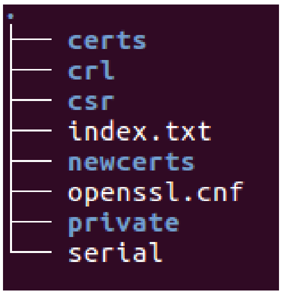
PRACTICA 4 SPSI

Certificados digitales

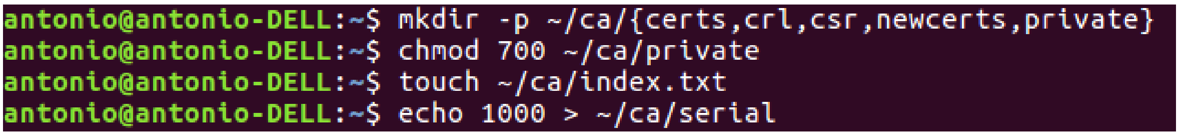
Antonio Manuel Rodriguez Martos

1. Cread una autoridad certicadora raiz. Mostrad los archivos creados y sus rutas, y los valores de las claves generadas.

Para empezar prepararemos el directorio donde operaremos, este tendrá la siguiente estructura:



```
.
├── certs
├── crl
├── csr
├── index.txt
├── newcerts
├── openssl.cnf
├── private
└── serial
```

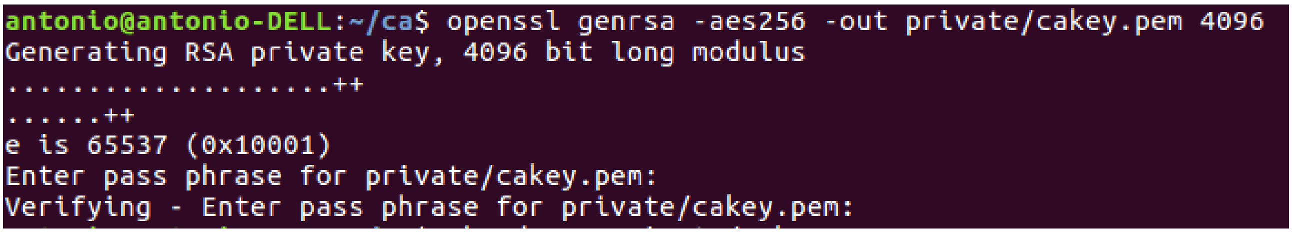


```
antonio@antonio-DELL:~$ mkdir -p ~/ca/{certs,crl,csr,newcerts,private}
antonio@antonio-DELL:~$ chmod 700 ~/ca/private
antonio@antonio-DELL:~$ touch ~/ca/index.txt
antonio@antonio-DELL:~$ echo 1000 > ~/ca/serial
```

Para configurar la autoridad certificadora tendremos que incluir y preparar el archivo openssl.cnf en nuestro directorio. Dicho archivo lo copiaremos de *etc/ssl.*
Después modificaremos algunos de sus parametros.

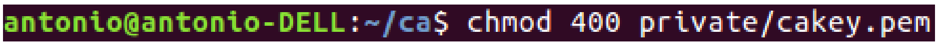
```
[ CA_default ]

dir             = /home/antonio/ca              # Where everything is kept

certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
new_certs_dir = $dir/newcerts                   # default place for new certs.
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number

certificate     = $dir/certs/cacert.pem         # The CA certificate
private_key     = $dir/private/cakey.pem

default_days    = 245                   # how long to certify for

countryName_default             = ES
stateOrProvinceName_default             = GRANADA
localityName_default            = GRANADA
0.organizationName_default  = UGR
organizationalUnitName_default          = ETSIIT
emailAddress_default            = antoniomrm@correo.ugr.es
```

A continuación crearemos la clave privada de la CA raíz, la cual estará protegida para el usuario en la carpeta private.
Utilizaremos por ejemplo el protocolo AES256 con un tamaño de 4096 bits. Contraseña 0123456789.



```
antonio@antonio-DELL:~/ca$ openssl genrsa -aes256 -out private/cakey.pem 4096
Generating RSA private key, 4096 bit long modulus
....................++
......++
e is 65537 (0x10001)
Enter pass phrase for private/cakey.pem:
Verifying - Enter pass phrase for private/cakey.pem:
```

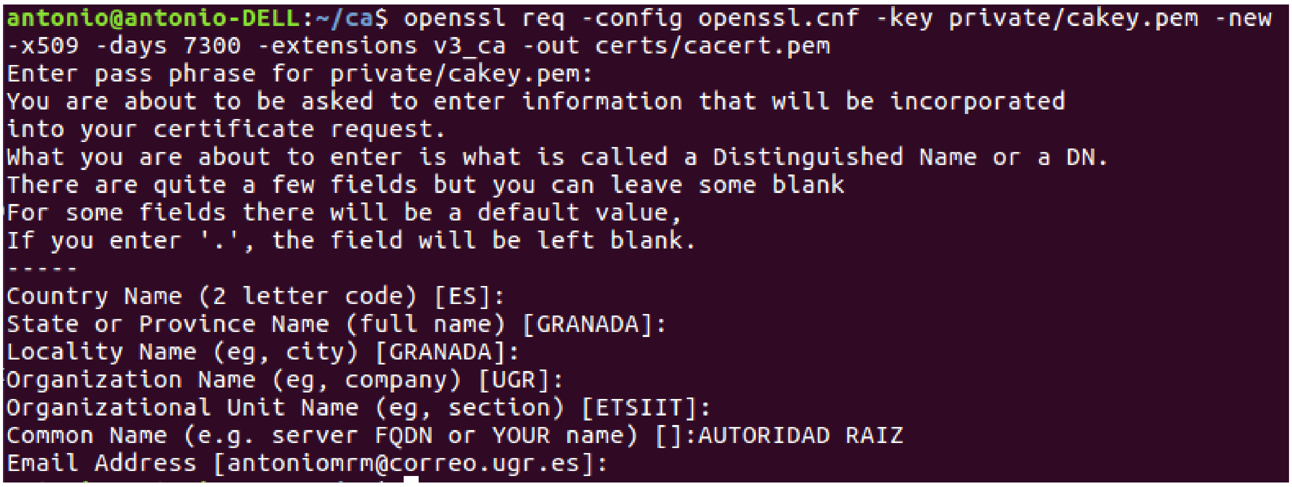
Protegemos modificando los permisos para solo lectura.



```
antonio@antonio-DELL:~/ca$ chmod 400 private/cakey.pem
```

