+eWF/mZ3p2mRsP
lhVSCAYIaYANxUHieJ1pAzL/48yKZJOdNYvR+y2tjpY1wkrYYt229L9jQHtIv17F
sBCrZf7zoG+AFA4+cDFPT3/kkWYsbOdMlejZ7c4Lbau7hvN1pYWv4lIpDWoSxmj1
OPeImZy5H4SFZldvCraJr24j06E5pGsl5wUkrrSJtcyd92tG1AgAmWdqm5HJ3Ra
Tp7G5iXgfpqJlRVgBK686ETf0/t1LiFanw+I0BMnT23LlN2KVZycJVpI2LdWuaST
5zOUlQSKXwwrlgPOZ4mS1jZroZIp47ENnPBYREsJtONhDzq+ytR9gJEsiR9DKEUE
068eSQdDkfiwvCxrC3ok8rd5OxWrXXmGh5gZtl7b8bNb44uvGVQTDYJOQLyes6k5
/PlPO7j11p2hYqY8NILVTn8bBm34sqT7KHnYvKPqly6Q997s6PU3AgMBAAGjZjBk
MB0GA1UdDgQWBBRykJ6y9orzSOvzb1zoArqIO8YR6zAfBgNVHSMEGDAWgBSHFOlN
ZvTGcvXCwXH5b4uHm099sTASBgNVHRMBAf8ECDAGAQH/AgEAMA4GA1UdDwEB/wQE
AwIBhjANBgkqhkiG9w0BAQsFAAOCAgEAOuyXp9CnC828ZNJBLNkiW52ujtZ3HD8g
g5OiJ+EVjxIfK9aCD8DQa+BhwoA/I7yjLRxp6sllzRkCqsArWRpV7tiY27NCc6b7
dqlescaAPNGrGZALpkn6CyOEuk3zXBjNJT8Nt1bkeAdrnGNghbmE0nkhIZ7SnGuc
rB5ADyNiLH9NitUWJ0dc5ChOA79a5KpeVncK9oy3fx+nIBT1bVH349QpcLe4T57n
8CZq7kySIEe85OHEOxAJkWjTo2qVyun5uXliUs8b2djxuutcYPB/ysbJT1L3eHS3
MQfAGoBS4qpct4qE5RgsX9mOBYoyNext7c1ZAupzq9da2so61zY8FyZiAFutZrw7
NwbuUesrK3UfAg1EhuLONqibexKhgSIYetD0kUjtRsjQARCqVgHUR7xNaaBKWa4o
N+G95PVEdm8r/ApxxjAmrv17RDSxPfs3nwtTPN39Devzc4/oWxb4IKb5YuVGpJCg
BA2ihyDtVg9HLPrV1xUWHL2vlAx2s2DCpHg9Qt7UChzL7Wes82Zbw8rNdikRN12J
7CRxp4w6ltdFTT4a+a+hZjCAjvqlWDkxTLxLTYtzKdSzHq0X1ls/WURk5OIRwoi2
iDLOO/lN28A6gY5tR6naADv1tBBNJNcqQcwZKNvrh6tixHzt5yHNnyOfQmt5OcCN
1kwvh9I22rk=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIF2DCCA8CgAwIBAgIJANWfkXNTkUjKMA0GCSqGSIb3DQEBCwUAMHkxCzAJBgNV
BAYTAkVTMRAwDgYDVQQIDAdHcmFuYWRhMREwDwYDVQQKDAhVR1ItU1BTSTENMAsG
A1UECwwEU1BTSTEQMA4GA1UEAwwHU1BTSS1DQTEkMCIGCSqGSIb3DQEJARYVYWdv
bWV6bUBjb3JyZW8udWdyLmVzMB4XDTE4MTEyNTEyNDk1MFoXDTM4MTEyMDEyNDk1
MFoweTELMAkGA1UEBhMCRVMxEDAOBgNVBAgMB0dyYW5hZGExETAPBgNVBAoMCFVH
Ui1TUFNJMQ0wCwYDVQQLDARTUFNJMRAwDgYDVQQDDAdTUFNJLUNBMSQwIgYJKoZI
hvcNAQkBFhVhZ29tZXptQGNvcnJlby51Z3IuZXMwggIiMA0GCSqGSIb3DQEBAQUA
A4ICDwAwggIKAoICAQDhGKuGPIiQ/O3psEXXW+7hhe06na325id7DmrLs0cPYzg5
uW8lVkS07yfotN2NFAN4i1zEkqDsbGGaG3ETOaoo1R9RXAPHUGtPpVOt4qXmC1jh
S2UZyqTtLeDX90ouzK4+1tKgbqY88UtWOM4dJ8pLlUR1RzBBU4lKTAA74KRFIa2v
2hSGrCt46uo+Hqf5spUWVPU1hL+6avw2jMXTHelskqszJw6VGYT4H9gvRI5JILjT
6ZpN9PPOJ5cGI/zeRAILDzI4ZKKjcRrU06z/GaHYEig8IQBwtqLqEAY5JMVRnY2/
HFXBSczrGm41naRAytNtFfv6vWQBsyRebHFyHwJS3JYC4EgKywyk6SEfSpi488y9
2OwFXecqoVDwWYzwo05DtkCFVAakdvL45BXK+oL5IQBEl5pdTcJbBDe7LdOLHtz7
6BSDjBMwOZD5qwjdjZWYySG2ZEhLDcun3ckBASECK123ugYCAYF6+MuBODUl5W/F
4/vjfT8EzY4qRY5HV0vJkGgcd92wwCemjZUP+xvr427GYNAjyhClPaPpZYEJeK2m
iUy0tr87Do430HqxYbFPqRbyqRFw1sDGLD4eBB3igvPGIfRPXyIhivCeeDGSi16K
Sv7QiCPgrQ5hmeQ+Ddb06IBfX0Lz1L6LpzfjpYpjHagT8Y5bCdCuQRfj8vf4IQID
AQABo2MwYTAdBgNVHQ4EFgQUhxTpTGb0xnL1wsFx+W+Lh5uvfbEwHwYDVR0jBBgw
FoAUhxTpTGb0xnL1wsFx+W+Lh5uvfbEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8B
Af8EBAMCAYYwDQYJKoZIhvcNAQELBQADggIBAKo/UNrx1hiK1LA/1T6SwCtwi/xH
XaQ+PhTmE7qowPV14/jL6EO08U++OwJFS2o6NBVA35Qrx47DQzTinfU0s8uaj7pF
RZuYJE31+AGEol6B/QPSVWyjYJN0Qck9TsrqupXlwdXGDjXx8cX2rgMQnHaCEy4a
wtcYbyIslKrIVhdrphtsTG4oV6+iw7EKvgQ0YJoWUVBi7cZTtgrPIkPhHigUz0jc
2O33wgxlQevwkN9N5TSfrdSUfD9JfdY3yObSAoDWsv8acvmHKydpOFwVJYR5fWOd
zpJkcqhPDvPU4nA1TTLNdcwRefyF7qgfFgZj/OJ5NZYkJrEOk2spIsCIgffIktwK
hTO5XGnc8qX6GPqfe6EEdY68u9lHDNxrUITg+tGpB0iuTOUDrvUSd9pQj4FN8Hkd
C5wweRPTVOd9e79CPejSi+RpvlPZUUUKJqhgYyzkgCqiNf/hKpSByfngpCfciEGk
O21z8kNj/ggAte2tnQsRZWk4bQ76xsJ7C8ZnYtceBQhnP5zmVFGUTQYfSYAN1lH2
SAm6azgcQOPbenHU51rydNYTAnOIO1OOYL8YQuEwo84L7nhilUUxFKq8juQXZYLm
pOXWWTnvI8QRKuslpeE9e928uFKHxv7BpapdtiWGRcf+5OZpowPOKbj8ASe5QPOg
JAN4lyuXyWVSOO+Z
-----END CERTIFICATE-----
vagrant@vagrant CA > 
```

Tras estos pasos ya quedaría creada la CA subordinada.

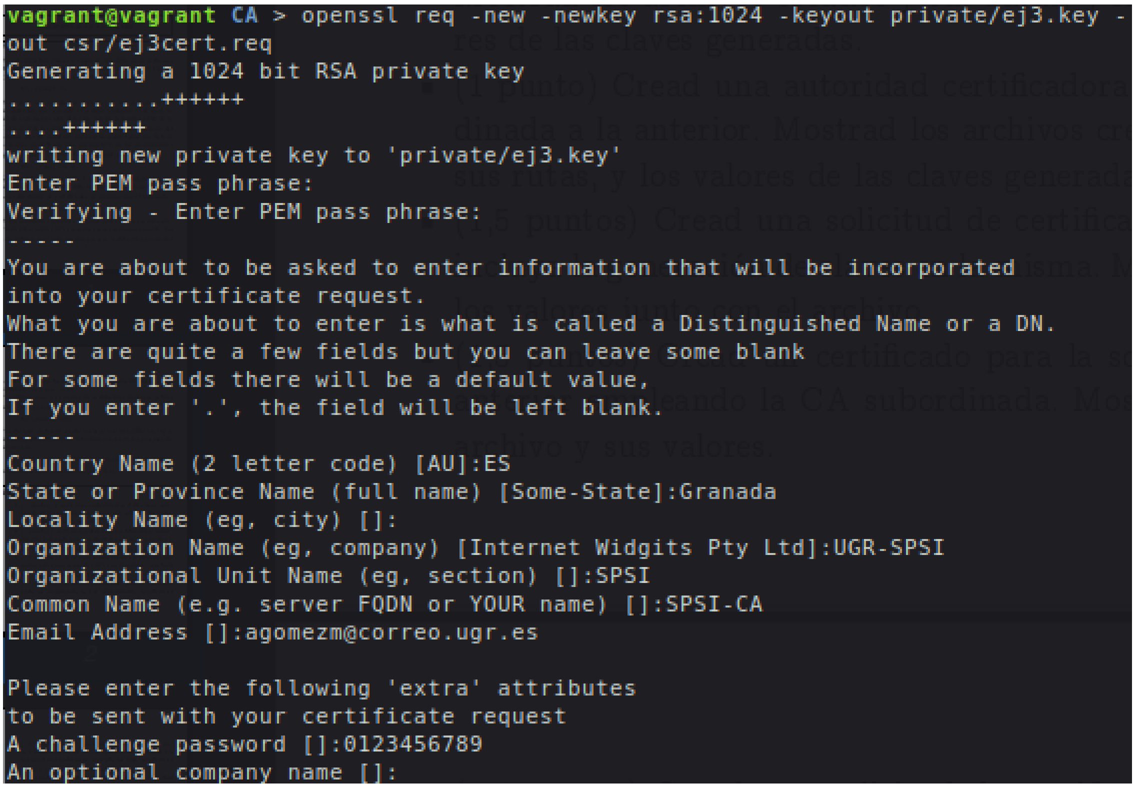
3

> Como contraseña de cifrado de la clave que se genera he usado: 0123456789

El comando para crear la solicitud generando también claves es el siguiente:

```
openssl req -new -newkey rsa:1024 -keyout private/ej3.key -out csr/ej3cert.req
```

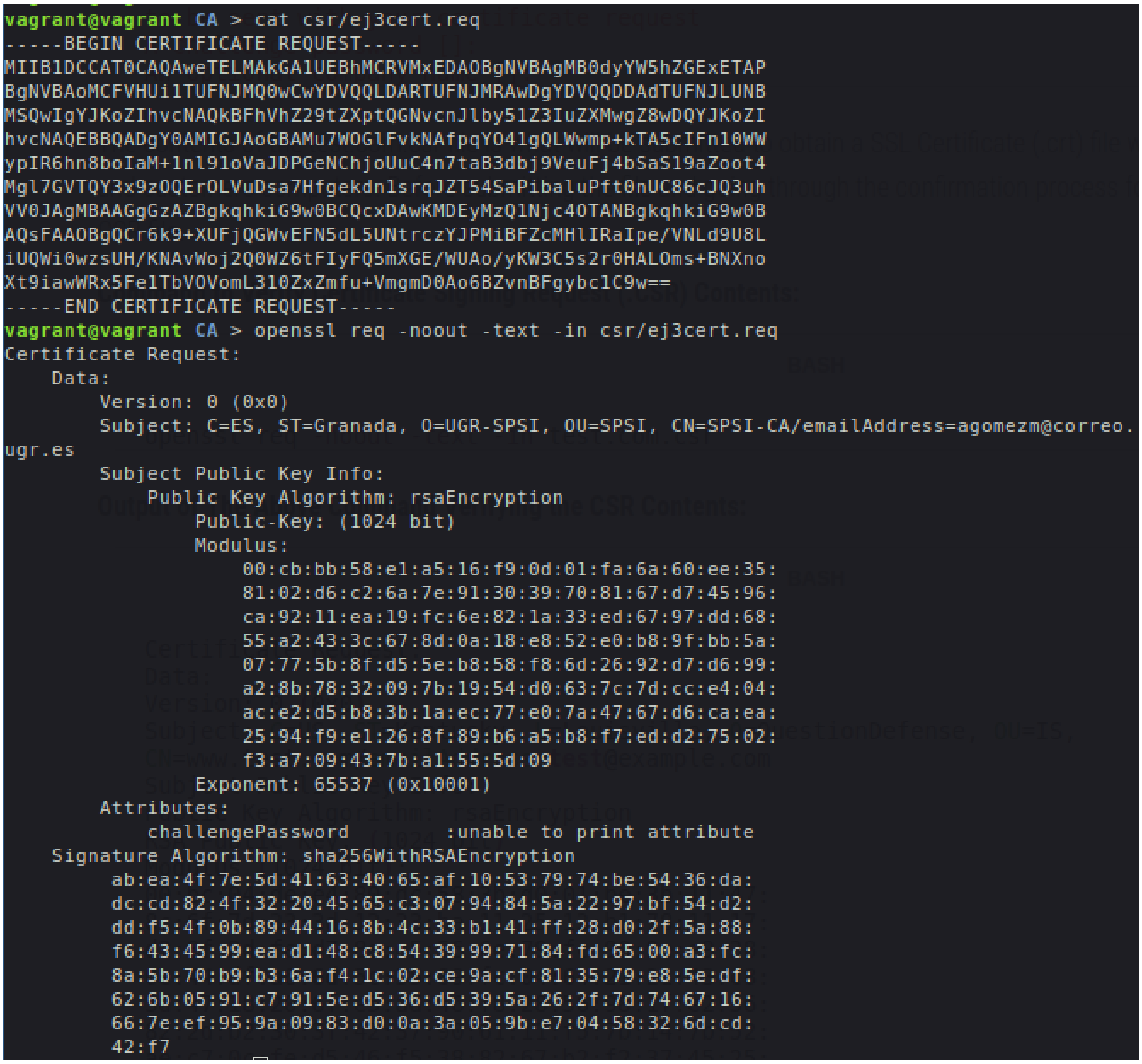
- *-new*: Crear nueva solicitud.
- *-newkey rsa:1024*: Tipo de clave.
- *-keyout private/ej3.key*: Archivo de salida que contendrá la clave.
- *-out csr/ej3cert.req*: Archivo de salida que contendrá la solicitud.



```
vagrant@vagrant CA > openssl req -new -newkey rsa:1024 -keyout private/ej3.key -
out csr/ej3cert.req
Generating a 1024 bit RSA private key
...........++++++
....++++++
writing new private key to 'private/ej3.key'
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]:Granada
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UGR-SPSI
Organizational Unit Name (eg, section) []:SPSI
Common Name (e.g. server FQDN or YOUR name) []:SPSI-CA
Email Address []:agomezm@correo.ugr.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:0123456789
An optional company name []:
```

Por otro lado para ver el contenido de la solicitud utilizo el comando:

```
openssl req -noout -text -in csr/ej3cert.req
```



```
vagrant@vagrant CA > cat csr/ej3cert.req
-----BEGIN CERTIFICATE REQUEST-----
MIIB1DCCAT0CAQAweTELMAkGA1UEBhMCRVMxEDAOBgNVBAgMB0dyYW5hZGExETAP
BgNVBAoMCFVHUi1TUFNJMQ0wCwYDVQQLDARTUFNJMRAwDgYDVQQDDAdTUFNJLUNB
MSQwIgYJKoZIhvcNAQkBFhVhZ29tZXptQGNvcnJlby51Z3IuZXMwgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMIGJAoGBAMu7WOGlFvkNAfpqYO41gQLWwmp+kTA5cIFn10WW
ypIR6hn8boIaM+1nl91oVaJDPGeNChjoUuC4n7taB3dbj9VeuFj4bSaS19aZoot4
Mgl7GVTQY3x9zOQErOLVuDsa7HfgekdnlsrqJZT54SaPibaluPft0nUC86cJQ3uh
VV0JAgMBAAGgGzAZBgkqhkiG9w0BCQcxDAwKMDEyMzQ1Njc4OTANBgkqhkiG9w0B
AQsFAAOBgQCr6k9+XUFjQGWvEFN5dL5UNtrczYJPMiBFZcMHlIRaIpe/VNLd9U8L
iUQWi0wzsUH/KNAvWoj2Q0WZ6tFIyFQ5mXGE/WUAo/yKW3C5s2r0HALOms+BNXno
Xt9iawWRx5Fe1TbVOVomL310ZxZmfu+VmgmD0Ao6BZvnBFgybc1C9w==
-----END CERTIFICATE REQUEST-----
vagrant@vagrant CA > openssl req -noout -text -in csr/ej3cert.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=ES, ST=Granada, O=UGR-SPSI, OU=SPSI, CN=SPSI-CA/emailAddress=agomezm@correo.
ugr.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:cb:bb:58:e1:a5:16:f9:0d:01:fa:6a:60:ee:35:
                    81:02:d6:c2:6a:7e:91:30:39:70:81:67:d7:45:96:
                    ca:92:11:ea:19:fc:6e:82:1a:33:ed:67:97:dd:68:
                    55:a2:43:3c:67:8d:0a:18:e8:52:e0:b8:9f:bb:5a:
                    07:77:5b:8f:d5:5e:b8:58:f8:6d:26:92:d7:d6:99:
                    a2:8b:78:32:09:7b:19:54:d0:63:7c:7d:cc:e4:04:
                    ac:e2:d5:b8:3b:1a:ec:77:e0:7a:47:67:d6:ca:ea:
                    25:94:f9:e1:26:8f:89:b6:a5:b8:f7:ed:d2:75:02:
                    f3:a7:09:43:7b:a1:55:5d:09
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :unable to print attribute
    Signature Algorithm: sha256WithRSAEncryption
         ab:ea:4f:7e:5d:41:63:40:65:af:10:53:79:74:be:54:36:da:
         dc:cd:82:4f:32:20:45:65:c3:07:94:84:5a:22:97:bf:54:d2:
         dd:f5:4f:0b:89:44:16:8b:4c:33:b1:41:ff:28:d0:2f:5a:88:
         f6:43:45:99:ea:d1:48:c8:54:39:99:71:84:fd:65:00:a3:fc:
         8a:5b:70:b9:b3:6a:f4:1c:02:ce:9a:cf:81:35:79:e8:5e:df:
         62:6b:05:91:c7:91:5e:d5:36:d5:39:5a:26:2f:7d:74:67:16:
         66:7e:ef:95:9a:09:83:d0:0a:3a:05:9b:e7:04:58:32:6d:cd:
         42:f7
```

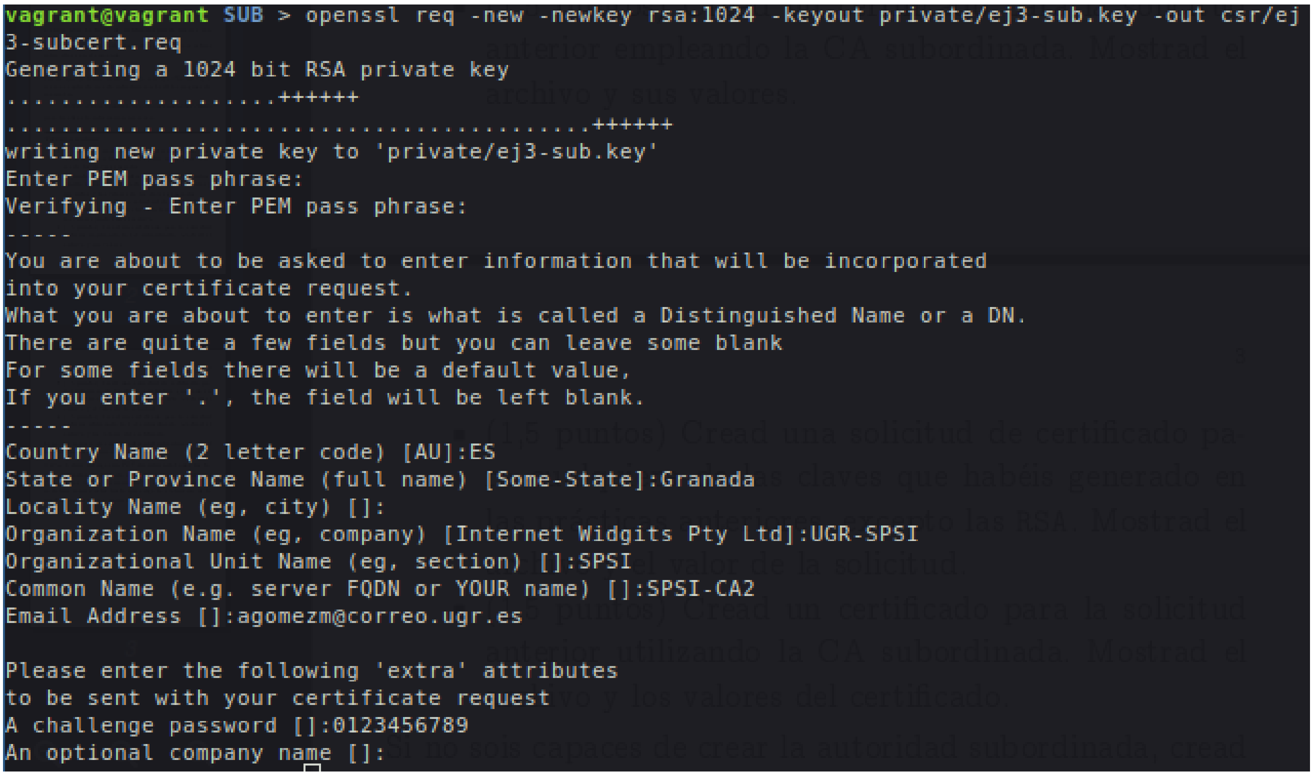
4

> Como contraseña de cifrado de la clave que se genera he usado: 0123456789

Para crear una solicitud en la entidad subordinada sigo los mismos paso que en el ejercicio anterior, pero en este caso dentro del directorio donde se encuentra dicha entidad.

En primer lugar creo la solicitud:

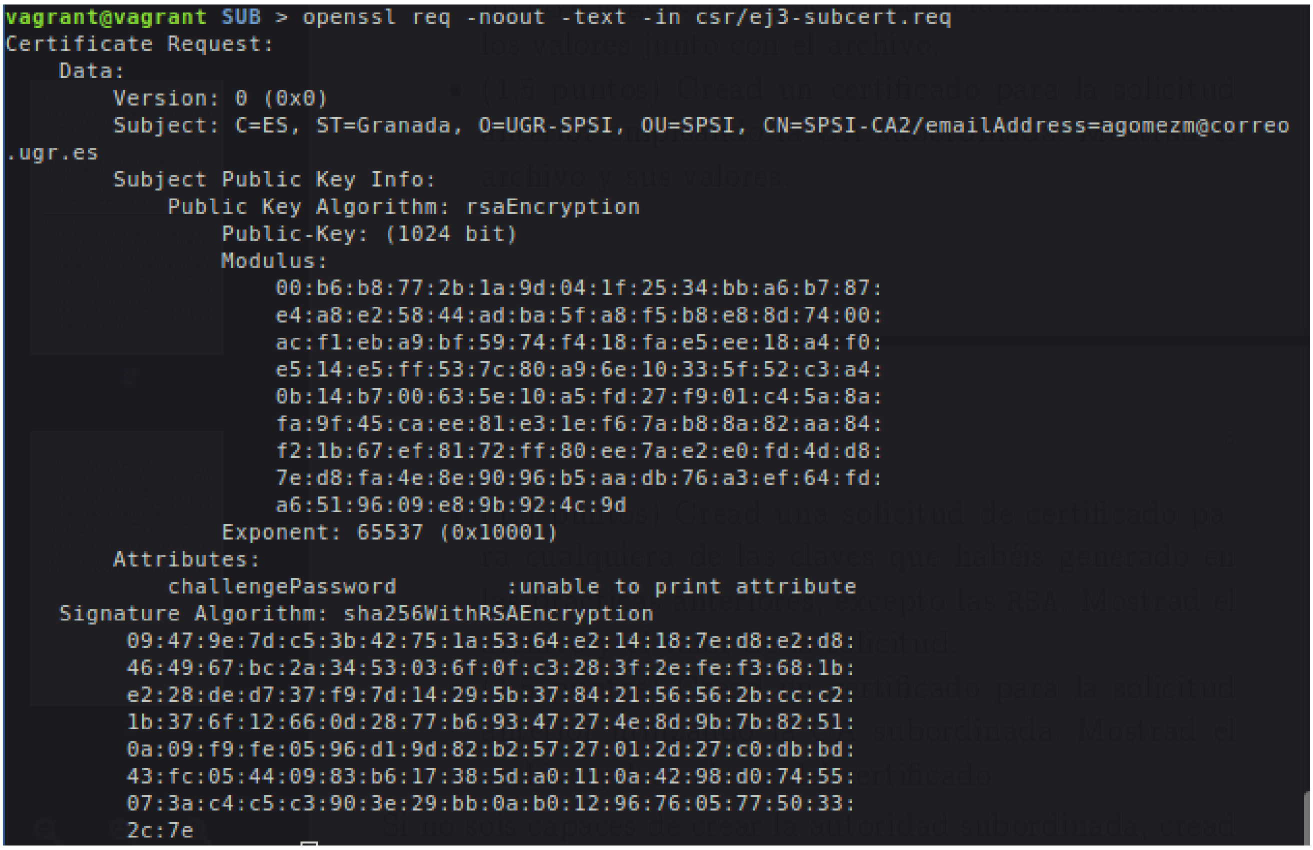
```
openssl req -new -newkey rsa:1024 -keyout private/ej3-sub.key -out csr/ej3-subcert.req
```