Ahora crearemos el certificado raiz *cacert.pem.*
Utilizando el comando de openssl req, le pasaremos el archivo de configuración *openssl.cnf* antes definido con la opcion -config y la clave privada con la opcion -key.
Con la opción -new se generará una nueva solicitud de certificado y con -x509 se generará un certificado autofirmado en lugar de una solicitud de certificado.
Después especificaremos los dias de expiración del certificado con -days (Pondremos 20 años porque una vez que expire el certificado raíz todos los certificados firmados por la CA Raíz no serán válidos) y la extension contenida en *openssl.cnf con* -extension, por defecto v3_ca.
Finalmente el archivo destino *ca/certs/cacert.pem*

Como ya definimos unas etiquetas por defecto solo escribiremos en Common Name para poder diferenciar.

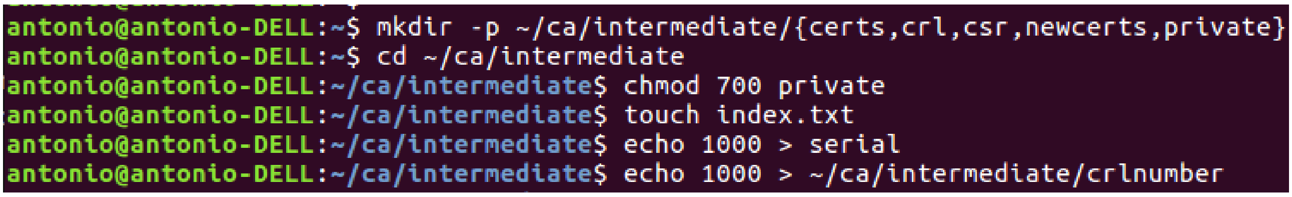


```
antonio@antonio-DELL:~/ca$ openssl req -config openssl.cnf -key private/cakey.pem -new
-x509 -days 7300 -extensions v3_ca -out certs/cacert.pem
Enter pass phrase for private/cakey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you 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 (full name) [GRANADA]:
Locality Name (eg, city) [GRANADA]:
Organization Name (eg, company) [UGR]:
Organizational Unit Name (eg, section) [ETSIIT]:
Common Name (e.g. server FQDN or YOUR name) []:AUTORIDAD RAIZ
Email Address [antoniomrm@correo.ugr.es]:
```

Como veremos mas tarde nosotros no utilizaremos la raíz para firmar directamente certificados, sino que mediante esta, crearemos una autoridad certificadora intermedia que firmará certificados en su nombre. (Lo que normalmente se hace).

2. Cread una autoridad certicadora subordinada a la anterior. Mostrad los archivos creados y sus rutas, y los valores de las claves generadas.

En la CA subordinada o intermedia crearemos la misma estructura de directorio que utilizamos con la CA raíz.

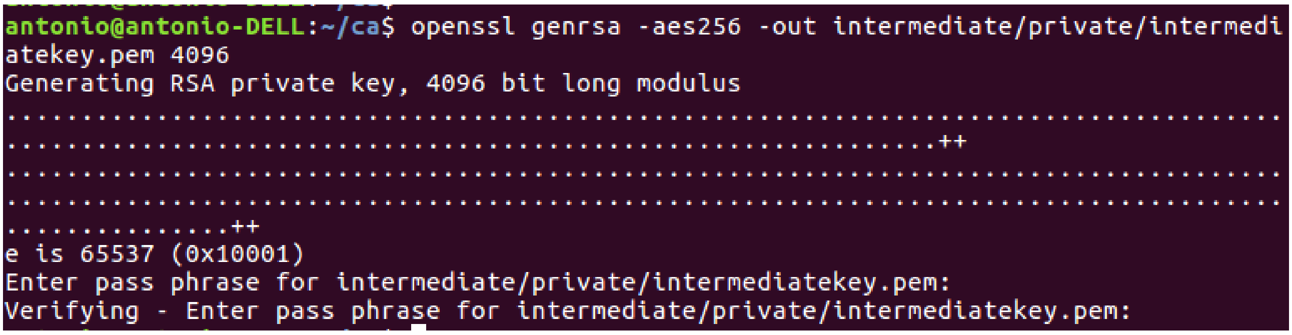


```
antonio@antonio-DELL:~$ mkdir -p ~/ca/intermediate/{certs,crl,csr,newcerts,private}
antonio@antonio-DELL:~$ cd ~/ca/intermediate
antonio@antonio-DELL:~/ca/intermediate$ chmod 700 private
antonio@antonio-DELL:~/ca/intermediate$ touch index.txt
antonio@antonio-DELL:~/ca/intermediate$ echo 1000 > serial
antonio@antonio-DELL:~/ca/intermediate$ echo 1000 > ~/ca/intermediate/crlnumber
```

Modificamos algunos valores de openssl.cnf.