```
vagrant@vagrant SUB > openssl req -new -newkey rsa:1024 -keyout private/ej3-sub.key -out csr/ej
3-subcert.req
Generating a 1024 bit RSA private key
...................++++++
............................................++++++
writing new private key to 'private/ej3-sub.key'
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]:Granada
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UGR-SPSI
Organizational Unit Name (eg, section) []:SPSI
Common Name (e.g. server FQDN or YOUR name) []:SPSI-CA2
Email Address []:agomezm@correo.ugr.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:0123456789
An optional company name []:
```

Y tras esto compruebo sus valores:

```
openssl req -noout -text -in csr/ej3-subcert.req
```

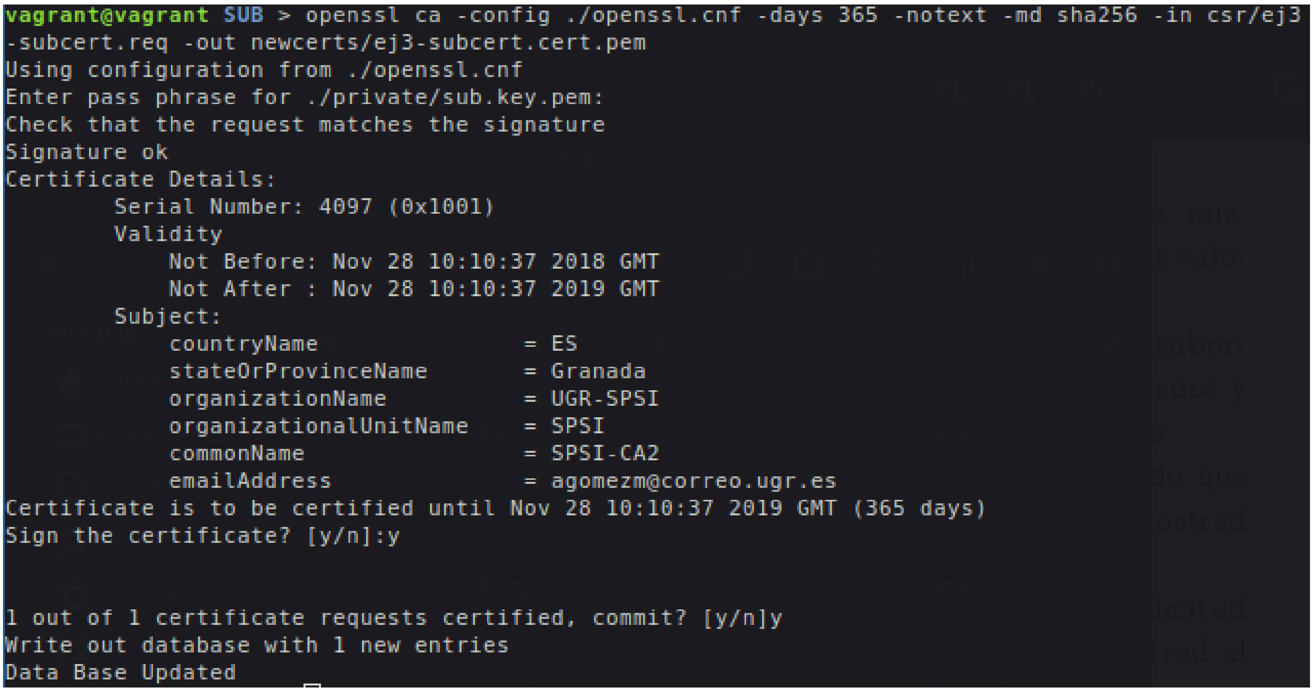


```
vagrant@vagrant SUB > openssl req -noout -text -in csr/ej3-subcert.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=ES, ST=Granada, O=UGR-SPSI, OU=SPSI, CN=SPSI-CA2/emailAddress=agomezm@correo
.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b6:b8:77:2b:1a:9d:04:1f:25:34:bb:a6:b7:87:
                    e4:a8:e2:58:44:ad:ba:5f:a8:f5:b8:e8:8d:74:00:
                    ac:f1:eb:a9:bf:59:74:f4:18:fa:e5:ee:18:a4:f0:
                    e5:14:e5:ff:53:7c:80:a9:6e:10:33:5f:52:c3:a4:
                    0b:14:b7:00:63:5e:10:a5:fd:27:f9:01:c4:5a:8a:
                    fa:9f:45:ca:ee:81:e3:1e:f6:7a:b8:8a:82:aa:84:
                    f2:1b:67:ef:81:72:ff:80:ee:7a:e2:e0:fd:4d:d8:
                    7e:d8:fa:4e:8e:90:96:b5:aa:db:76:a3:ef:64:fd:
                    a6:51:96:09:e8:9b:92:4c:9d
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :unable to print attribute
    Signature Algorithm: sha256WithRSAEncryption
         09:47:9e:7d:c5:3b:42:75:1a:53:64:e2:14:18:7e:d8:e2:d8:
         46:49:67:bc:2a:34:53:03:6f:0f:c3:28:3f:2e:fe:f3:68:1b:
         e2:28:de:d7:37:f9:7d:14:29:5b:37:84:21:56:56:2b:cc:c2:
         1b:37:6f:12:66:0d:28:77:b6:93:47:27:4e:8d:9b:7b:82:51:
         0a:09:f9:fe:05:96:d1:9d:82:b2:57:27:01:2d:27:c0:db:bd:
         43:fc:05:44:09:83:b6:17:38:5d:a0:11:0a:42:98:d0:74:55:
         07:3a:c4:c5:c3:90:3e:29:bb:0a:b0:12:96:76:05:77:50:33:
         2c:7e
```

Ahora genero el certificado, para ello firmo la solicitud que acabo de crear:

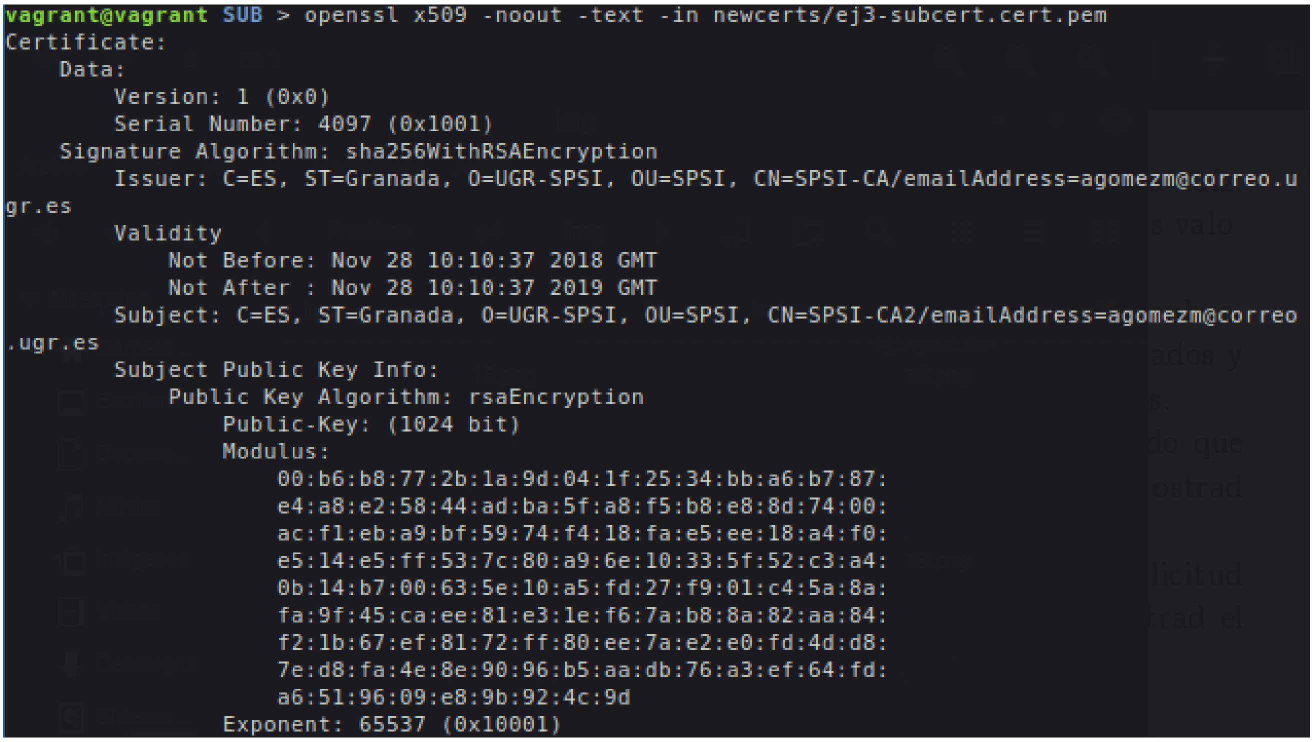
```
openssl ca -config ./openssl.cnf -days 365 -notext -md sha256 -in csr/ej3-subcert.req -out
newcerts/ej3-subcert.cert.pem
```

- -config ./openssl.cnf*: Archivo de configuración a usar.
- *-days 356*: Días para los que es válido el certificado.
- *-md sha256*: Tipo de Message Digest.
- *-in csr/angelcert.req*: Archivo de entrada con la solicitud de certificado.
- *-out newcerts/angelsub.cert.pem*: Archivo de salida con el certificado firmado.

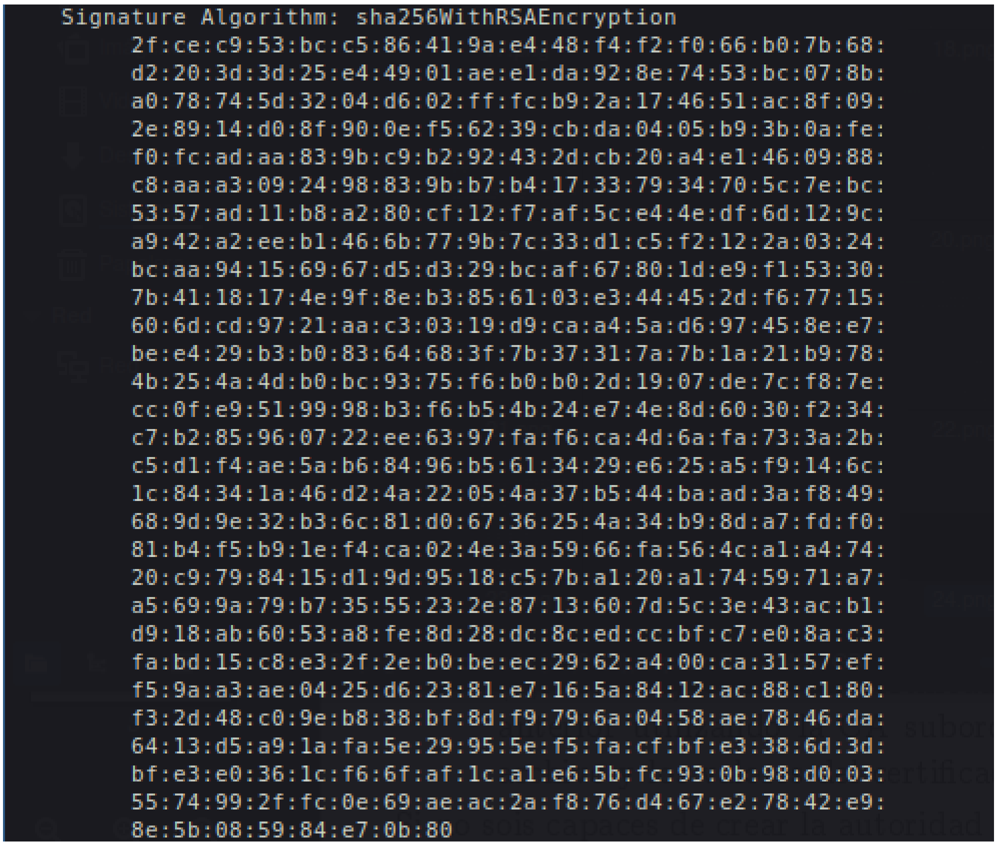