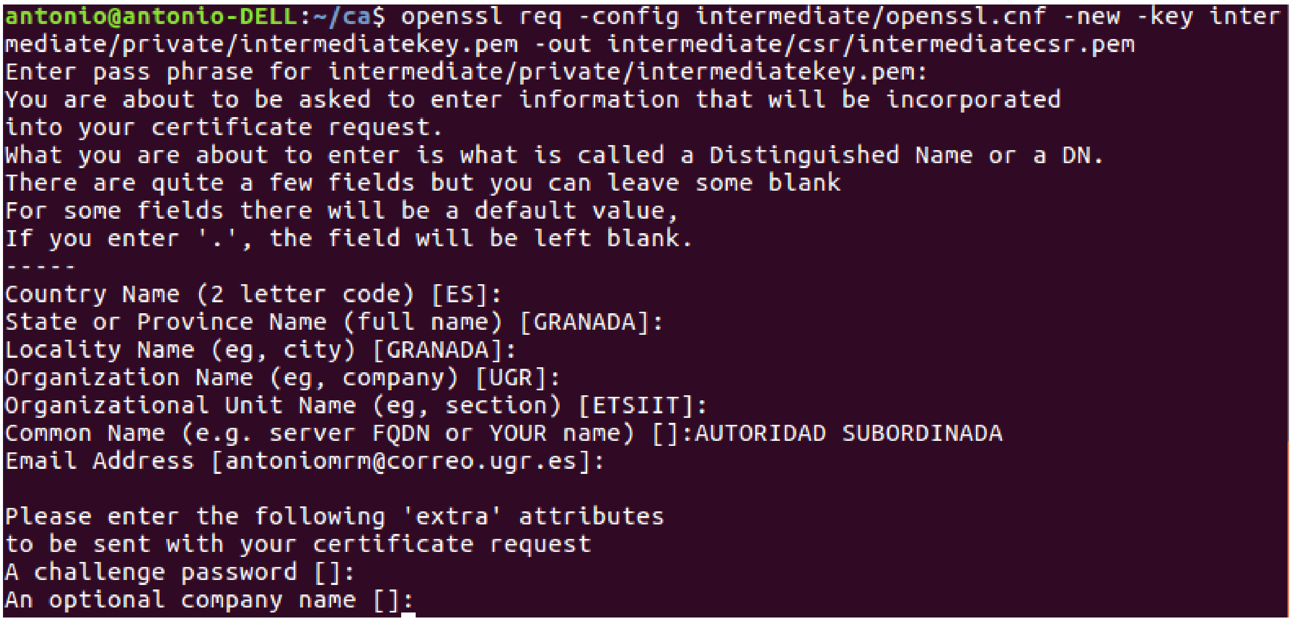
```
dir             = /home/antonio/ca/intermediate              # Where everything is kept
certificate     = $dir/certs/intermediatecert.pem      # The CA certificate
crl             = $dir/crl/intermediatecrl.pem               # The current CRL
private_key     = $dir/private/intermediatekey.pem   # The private key

policy          = policy_loose
# política relajada: Permite a las Autoridades Intermedias
# firmar certificados de terceras partes
# Esta política se usará en las firmas que realice la Autoridad Intermedia
# Esta política requiere que:
#         - Se exige la introducción de todos los campos
#         - El ON debe coincidir con la Autoridad Certificadora Intermedia
[ policy_loose ]
countryName             = supplied
stateOrProvinceName     = supplied
localityName            = supplied
organizationName        = match
organizationalUnitName  = supplied
commonName              = supplied
emailAddress            = supplied
```

A continuación crearemos la clave privada de la CA subordinada, la cual estará protegida para el usuario en la carpeta private.
Utilizaremos como antes AES256 con un tamaño de 4096 bits. Contraseña 0123456789.



```
antonio@antonio-DELL:~/ca$ openssl genrsa -aes256 -out intermediate/private/intermedi
atekey.pem 4096
Generating RSA private key, 4096 bit long modulus
...........................................................................................
.............................................................++
...........................................................................................
...........................................................................................
...............++
e is 65537 (0x10001)
Enter pass phrase for intermediate/private/intermediatekey.pem:
Verifying - Enter pass phrase for intermediate/private/intermediatekey.pem:
```

Ahora crearemos el certificado, utilizaremos el mismo comando del apartado anterior, openssl req. Le pasaremos el archivo de configuración *openssl.cnf* de la subordinada antes definido con la opción -config y la clave privada con la opcion -key.
Con la opción -new se generará una nueva solicitud de certificado.
Finalmente el archivo destino *ca/intermediate/csr/intermediatecsr.pem*

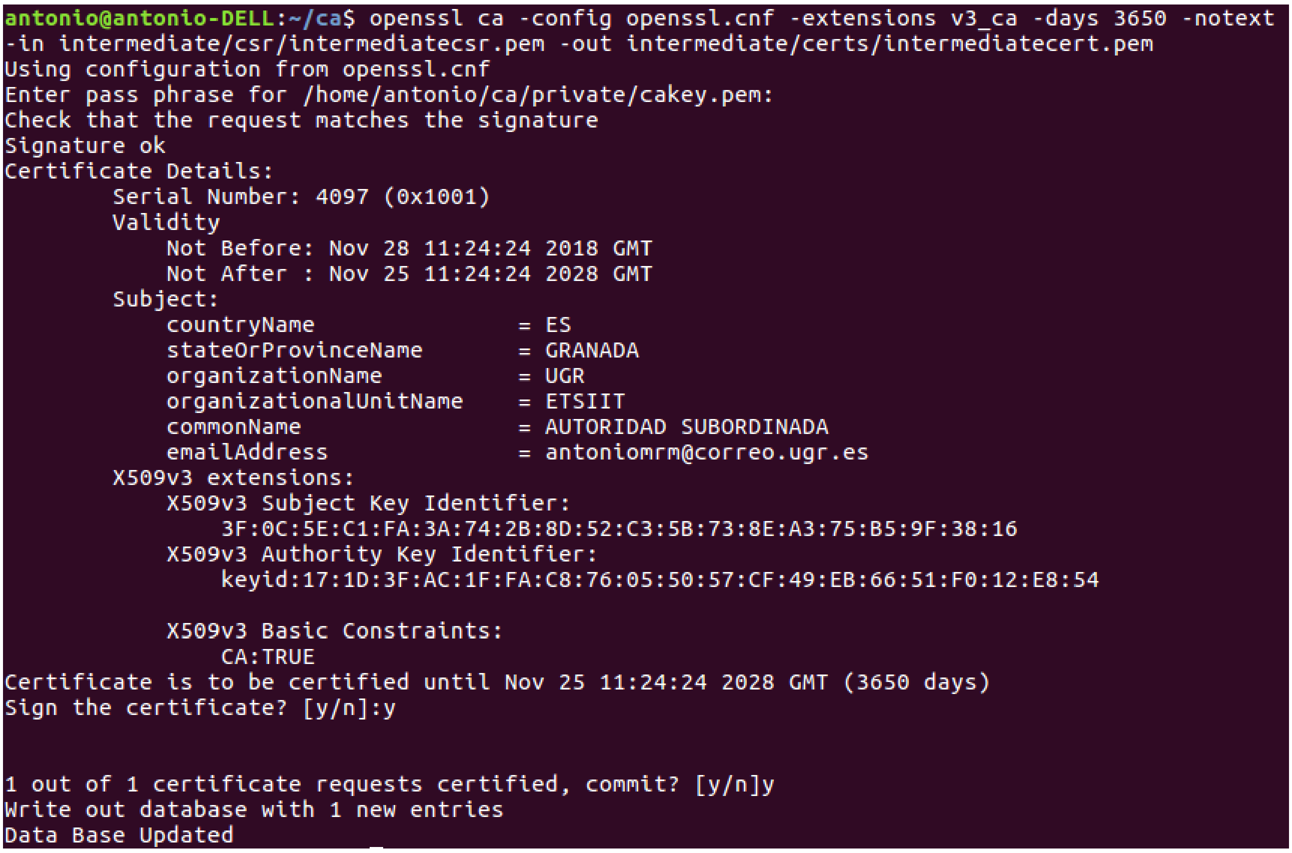


```
antonio@antonio-DELL:~/ca$ openssl req -config intermediate/openssl.cnf -new -key inter
mediate/private/intermediatekey.pem -out intermediate/csr/intermediatecsr.pem
Enter pass phrase for intermediate/private/intermediatekey.pem:
You are about to be asked to enter information that will be incorporated
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 (full name) [GRANADA]:
Locality Name (eg, city) [GRANADA]:
Organization Name (eg, company) [UGR]:
Organizational Unit Name (eg, section) [ETSIIT]:
Common Name (e.g. server FQDN or YOUR name) []:AUTORIDAD SUBORDINADA
Email Address [antoniomrm@correo.ugr.es]:

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

Solo ingresaremos el nombre (AUTORIDAD SUBORDINADA), es recomendable que todos los valores coincidan con los de la CA raíz.

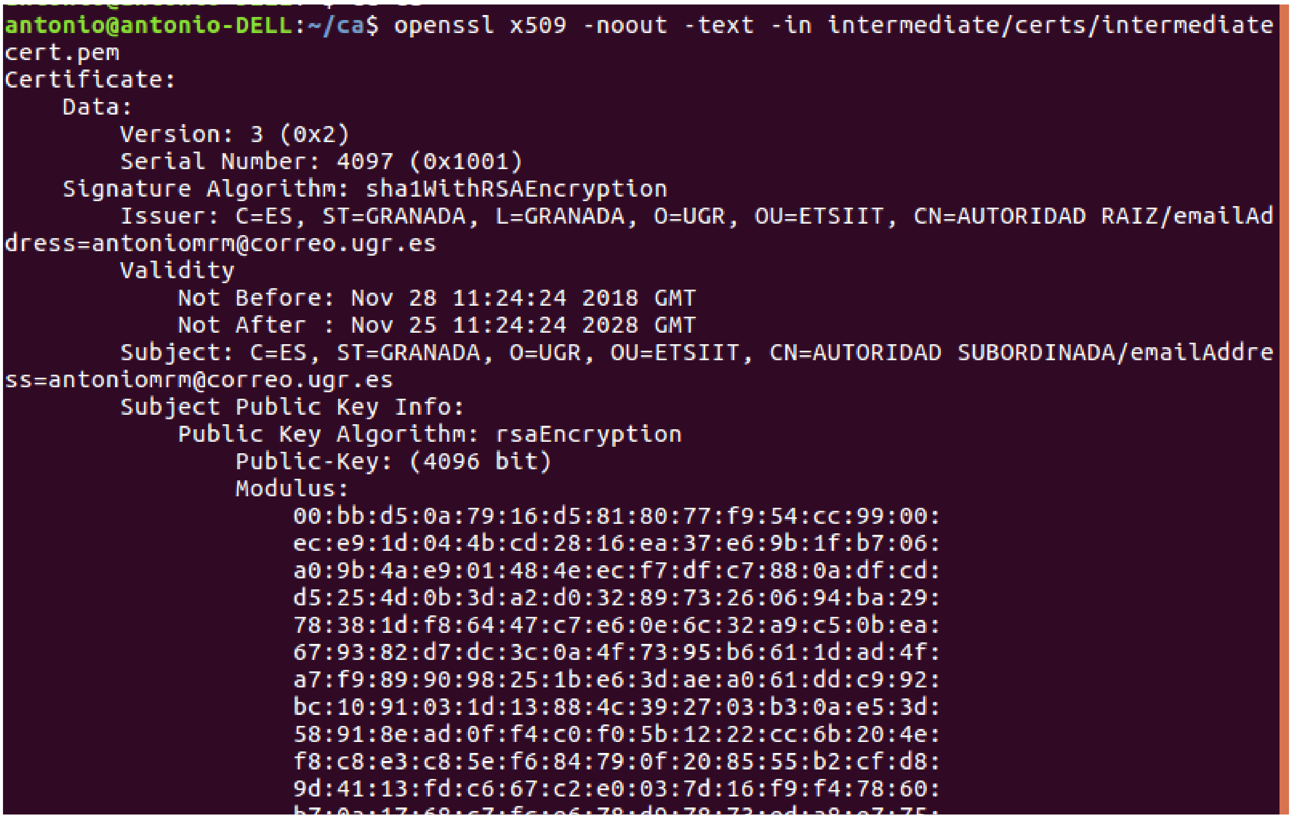
A continuación firmaremos con la autoridad subordinada con la raiz.

Usaremos el comando de openssl ca. Como antes le pasamos el archivo de configuracion con la opcion -config, muy importante pasarle la de CA raiz, la extesión con -extension, por defecto v3_ca, y el tiempo antes de que expire con -days.
Después le pasaremos la solicitud de certificado a firmar y el nombre del certificado final firmado.