```
vagrant@vagrant SUB > openssl ca -config ./openssl.cnf -days 365 -notext -md sha256 -in csr/ej3
-subcert.req -out newcerts/ej3-subcert.cert.pem
Using configuration from ./openssl.cnf
Enter pass phrase for ./private/sub.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Nov 28 10:10:37 2018 GMT
            Not After : Nov 28 10:10:37 2019 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = Granada
            organizationName          = UGR-SPSI
            organizationalUnitName    = SPSI
            commonName                = SPSI-CA2
            emailAddress              = agomezm@correo.ugr.es
Certificate is to be certified until Nov 28 10:10:37 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
```

Y compruebo sus valores:



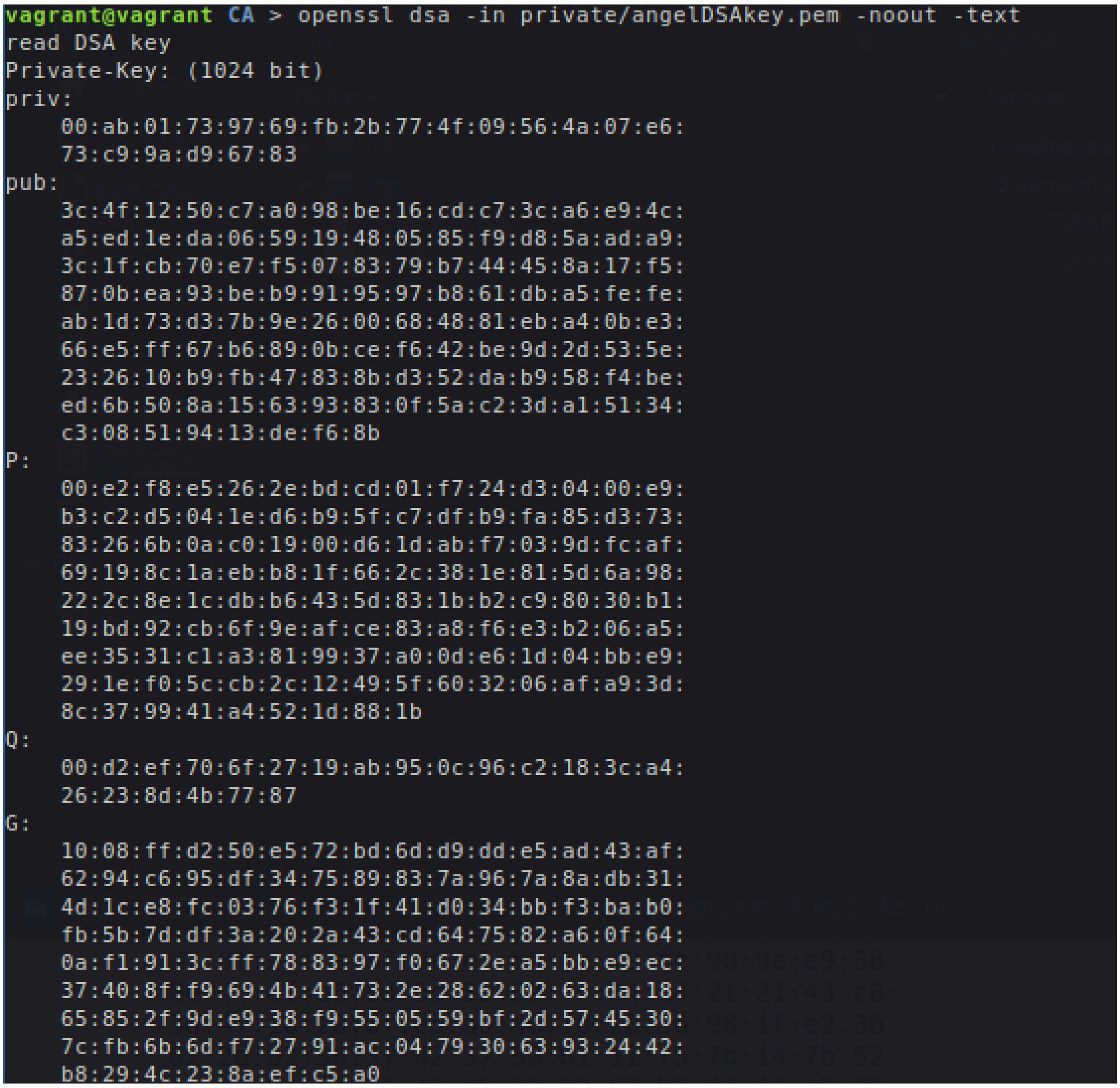
```
vagrant@vagrant SUB > openssl x509 -noout -text -in newcerts/ej3-subcert.cert.pem
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 4097 (0x1001)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, ST=Granada, O=UGR-SPSI, OU=SPSI, CN=SPSI-CA/emailAddress=agomezm@correo.u
gr.es
        Validity
            Not Before: Nov 28 10:10:37 2018 GMT
            Not After : Nov 28 10:10:37 2019 GMT
        Subject: C=ES, ST=Granada, O=UGR-SPSI, OU=SPSI, CN=SPSI-CA2/emailAddress=agomezm@correo
.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b6:b8:77:2b:1a:9d:04:1f:25:34:bb:a6:b7:87:
                    e4:a8:e2:58:44:ad:ba:5f:a8:f5:b8:e8:8d:74:00:
                    ac:f1:eb:a9:bf:59:74:f4:18:fa:e5:ee:18:a4:f0:
                    e5:14:e5:ff:53:7c:80:a9:6e:10:33:5f:52:c3:a4:
                    0b:14:b7:00:63:5e:10:a5:fd:27:f9:01:c4:5a:8a:
                    fa:9f:45:ca:ee:81:e3:1e:f6:7a:b8:8a:82:aa:84:
                    f2:1b:67:ef:81:72:ff:80:ee:7a:e2:e0:fd:4d:d8:
                    7e:d8:fa:4e:8e:90:96:b5:aa:db:76:a3:ef:64:fd:
                    a6:51:96:09:e8:9b:92:4c:9d
                Exponent: 65537 (0x10001)
```



```
    Signature Algorithm: sha256WithRSAEncryption
         2f:ce:c9:53:bc:c5:86:41:9a:e4:48:f4:f2:f0:66:b0:7b:68:
         d2:20:3d:3d:25:e4:49:01:ae:e1:da:92:8e:74:53:bc:07:8b:
         a0:78:74:5d:32:04:d6:02:ff:fc:b9:2a:17:46:51:ac:8f:09:
         2e:89:14:d0:8f:90:0e:f5:62:39:cb:da:04:05:b9:3b:0a:fe:
         f0:fc:ad:aa:83:9b:c9:b2:92:43:2d:cb:20:a4:e1:46:09:88:
         c8:aa:a3:09:24:98:83:9b:b7:b4:17:33:79:34:70:5c:7e:bc:
         53:57:ad:11:b8:a2:80:cf:12:f7:af:5c:e4:4e:df:6d:12:9c:
         a9:42:a2:ee:b1:46:6b:77:9b:7c:33:d1:c5:f2:12:2a:03:24:
         bc:aa:94:15:69:67:d5:d3:29:bc:af:67:80:1d:e9:f1:53:30:
         7b:41:18:17:4e:9f:8e:b3:85:61:03:e3:44:45:2d:f6:77:15:
         60:6d:cd:97:21:aa:c3:03:19:d9:ca:a4:5a:d6:97:45:8e:e7:
         be:e4:29:b3:b0:83:64:68:3f:7b:37:31:7a:7b:1a:21:b9:78:
         4b:25:4a:4d:b0:bc:93:75:f6:b0:b0:2d:19:07:de:7c:f8:7e:
         cc:0f:e9:51:99:98:b3:f6:b5:4b:24:e7:4e:8d:60:30:f2:34:
         c7:b2:85:96:07:22:ee:63:97:fa:f6:ca:4d:6a:fa:73:3a:2b:
         c5:d1:f4:ae:5a:b6:84:96:b5:61:34:29:e6:25:a5:f9:14:6c:
         1c:84:34:1a:46:d2:4a:22:05:4a:37:b5:44:ba:ad:3a:f8:49:
         68:9d:9e:32:b3:6c:81:d0:67:36:25:4a:34:b9:8d:a7:fd:f0:
         81:b4:f5:b9:1e:f4:ca:02:4e:3a:59:66:fa:56:4c:a1:a4:74:
         20:c9:79:84:15:d1:9d:95:18:c5:7b:a1:20:a1:74:59:71:a7:
         a5:69:9a:79:b7:35:55:23:2e:87:13:60:7d:5c:3e:43:ac:b1:
         d9:18:ab:60:53:a8:fe:8d:28:dc:8c:ed:cc:bf:c7:e0:8a:c3:
         fa:bd:15:c8:e3:2f:2e:b0:be:ec:29:62:a4:00:ca:31:57:ef:
         f5:9a:a3:ae:04:25:d6:23:81:e7:16:5a:84:12:ac:88:c1:80:
         f3:2d:48:c0:9e:b8:38:bf:8d:f9:79:6a:04:58:ae:78:46:da:
         64:13:d5:a9:1a:fa:5e:29:95:5e:f5:fa:cf:bf:e3:38:6d:3d:
         bf:e3:e0:36:1c:f6:6f:af:1c:a1:e6:5b:fc:93:0b:98:d0:03:
         55:74:99:2f:fc:0e:69:ae:ac:2a:f8:76:d4:67:e2:78:42:e9:
         8e:5b:08:59:84:e7:0b:80
```

Para este ejercicio he tomado la clave *angelDSAkey.pem*, generada en la práctica anterior, la cual tiene el siguiente contenido:

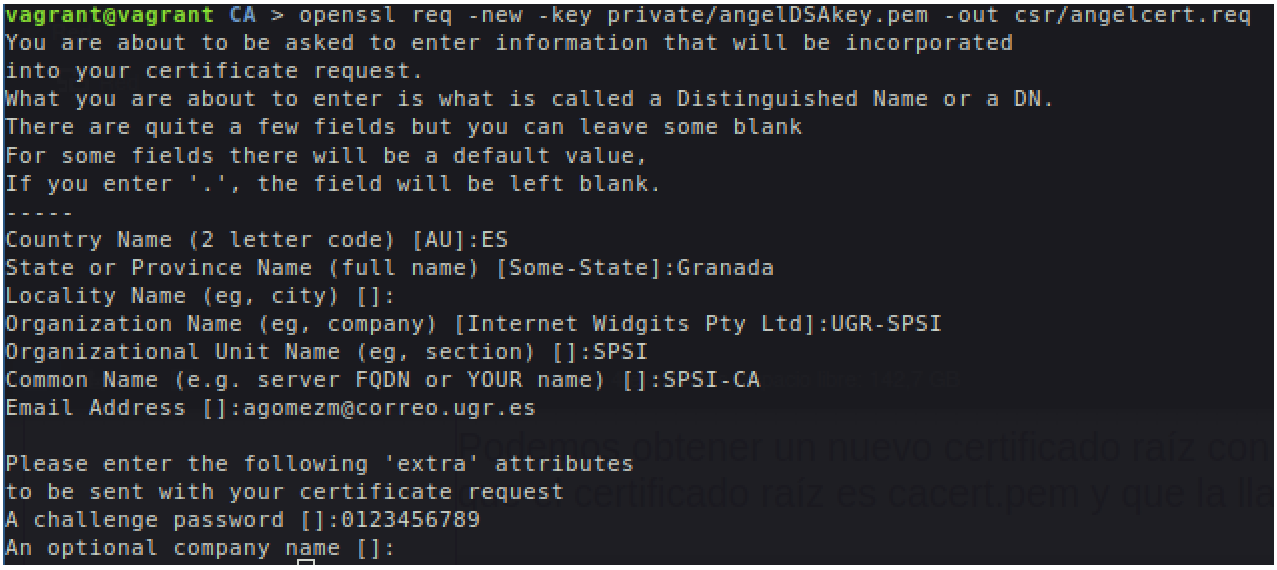
```
openssl dsa -in angelDSAkey.pem -noout -text
```