```
antonio@antonio-DELL:~/ca$ openssl ca -config openssl.cnf -extensions v3_ca -days 3650 -notext
-in intermediate/csr/intermediatecsr.pem -out intermediate/certs/intermediatecert.pem
Using configuration from openssl.cnf
Enter pass phrase for /home/antonio/ca/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Nov 28 11:24:24 2018 GMT
            Not After : Nov 25 11:24:24 2028 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = GRANADA
            organizationName          = UGR
            organizationalUnitName    = ETSIIT
            commonName                = AUTORIDAD SUBORDINADA
            emailAddress              = antoniomrm@correo.ugr.es
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                3F:0C:5E:C1:FA:3A:74:2B:8D:52:C3:5B:73:8E:A3:75:B5:9F:38:16
            X509v3 Authority Key Identifier:
                keyid:17:1D:3F:AC:1F:FA:C8:76:05:50:57:CF:49:EB:66:51:F0:12:E8:54

            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until Nov 25 11:24:24 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
```

Con la opción de openssl x509 podremos ver más detalles a cerca del certificado.



```
antonio@antonio-DELL:~/ca$ openssl x509 -noout -text -in intermediate/certs/intermediate
cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4097 (0x1001)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=ES, ST=GRANADA, L=GRANADA, O=UGR, OU=ETSIIT, CN=AUTORIDAD RAIZ/emailAd
dress=antoniomrm@correo.ugr.es
        Validity
            Not Before: Nov 28 11:24:24 2018 GMT
            Not After : Nov 25 11:24:24 2028 GMT
        Subject: C=ES, ST=GRANADA, O=UGR, OU=ETSIIT, CN=AUTORIDAD SUBORDINADA/emailAddre
ss=antoniomrm@correo.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:bb:d5:0a:79:16:d5:81:80:77:f9:54:cc:99:00:
                    ec:e9:1d:04:4b:cd:28:16:ea:37:e6:9b:1f:b7:06:
                    a0:9b:4a:e9:01:48:4e:ec:f7:df:c7:88:0a:df:cd:
                    d5:25:4d:0b:3d:a2:d0:32:89:73:26:06:94:ba:29:
                    78:38:1d:f8:64:47:c7:e6:0e:6c:32:a9:c5:0b:ea:
                    67:93:82:d7:dc:3c:0a:4f:73:95:b6:61:1d:ad:4f:
                    a7:f9:89:90:98:25:1b:e6:3d:ae:a0:61:dd:c9:92:
                    bc:10:91:03:1d:13:88:4c:39:27:03:b3:0a:e5:3d:
                    58:91:8e:ad:0f:f4:c0:f0:5b:12:22:cc:6b:20:4e:
                    f8:c8:e3:c8:5e:f6:84:79:0f:20:85:55:b2:cf:d8:
                    9d:41:13:fd:c6:67:c2:e0:03:7d:16:f9:f4:78:60:
                    b7:0a:17:68:c7:fc:e6:78:d0:78:73:ed:a8:e7:75:
```

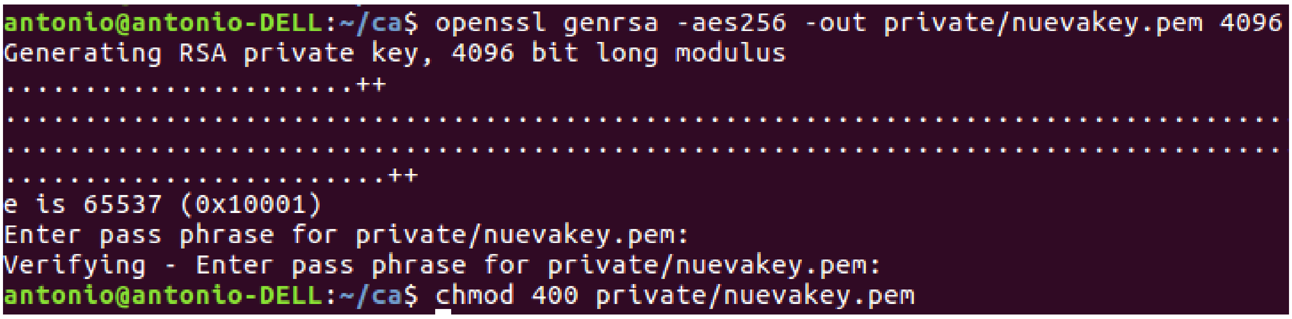
Como vemos el emisor es la Autoridad Raíz.

Tambien podemos ver el index.txt de la CA Raíz para mirar la firma emitida.

```
V       281125112424Z           1001    unknown
        /C=ES/ST=GRANADA/O=UGR/OU=ETSIIT/CN=AUTORIDAD SUBORDINADA
/emailAddress=antoniomrm@correo.ugr.es
```

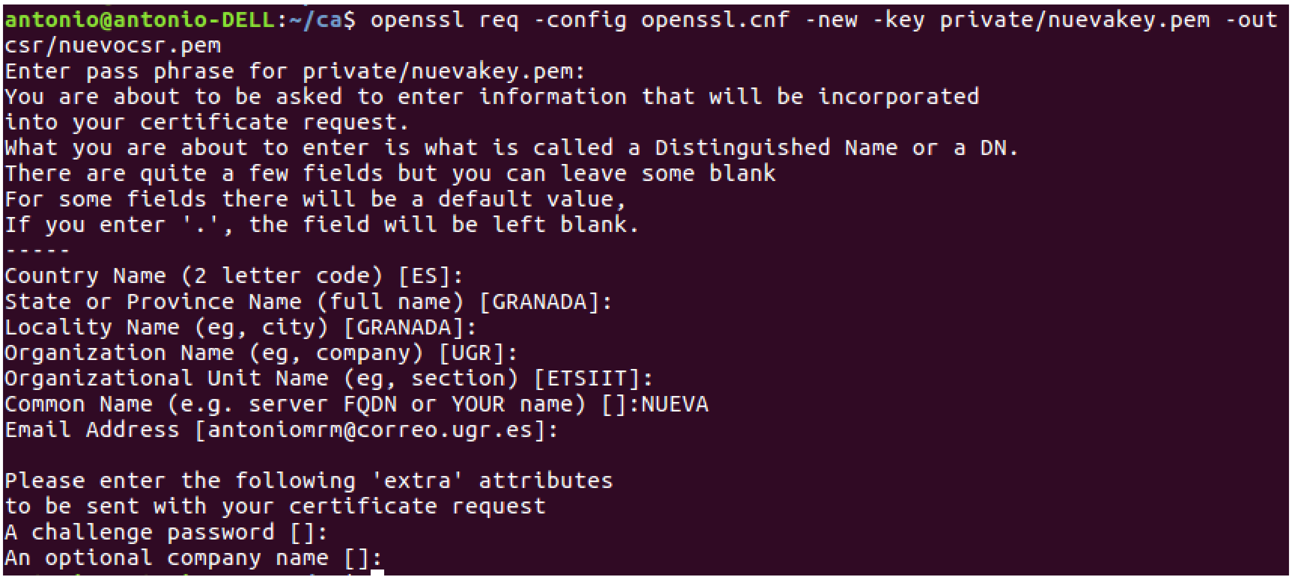
3. Cread una solicitud de certicado que incluya la generación de claves en la misma. Mostrad los valores junto con el archivo.

Primero generamos una clave privada para el que solicita el certificado como hemos hecho antes. Y modifico los permisos para solo lectura.