```
vagrant@vagrant CA > openssl dsa -in private/angelDSAkey.pem -noout -text
read DSA key
Private-Key: (1024 bit)
priv:
    00:ab:01:73:97:69:fb:2b:77:4f:09:56:4a:07:e6:
    73:c9:9a:d9:67:83
pub:
    3c:4f:12:50:c7:a0:98:be:16:cd:c7:3c:a6:e9:4c:
    a5:ed:1e:da:06:59:19:48:05:85:f9:d8:5a:ad:a9:
    3c:1f:cb:70:e7:f5:07:83:79:b7:44:45:8a:17:f5:
    87:0b:ea:93:be:b9:91:95:97:b8:61:db:a5:fe:fe:
    ab:1d:73:d3:7b:9e:26:00:68:48:81:eb:a4:0b:e3:
    66:e5:ff:67:b6:89:0b:ce:f6:42:be:9d:2d:53:5e:
    23:26:10:b9:fb:47:83:8b:d3:52:da:b9:58:f4:be:
    ed:6b:50:8a:15:63:93:83:0f:5a:c2:3d:a1:51:34:
    c3:08:51:94:13:de:f6:8b
P:
    00:e2:f8:e5:26:2e:bd:cd:01:f7:24:d3:04:00:e9:
    b3:c2:d5:04:1e:d6:b9:5f:c7:df:b9:fa:85:d3:73:
    83:26:6b:0a:c0:19:00:d6:1d:ab:f7:03:9d:fc:af:
    69:19:8c:1a:eb:b8:1f:66:2c:38:1e:81:5d:6a:98:
    22:2c:8e:1c:db:b6:43:5d:83:1b:b2:c9:80:30:b1:
    19:bd:92:cb:6f:9e:af:ce:83:a8:f6:e3:b2:06:a5:
    ee:35:31:c1:a3:81:99:37:a0:0d:e6:1d:04:bb:e9:
    29:1e:f0:5c:cb:2c:12:49:5f:60:32:06:af:a9:3d:
    8c:37:99:41:a4:52:1d:88:1b
Q:
    00:d2:ef:70:6f:27:19:ab:95:0c:96:c2:18:3c:a4:
    26:23:8d:4b:77:87
G:
    10:08:ff:d2:50:e5:72:bd:6d:d9:dd:e5:ad:43:af:
    62:94:c6:95:df:34:75:89:83:7a:96:7a:8a:db:31:
    4d:1c:e8:fc:03:76:f3:1f:41:d0:34:bb:f3:ba:b0:
    fb:5b:7d:df:3a:20:2a:43:cd:64:75:82:a6:0f:64:
    0a:f1:91:3c:ff:78:83:97:f0:67:2e:a5:bb:e9:ec:
    37:40:8f:f9:69:4b:41:73:2e:28:62:02:63:da:18:
    65:85:2f:9d:e9:38:f9:55:05:59:bf:2d:57:45:30:
    7c:fb:6b:6d:f7:27:91:ac:04:79:30:63:93:24:42:
    b8:29:4c:23:8a:ef:c5:a0
```

En este caso, como ya tenemos la clave, modifico el comando usado en los ejercicios anteriores para que no genere una clave y en su lugar utilice una existente:

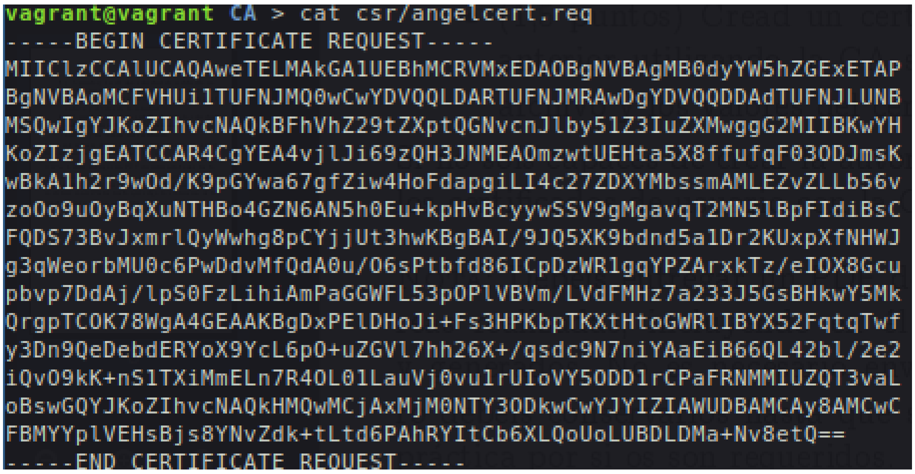
```
openssl req -new -key private/angelDSAkey.pem -out csr/angelcert.req
```



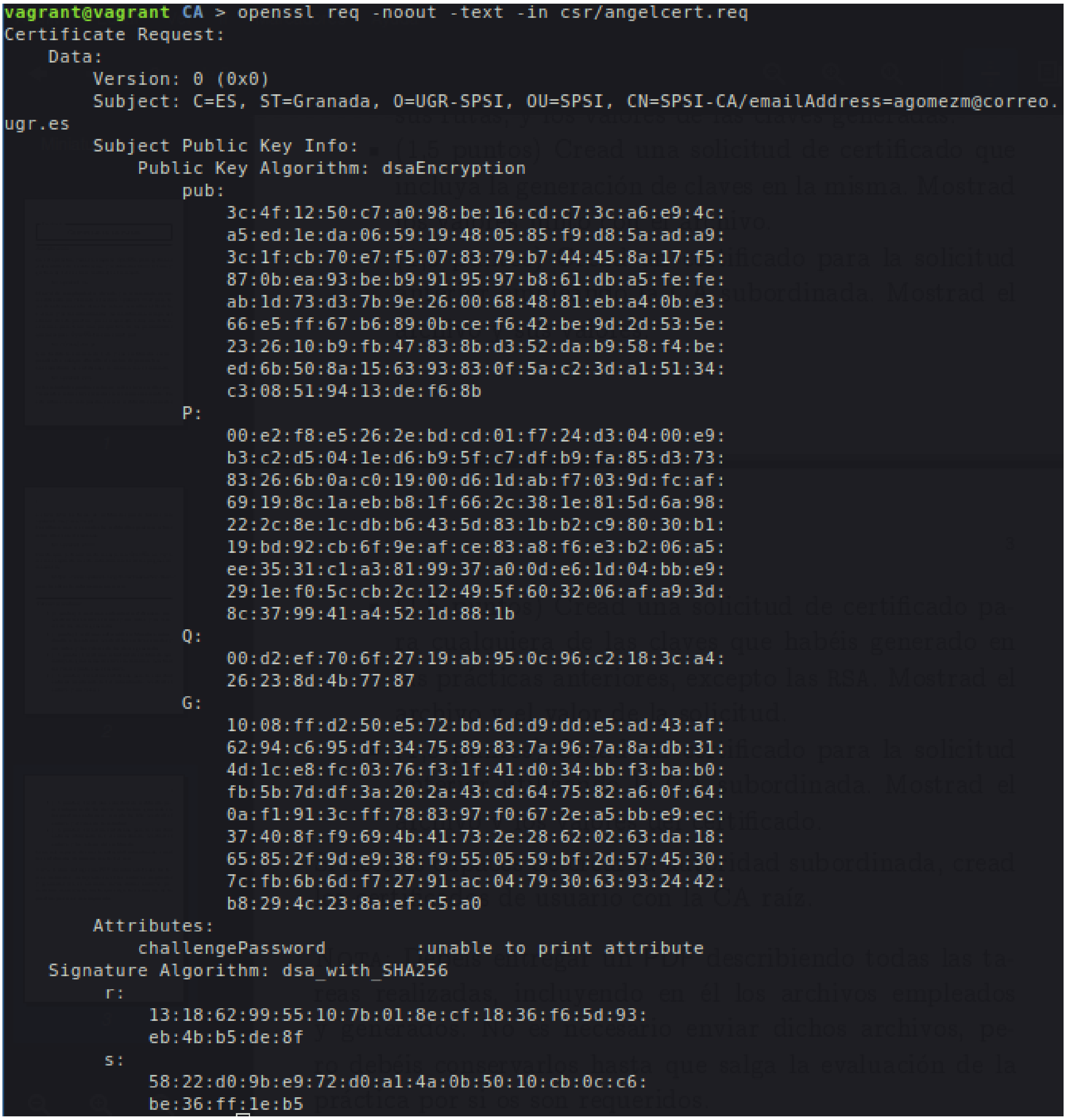
```
vagrant@vagrant CA > openssl req -new -key private/angelDSAkey.pem -out csr/angelcert.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields 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]:Granada
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UGR-SPSI
Organizational Unit Name (eg, section) []:SPSI
Common Name (e.g. server FQDN or YOUR name) []:SPSI-CA
Email Address []:agomezm@correo.ugr.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:0123456789
An optional company name []:
```

Y muestro sus valores:

```
openssl req -noout -text -in csr/angelcert.req
```



```
vagrant@vagrant CA > cat csr/angelcert.req
-----BEGIN CERTIFICATE REQUEST-----
MIIClzCCAlUCAQAweTELMAkGA1UEBhMCRVMxEDAOBgNVBAgMB0dyYW5hZGExETAP
BgNVBAoMCFVHUi1TUFNJMQ0wCwYDVQQLDARTUFNJMRAwDgYDVQQDDAdTUFNJLUNB
MSQwIgYJKoZIhvcNAQkBFhVhZ29tZXptQGNvcnJlby51Z3IuZXMwggG2MIIBKwYH
KoZIzjgEATCCAR4CgYEA4vjlJi69zQH3JNMEAOmzwtUEHta5X8ffufqF030DJmsK
wBkA1h2r9w0d/K9pGYwa67gfZiw4HoFdapgiLI4c27ZDXYMbssmAMLEZvZLLb56v
zoOo9uOyBqXuNTHBo4GZN6AN5h0Eu+kpHvBcyywSSV9gMgavqT2MN5lBpFIdiBsC
FQDS73BvJxmrlQyWwhg8pCYjjUt3hwKBgBAI/9JQ5XK9bdnd5a1Dr2KUxpXfNHWJ
g3qWeorbMU0c6PwDdvMfQdA0u/O6sPtbfd86ICpDzWR1gqYPZArxkTz/eIOX8Gcu
pbvp7DdAj/lpS0FzLihiAmPaGGWFL53pOPlVBVm/LVdFMHz7a233J5GsBHkwY5Mk
QrgpTCOK78WgA4GEAAKBgDxPElDHoJi+Fs3HPKbpTKXtHtoGWRlIBYX52FqtqTwf
y3Dn9QeDebdERYoX9YcL6pO+uZGVl7hh26X+/qsdc9N7niYAaEiB66QL42bl/2e2
iQvO9kK+nS1TXiMmELn7R4OL01LauVj0vu1rUIoVY5ODD1rCPaFRNMMIUZQT3vaL
oBswGQYJKoZIhvcNAQkHMQwMCjAxMjM0NTY3ODkwCwYJYIZIAWUDBAMCAy8AMCwC
FBMYYplVEHsBjs8YNvZdk+tLtd6PAhRYItCb6XLQoUoLUBDLDMa+Nv8etQ==
-----END CERTIFICATE REQUEST-----
```



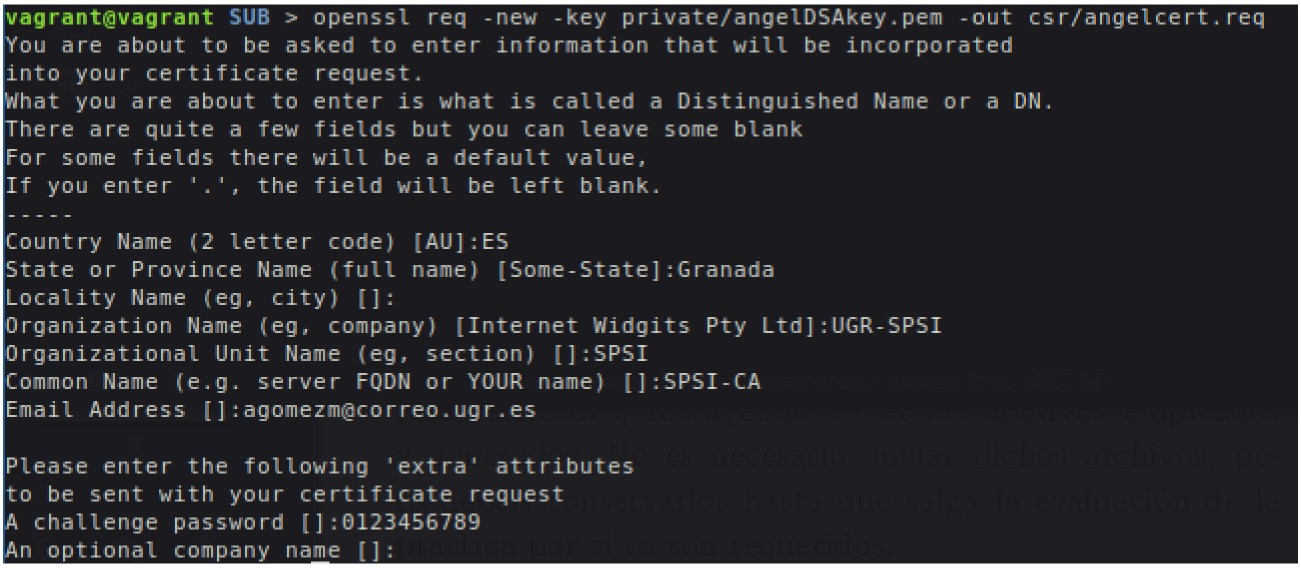
```
vagrant@vagrant CA > openssl req -noout -text -in csr/angelcert.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=ES, ST=Granada, O=UGR-SPSI, OU=SPSI, CN=SPSI-CA/emailAddress=agomezm@correo.
ugr.es
        Subject Public Key Info:
            Public Key Algorithm: dsaEncryption
                pub:
                    3c:4f:12:50:c7:a0:98:be:16:cd:c7:3c:a6:e9:4c:
                    a5:ed:1e:da:06:59:19:48:05:85:f9:d8:5a:ad:a9:
                    3c:1f:cb:70:e7:f5:07:83:79:b7:44:45:8a:17:f5:
                    87:0b:ea:93:be:b9:91:95:97:b8:61:db:a5:fe:fe:
                    ab:1d:73:d3:7b:9e:26:00:68:48:81:eb:a4:0b:e3:
                    66:e5:ff:67:b6:89:0b:ce:f6:42:be:9d:2d:53:5e:
                    23:26:10:b9:fb:47:83:8b:d3:52:da:b9:58:f4:be:
                    ed:6b:50:8a:15:63:93:83:0f:5a:c2:3d:a1:51:34:
                    c3:08:51:94:13:de:f6:8b
                P:
                    00:e2:f8:e5:26:2e:bd:cd:01:f7:24:d3:04:00:e9:
                    b3:c2:d5:04:1e:d6:b9:5f:c7:df:b9:fa:85:d3:73:
                    83:26:6b:0a:c0:19:00:d6:1d:ab:f7:03:9d:fc:af:
                    69:19:8c:1a:eb:b8:1f:66:2c:38:1e:81:5d:6a:98:
                    22:2c:8e:1c:db:b6:43:5d:83:1b:b2:c9:80:30:b1:
                    19:bd:92:cb:6f:9e:af:ce:83:a8:f6:e3:b2:06:a5:
                    ee:35:31:c1:a3:81:99:37:a0:0d:e6:1d:04:bb:e9:
                    29:1e:f0:5c:cb:2c:12:49:5f:60:32:06:af:a9:3d:
                    8c:37:99:41:a4:52:1d:88:1b
                Q:
                    00:d2:ef:70:6f:27:19:ab:95:0c:96:c2:18:3c:a4:
                    26:23:8d:4b:77:87
                G:
                    10:08:ff:d2:50:e5:72:bd:6d:d9:dd:e5:ad:43:af:
                    62:94:c6:95:df:34:75:89:83:7a:96:7a:8a:db:31:
                    4d:1c:e8:fc:03:76:f3:1f:41:d0:34:bb:f3:ba:b0:
                    fb:5b:7d:df:3a:20:2a:43:cd:64:75:82:a6:0f:64:
                    0a:f1:91:3c:ff:78:83:97:f0:67:2e:a5:bb:e9:ec:
                    37:40:8f:f9:69:4b:41:73:2e:28:62:02:63:da:18:
                    65:85:2f:9d:e9:38:f9:55:05:59:bf:2d:57:45:30:
                    7c:fb:6b:6d:f7:27:91:ac:04:79:30:63:93:24:42:
                    b8:29:4c:23:8a:ef:c5:a0
        Attributes:
            challengePassword        :unable to print attribute
    Signature Algorithm: dsa_with_SHA256
         r:
             13:18:62:99:55:10:7b:01:8e:cf:18:36:f6:5d:93:
             eb:4b:b5:de:8f
         s:
             58:22:d0:9b:e9:72:d0:a1:4a:0b:50:10:cb:0c:c6:
             be:36:ff:1e:b5
```

6

En primer lugar creo la solicitud del mismo modo que lo hice en el ejercicio anterior, pero en la entidad subordinada:

Genero la solicitud:

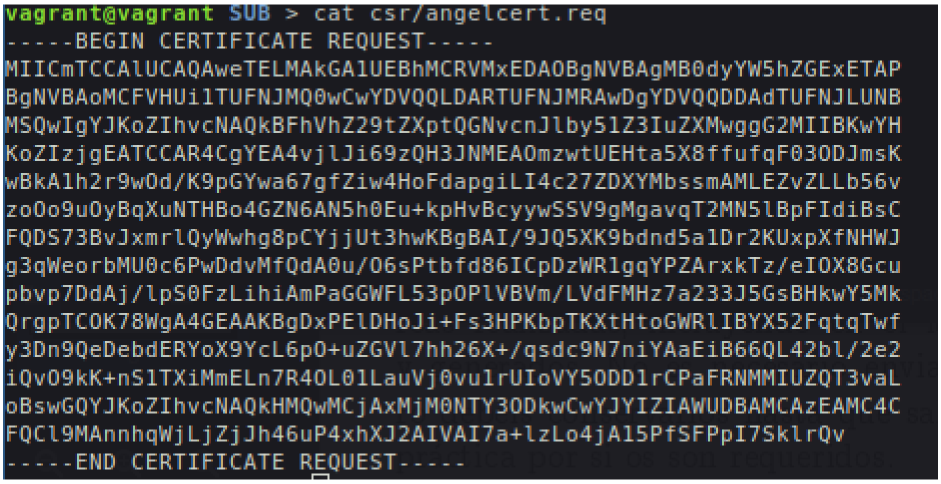
```
openssl req -new -key private/angelDSAkey.pem -out csr/angelcert.req
```



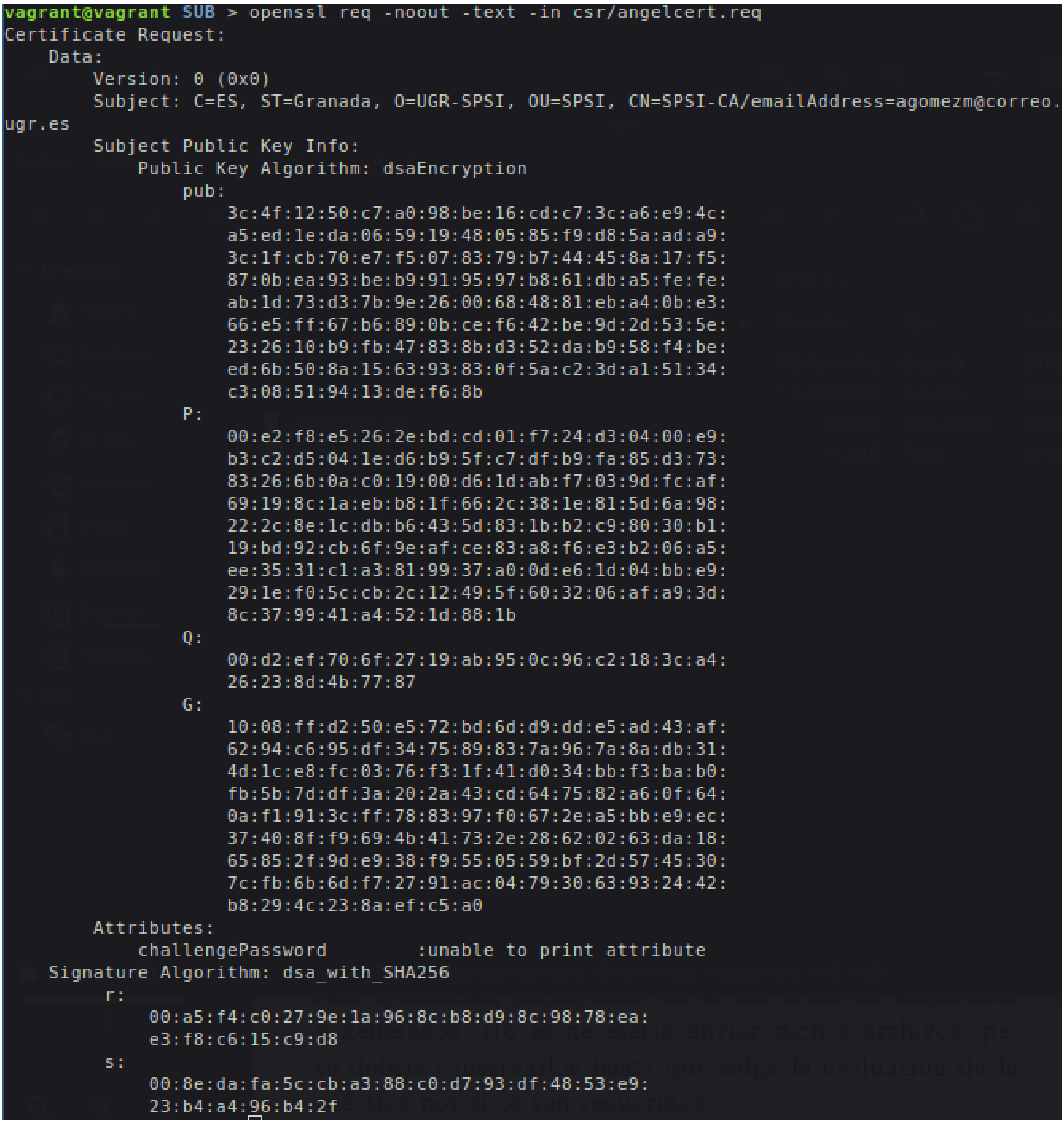
```
vagrant@vagrant SUB > openssl req -new -key private/angelDSAkey.pem -out csr/angelcert.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields 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]:Granada
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UGR-SPSI
Organizational Unit Name (eg, section) []:SPSI
Common Name (e.g. server FQDN or YOUR name) []:SPSI-CA
Email Address []:agomezm@correo.ugr.es