```
antonio@antonio-DELL:~/ca$ openssl genrsa -aes256 -out private/nuevakey.pem 4096
Generating RSA private key, 4096 bit long modulus
.......................++
..............................................................................
..............................................................................
.........................++
e is 65537 (0x10001)
Enter pass phrase for private/nuevakey.pem:
Verifying - Enter pass phrase for private/nuevakey.pem:
antonio@antonio-DELL:~/ca$ chmod 400 private/nuevakey.pem
```

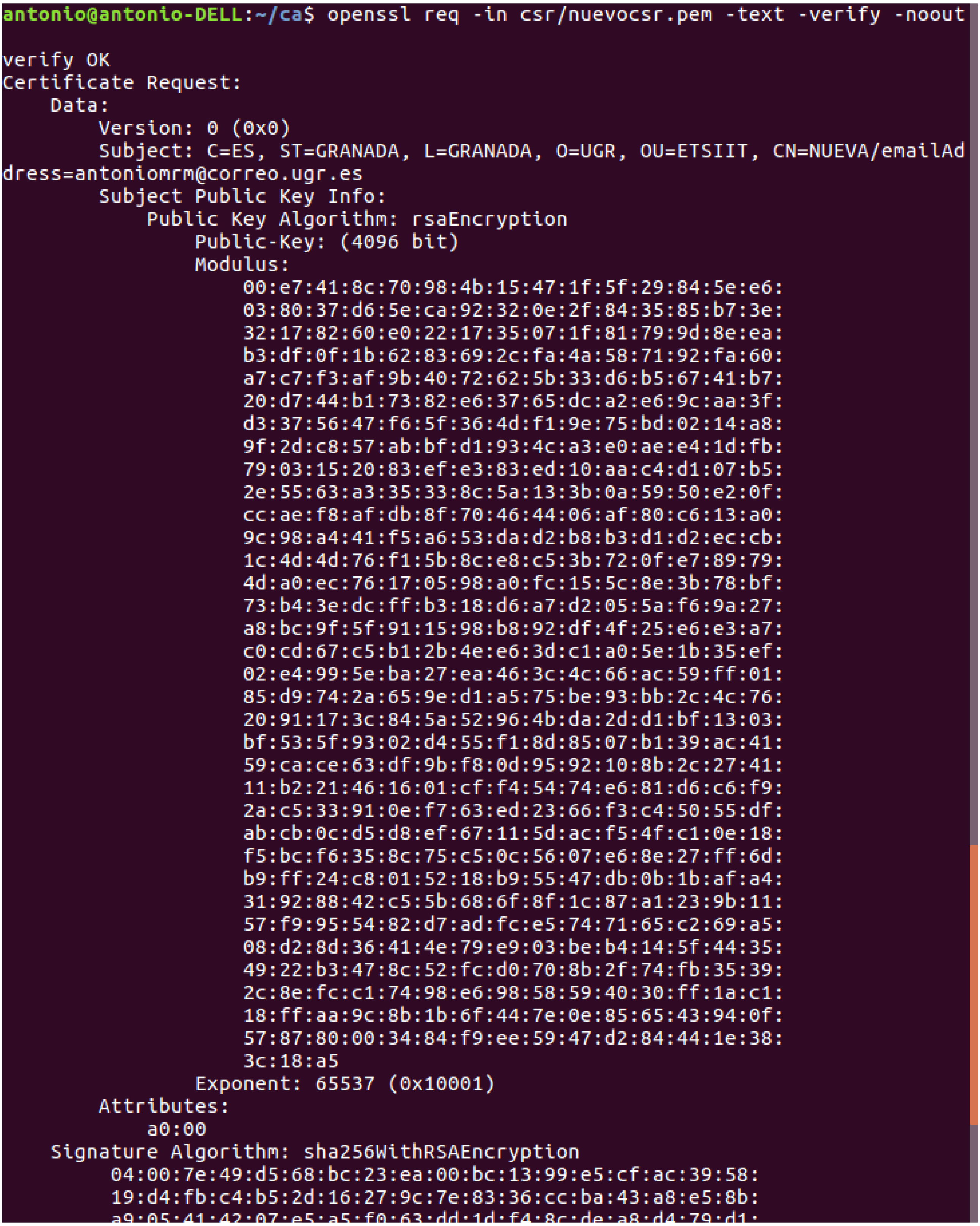
Ahora crearemos la solicitud de certificado con req con el archivo openssl.cnf de mi subordinada o raíz y la clave que generamos antes.
Finalmente el archivo destino */csr/nuevocsr.pem*



```
antonio@antonio-DELL:~/ca$ openssl req -config openssl.cnf -new -key private/nuevakey.pem -out
csr/nuevocsr.pem
Enter pass phrase for private/nuevakey.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 (full name) [GRANADA]:
Locality Name (eg, city) [GRANADA]:
Organization Name (eg, company) [UGR]:
Organizational Unit Name (eg, section) [ETSIIT]:
Common Name (e.g. server FQDN or YOUR name) []:NUEVA
Email Address [antoniomrm@correo.ugr.es]:

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

Como ya definimos unas etiquetas por defecto solo escribiremos el nombre (NUEVA).

Con -req también podemos ver mas informacion de la solicitud de firma del certificado y sus atributos.