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:0123456789
An optional company name []:
```

Muestro sus valores:

```
openssl req -noout -text -in csr/angelcert.req
```



```
vagrant@vagrant SUB > cat csr/angelcert.req
-----BEGIN CERTIFICATE REQUEST-----
MIICmTCCAlUCAQAweTELMAkGA1UEBhMCRVMxEDAOBgNVBAgMB0dyYW5hZGExETAP
BgNVBAoMCFVHUi1TUFNJMQ0wCwYDVQQLDARTUFNJMRAwDgYDVQQDDAdTUFNJLUNB
MSQwIgYJKoZIhvcNAQkBFhVhZ29tZXptQGNvcnJlby51Z3IuZXMwggG2MIIBKwYH
KoZIzjgEATCCAR4CgYEA4vjlJi69zQH3JNMEAOmzwtUEHta5X8ffufqF03ODJmsK
wBkA1h2r9wOd/K9pGYwa67gfZiw4HoFdapgiLI4c27ZDXYMbssmAMLEZvZLLb56v
zoOo9uOyBqXuNTHBo4GZN6AN5h0Eu+kpHvBcyywSSV9gMgavqT2MN5lBpFIdiBsC
FQDS73BvJxmrlQyWwhg8pCYjjUt3hwKBgBAI/9JQ5XK9bdnd5a1Dr2KUxpXfNHWJ
g3qWeorbMU0c6PwDdvMfQdA0u/O6sPtbfd86ICpDzWR1gqYPZArxkTz/eIOX8Gcu
pbvp7DdAj/lpS0FzLihiAmPaGGWFL53pOPlVBVm/LVdFMHz7a233J5GsBHkwY5Mk
QrgpTCOK78WgA4GEAAKBgDxPElDHoJi+Fs3HPKbpTKXtHtoGWRlIBYX52FqtqTwf
y3Dn9QeDebdERYoX9YcL6pO+uZGVl7hh26X+/qsdc9N7niYAaEiB66QL42bl/2e2
iQvO9kK+nS1TXiMmELn7R4OL01LauVj0vu1rUIoVY5ODD1rCPaFRNMMIUZQT3vaL
oBswGQYJKoZIhvcNAQkHMQwMCjAxMjM0NTY3ODkwCwYJYIZIAWUDBAMCAzEAMC4C
FQCl9MAnnhqWjLjZjJh46uP4xhXJ2AIVAI7a+lzLo4jA15PfSFPpI7SklrQv
-----END CERTIFICATE REQUEST-----
```

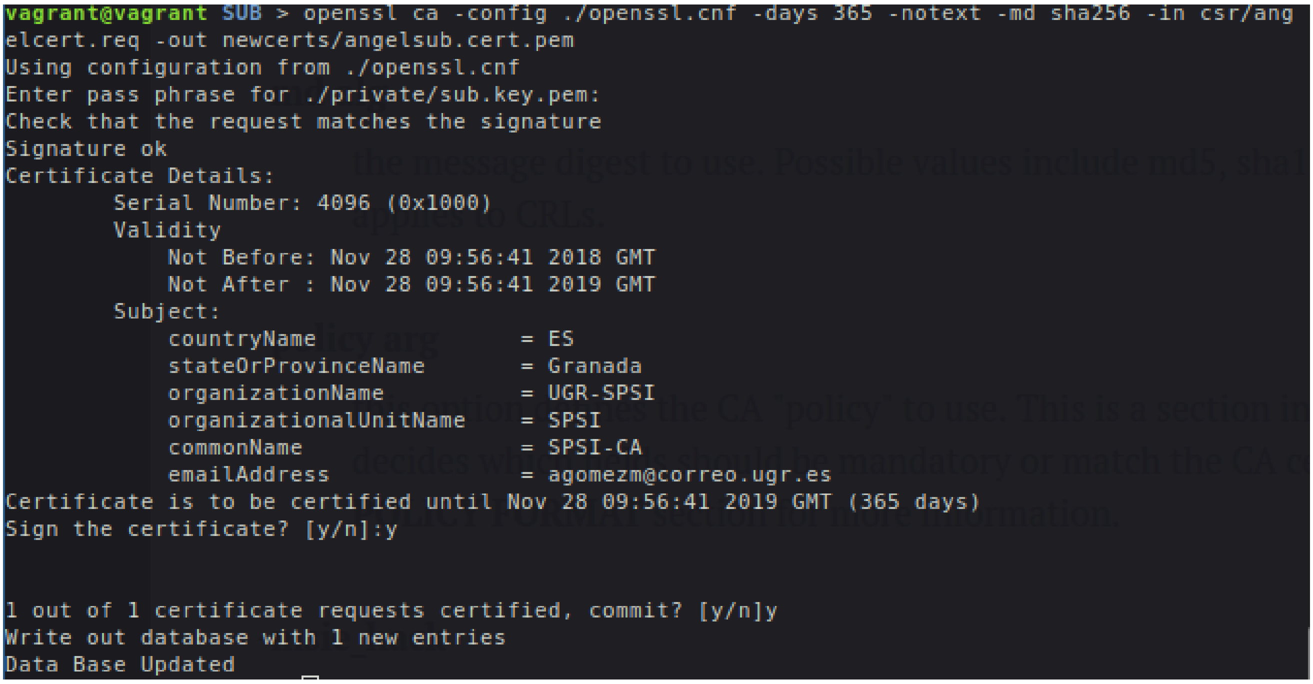


```
vagrant@vagrant SUB > openssl req -noout -text -in csr/angelcert.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=ES, ST=Granada, O=UGR-SPSI, OU=SPSI, CN=SPSI-CA/emailAddress=agomezm@correo.
ugr.es
        Subject Public Key Info:
            Public Key Algorithm: dsaEncryption
                pub:
                    3c:4f:12:50:c7:a0:98:be:16:cd:c7:3c:a6:e9:4c:
                    a5:ed:1e:da:06:59:19:48:05:85:f9:d8:5a:ad:a9:
                    3c:1f:cb:70:e7:f5:07:83:79:b7:44:45:8a:17:f5:
                    87:0b:ea:93:be:b9:91:95:97:b8:61:db:a5:fe:fe:
                    ab:1d:73:d3:7b:9e:26:00:68:48:81:eb:a4:0b:e3:
                    66:e5:ff:67:b6:89:0b:ce:f6:42:be:9d:2d:53:5e:
                    23:26:10:b9:fb:47:83:8b:d3:52:da:b9:58:f4:be:
                    ed:6b:50:8a:15:63:93:83:0f:5a:c2:3d:a1:51:34:
                    c3:08:51:94:13:de:f6:8b
                P:
                    00:e2:f8:e5:26:2e:bd:cd:01:f7:24:d3:04:00:e9:
                    b3:c2:d5:04:1e:d6:b9:5f:c7:df:b9:fa:85:d3:73:
                    83:26:6b:0a:c0:19:00:d6:1d:ab:f7:03:9d:fc:af:
                    69:19:8c:1a:eb:b8:1f:66:2c:38:1e:81:5d:6a:98:
                    22:2c:8e:1c:db:b6:43:5d:83:1b:b2:c9:80:30:b1:
                    19:bd:92:cb:6f:9e:af:ce:83:a8:f6:e3:b2:06:a5:
                    ee:35:31:c1:a3:81:99:37:a0:0d:e6:1d:04:bb:e9:
                    29:1e:f0:5c:cb:2c:12:49:5f:60:32:06:af:a9:3d:
                    8c:37:99:41:a4:52:1d:88:1b
                Q:
                    00:d2:ef:70:6f:27:19:ab:95:0c:96:c2:18:3c:a4:
                    26:23:8d:4b:77:87
                G:
                    10:08:ff:d2:50:e5:72:bd:6d:d9:dd:e5:ad:43:af:
                    62:94:c6:95:df:34:75:89:83:7a:96:7a:8a:db:31:
                    4d:1c:e8:fc:03:76:f3:1f:41:d0:34:bb:f3:ba:b0:
                    fb:5b:7d:df:3a:20:2a:43:cd:64:75:82:a6:0f:64:
                    0a:f1:91:3c:ff:78:83:97:f0:67:2e:a5:bb:e9:ec:
                    37:40:8f:f9:69:4b:41:73:2e:28:62:02:63:da:18:
                    65:85:2f:9d:e9:38:f9:55:05:59:bf:2d:57:45:30:
                    7c:fb:6b:6d:f7:27:91:ac:04:79:30:63:93:24:42:
                    b8:29:4c:23:8a:ef:c5:a0
        Attributes:
            challengePassword        :unable to print attribute
    Signature Algorithm: dsa_with_SHA256
         r:
             00:a5:f4:c0:27:9e:1a:96:8c:b8:d9:8c:98:78:ea:
             e3:f8:c6:15:c9:d8
         s:
             00:8e:da:fa:5c:cb:a3:88:c0:d7:93:df:48:53:e9:
             23:b4:a4:96:b4:2f
```

Y ahora firmo la solicitud para completar el certificado:

```
openssl ca -config ./openssl.cnf -days 365 -notext -md sha256 -in csr/angelcert.req -out
newcerts/angelsub.cert.pem
```

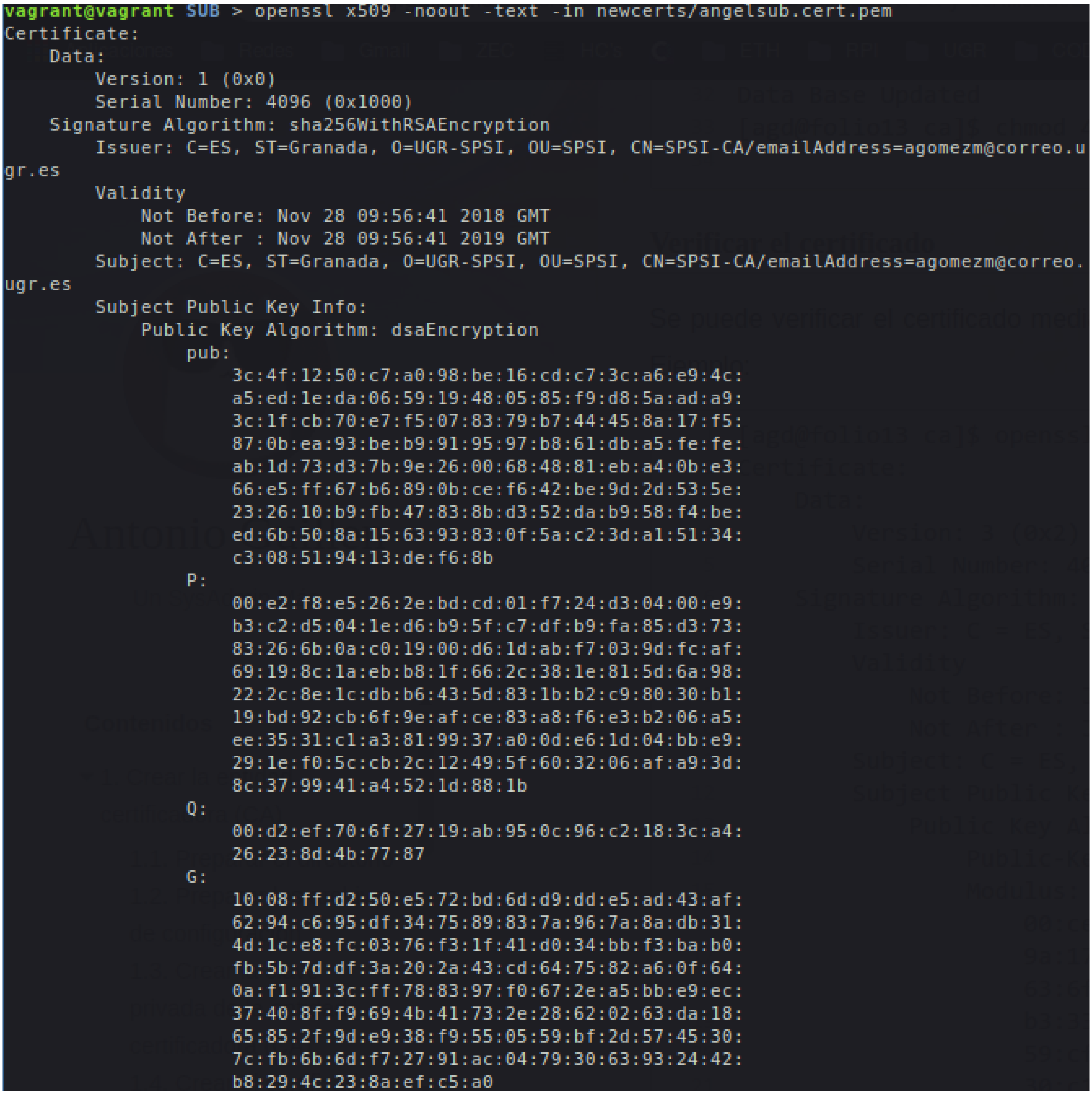
- *-config ./openssl.cnf*: Archivo de configuración a usar.
- *-days 356*: Días para los que es válido el certificado.
- *-md sha256*: Tipo de Message Digest.
- *-in csr/angelcert.req*: Archivo de entrada con la solicitud de certificado.
- *-out newcerts/angelsub.cert.pem*: Archivo de salida con el certificado firmado.



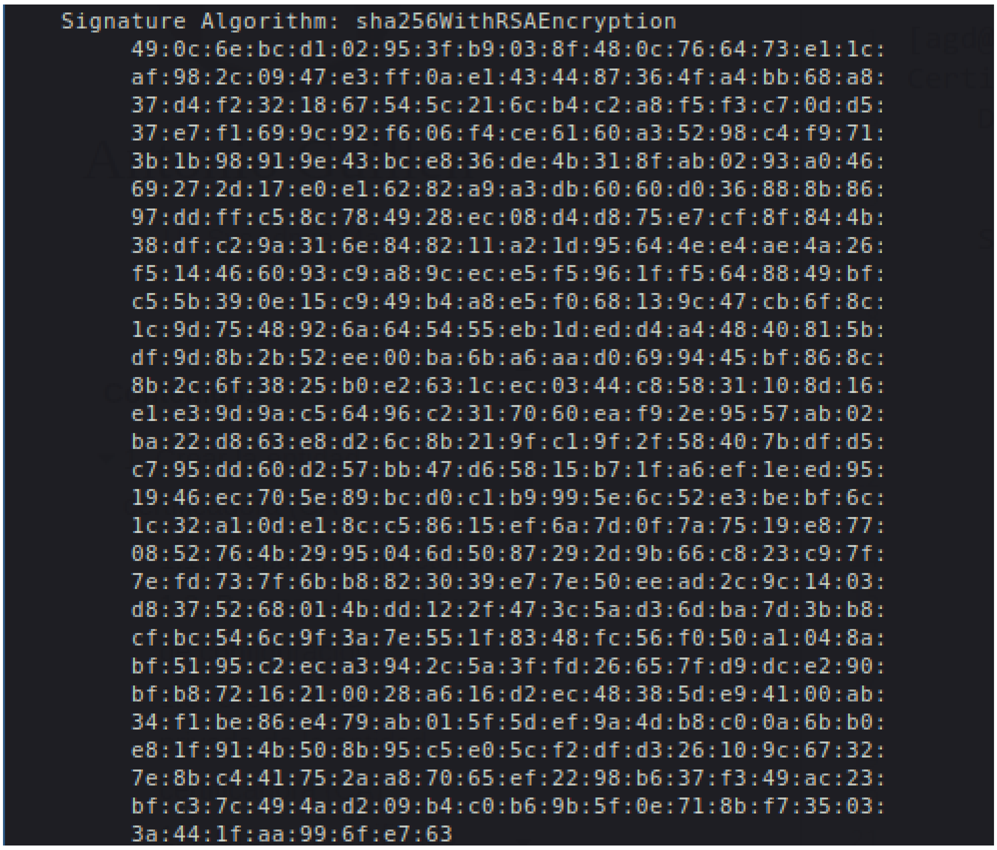
```
vagrant@vagrant SUB > openssl ca -config ./openssl.cnf -days 365 -notext -md sha256 -in csr/ang
elcert.req -out newcerts/angelsub.cert.pem
Using configuration from ./openssl.cnf
Enter pass phrase for ./private/sub.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Nov 28 09:56:41 2018 GMT
            Not After : Nov 28 09:56:41 2019 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = Granada
            organizationName          = UGR-SPSI
            organizationalUnitName    = SPSI
            commonName                = SPSI-CA
            emailAddress              = agomezm@correo.ugr.es
Certificate is to be certified until Nov 28 09:56:41 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
```

Y finalmente compruebo sus valores:

```
openssl x509 -noout -text -in newcerts/angelsub.cert.pem
```



```
vagrant@vagrant SUB > openssl x509 -noout -text -in newcerts/angelsub.cert.pem
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, ST=Granada, O=UGR-SPSI, OU=SPSI, CN=SPSI-CA/emailAddress=agomezm@correo.u
gr.es
        Validity
            Not Before: Nov 28 09:56:41 2018 GMT
            Not After : Nov 28 09:56:41 2019 GMT
        Subject: C=ES, ST=Granada, O=UGR-SPSI, OU=SPSI, CN=SPSI-CA/emailAddress=agomezm@correo.
ugr.es
        Subject Public Key Info:
            Public Key Algorithm: dsaEncryption
                pub:
                    3c:4f:12:50:c7:a0:98:be:16:cd:c7:3c:a6:e9:4c:
                    a5:ed:1e:da:06:59:19:48:05:85:f9:d8:5a:ad:a9:
                    3c:1f:cb:70:e7:f5:07:83:79:b7:44:45:8a:17:f5:
                    87:0b:ea:93:be:b9:91:95:97:b8:61:db:a5:fe:fe:
                    ab:1d:73:d3:7b:9e:26:00:68:48:81:eb:a4:0b:e3:
                    66:e5:ff:67:b6:89:0b:ce:f6:42:be:9d:2d:53:5e:
                    23:26:10:b9:fb:47:83:8b:d3:52:da:b9:58:f4:be:
                    ed:6b:50:8a:15:63:93:83:0f:5a:c2:3d:a1:51:34:
                    c3:08:51:94:13:de:f6:8b
                P:
                    00:e2:f8:e5:26:2e:bd:cd:01:f7:24:d3:04:00:e9:
                    b3:c2:d5:04:1e:d6:b9:5f:c7:df:b9:fa:85:d3:73:
                    83:26:6b:0a:c0:19:00:d6:1d:ab:f7:03:9d:fc:af:
                    69:19:8c:1a:eb:b8:1f:66:2c:38:1e:81:5d:6a:98:
                    22:2c:8e:1c:db:b6:43:5d:83:1b:b2:c9:80:30:b1:
                    19:bd:92:cb:6f:9e:af:ce:83:a8:f6:e3:b2:06:a5:
                    ee:35:31:c1:a3:81:99:37:a0:0d:e6:1d:04:bb:e9:
                    29:1e:f0:5c:cb:2c:12:49:5f:60:32:06:af:a9:3d:
                    8c:37:99:41:a4:52:1d:88:1b
                Q:
                    00:d2:ef:70:6f:27:19:ab:95:0c:96:c2:18:3c:a4:
                    26:23:8d:4b:77:87
                G:
                    10:08:ff:d2:50:e5:72:bd:6d:d9:dd:e5:ad:43:af:
                    62:94:c6:95:df:34:75:89:83:7a:96:7a:8a:db:31:
                    4d:1c:e8:fc:03:76:f3:1f:41:d0:34:bb:f3:ba:b0:
                    fb:5b:7d:df:3a:20:2a:43:cd:64:75:82:a6:0f:64:
                    0a:f1:91:3c:ff:78:83:97:f0:67:2e:a5:bb:e9:ec:
                    37:40:8f:f9:69:4b:41:73:2e:28:62:02:63:da:18:
                    65:85:2f:9d:e9:38:f9:55:05:59:bf:2d:57:45:30:
                    7c:fb:6b:6d:f7:27:91:ac:04:79:30:63:93:24:42:
                    b8:29:4c:23:8a:ef:c5:a0
```



```
    Signature Algorithm: sha256WithRSAEncryption
         49:0c:6e:bc:d1:02:95:3f:b9:03:8f:48:0c:76:64:73:e1:1c:
         af:98:2c:09:47:e3:ff:0a:e1:43:44:87:36:4f:a4:bb:68:a8:
         37:d4:f2:32:18:67:54:5c:21:6c:b4:c2:a8:f5:f3:c7:0d:d5:
         37:e7:f1:69:9c:92:f6:06:f4:ce:61:60:a3:52:98:c4:f9:71:
         3b:1b:98:91:9e:43:bc:e8:36:de:4b:31:8f:ab:02:93:a0:46:
         69:27:2d:17:e0:e1:62:82:a9:a3:db:60:60:d0:36:88:8b:86:
         97:dd:ff:c5:8c:78:49:28:ec:08:d4:d8:75:e7:cf:8f:84:4b:
         38:df:c2:9a:31:6e:84:82:11:a2:1d:95:64:4e:e4:ae:4a:26:
         f5:14:46:60:93:c9:a8:9c:ec:e5:f5:96:1f:f5:64:88:49:bf:
         c5:5b:39:0e:15:c9:49:b4:a8:e5:f0:68:13:9c:47:cb:6f:8c:
         1c:9d:75:48:92:6a:64:54:55:eb:1d:ed:d4:a4:48:40:81:5b:
         df:9d:8b:2b:52:ee:00:ba:6b:a6:aa:d0:69:94:45:bf:86:8c:
         8b:2c:6f:38:25:b0:e2:63:1c:ec:03:44:c8:58:31:10:8d:16:
         e1:e3:9d:9a:c5:64:96:c2:31:70:60:ea:f9:2e:95:57:ab:02:
         ba:22:d8:63:e8:d2:6c:8b:21:9f:c1:9f:2f:58:40:7b:df:d5:
         c7:95:dd:60:d2:57:bb:47:d6:58:15:b7:1f:a6:ef:1e:ed:95:
         19:46:ec:70:5e:89:bc:d0:c1:b9:99:5e:6c:52:e3:be:bf:6c:
         1c:32:a1:0d:e1:8c:c5:86:15:ef:6a:7d:0f:7a:75:19:e8:77:
         08:52:76:4b:29:95:04:6d:50:87:29:2d:9b:66:c8:23:c9:7f:
         7e:fd:73:7f:6b:b8:82:30:39:e7:7e:50:ee:ad:2c:9c:14:03:
         d8:37:52:68:01:4b:dd:12:2f:47:3c:5a:d3:6d:ba:7d:3b:b8:
         cf:bc:54:6c:9f:3a:7e:55:1f:83:48:fc:56:f0:50:a1:04:8a:
         bf:51:95:c2:ec:a3:94:2c:5a:3f:fd:26:65:7f:d9:dc:e2:90:
         bf:b8:72:16:21:00:28:a6:16:d2:ec:48:38:5d:e9:41:00:ab:
         34:f1:be:86:e4:79:ab:01:5f:5d:ef:9a:4d:b8:c0:0a:6b:b0:
         e8:1f:91:4b:50:8b:95:c5:e0:5c:f2:df:d3:26:10:9c:67:32:
         7e:8b:c4:41:75:2a:a8:70:65:ef:22:98:b6:37:f3:49:ac:23:
         bf:c3:7c:49:4a:d2:09:b4:c0:b6:9b:5f:0e:71:8b:f7:35:03:
         3a:44:1f:aa:99:6f:e7:63
```