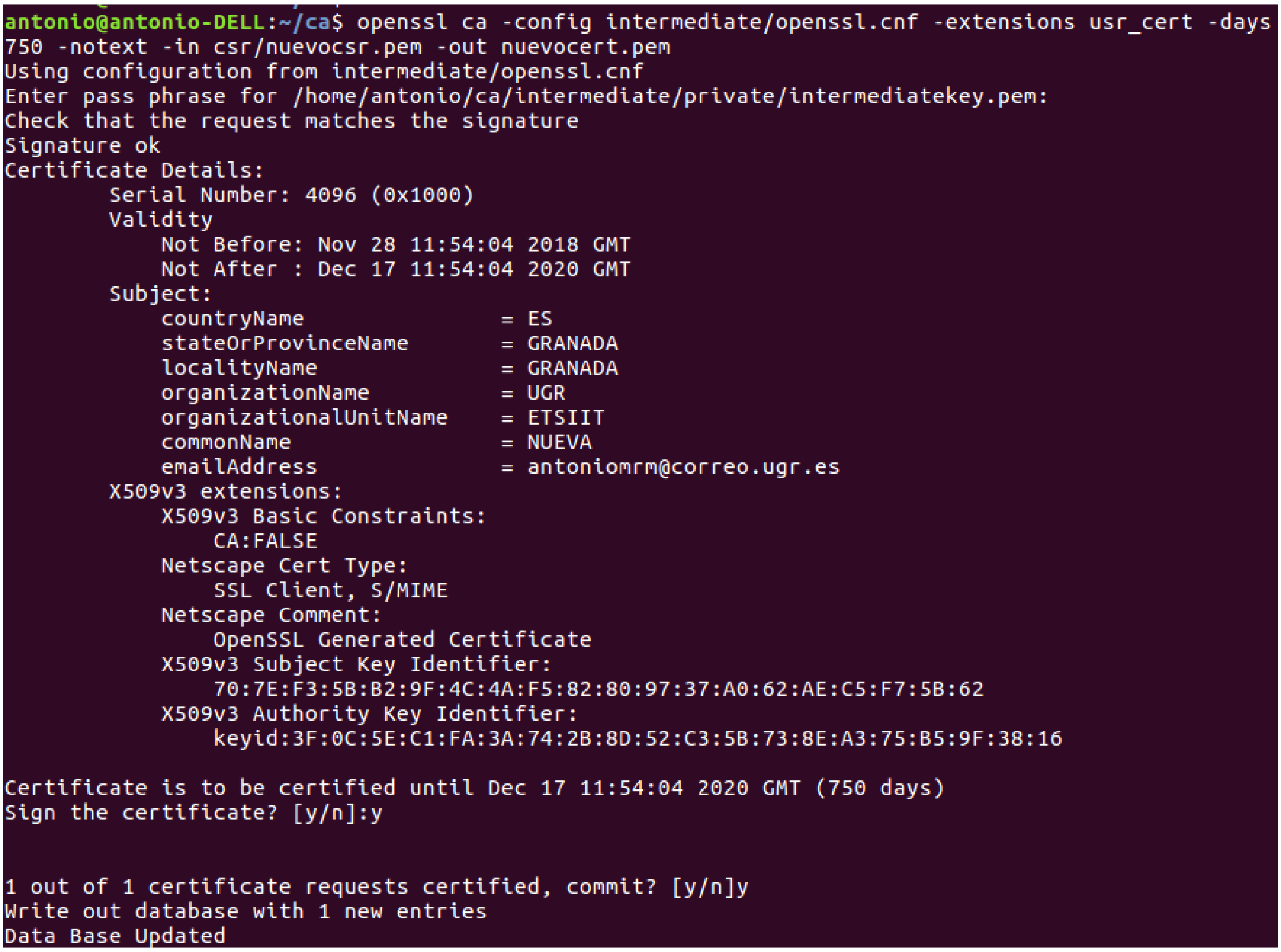


```
antonio@antonio-DELL:~/ca$ openssl req -in csr/nuevocsr.pem -text -verify -noout

verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=ES, ST=GRANADA, L=GRANADA, O=UGR, OU=ETSIIT, CN=NUEVA/emailAd
dress=antoniomrm@correo.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:e7:41:8c:70:98:4b:15:47:1f:5f:29:84:5e:e6:
                    03:80:37:d6:5e:ca:92:32:0e:2f:84:35:85:b7:3e:
                    32:17:82:60:e0:22:17:35:07:1f:81:79:9d:8e:ea:
                    b3:df:0f:1b:62:83:69:2c:fa:4a:58:71:92:fa:60:
                    a7:c7:f3:af:9b:40:72:62:5b:33:d6:b5:67:41:b7:
                    20:d7:44:b1:73:82:e6:37:65:dc:a2:e6:9c:aa:3f:
                    d3:37:56:47:f6:5f:36:4d:f1:9e:75:bd:02:14:a8:
                    9f:2d:c8:57:ab:bf:d1:93:4c:a3:e0:ae:e4:1d:fb:
                    79:03:15:20:83:ef:e3:83:ed:10:aa:c4:d1:07:b5:
                    2e:55:63:a3:35:33:8c:5a:13:3b:0a:59:50:e2:0f:
                    cc:ae:f8:af:db:8f:70:46:44:06:af:80:c6:13:a0:
                    9c:98:a4:41:f5:a6:53:da:d2:b8:b3:d1:d2:ec:cb:
                    1c:4d:4d:76:f1:5b:8c:e8:c5:3b:72:0f:e7:89:79:
                    4d:a0:ec:76:17:05:98:a0:fc:15:5c:8e:3b:78:bf:
                    73:b4:3e:dc:ff:b3:18:d6:a7:d2:05:5a:f6:9a:27:
                    a8:bc:9f:5f:91:15:98:b8:92:df:4f:25:e6:e3:a7:
                    c0:cd:67:c5:b1:2b:4e:e6:3d:c1:a0:5e:1b:35:ef:
                    02:e4:99:5e:ba:27:ea:46:3c:4c:66:ac:59:ff:01:
                    85:d9:74:2a:65:9e:d1:a5:75:be:93:bb:2c:4c:76:
                    20:91:17:3c:84:5a:52:96:4b:da:2d:d1:bf:13:03:
                    bf:53:5f:93:02:d4:55:f1:8d:85:07:b1:39:ac:41:
                    59:ca:ce:63:df:9b:f8:0d:95:92:10:8b:2c:27:41:
                    11:b2:21:46:16:01:cf:f4:54:74:e6:81:d6:c6:f9:
                    2a:c5:33:91:0e:f7:63:ed:23:66:f3:c4:50:55:df:
                    ab:cb:0c:d5:d8:ef:67:11:5d:ac:f5:4f:c1:0e:18:
                    f5:bc:f6:35:8c:75:c5:0c:56:07:e6:8e:27:ff:6d:
                    b9:ff:24:c8:01:52:18:b9:55:47:db:0b:1b:af:a4:
                    31:92:88:42:c5:5b:68:6f:8f:1c:87:a1:23:9b:11:
                    57:f9:95:54:82:d7:ad:fc:e5:74:71:65:c2:69:a5:
                    08:d2:8d:36:41:4e:79:e9:03:be:b4:14:5f:44:35:
                    49:22:b3:47:8c:52:fc:d0:70:8b:2f:74:fb:35:39:
                    2c:8e:fc:c1:74:98:e6:98:58:59:40:30:ff:1a:c1:
                    18:ff:aa:9c:8b:1b:6f:44:7e:0e:85:65:43:94:0f:
                    57:87:80:00:34:84:f9:ee:59:47:d2:84:44:1e:38:
                    3c:18:a5
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         04:00:7e:49:d5:68:bc:23:ea:00:bc:13:99:e5:cf:ac:39:58:
         19:d4:fb:c4:b5:2d:16:27:9c:7e:83:36:cc:ba:43:a8:e5:8b:
         a9:05:41:42:07:e5:a5:f0:63:dd:1d:f4:8c:de:a8:d4:79:d1:
```

4. Cread un certicado para la solicitud anterior empleando la CA subordinada. Mostrad el archivo y sus valores.

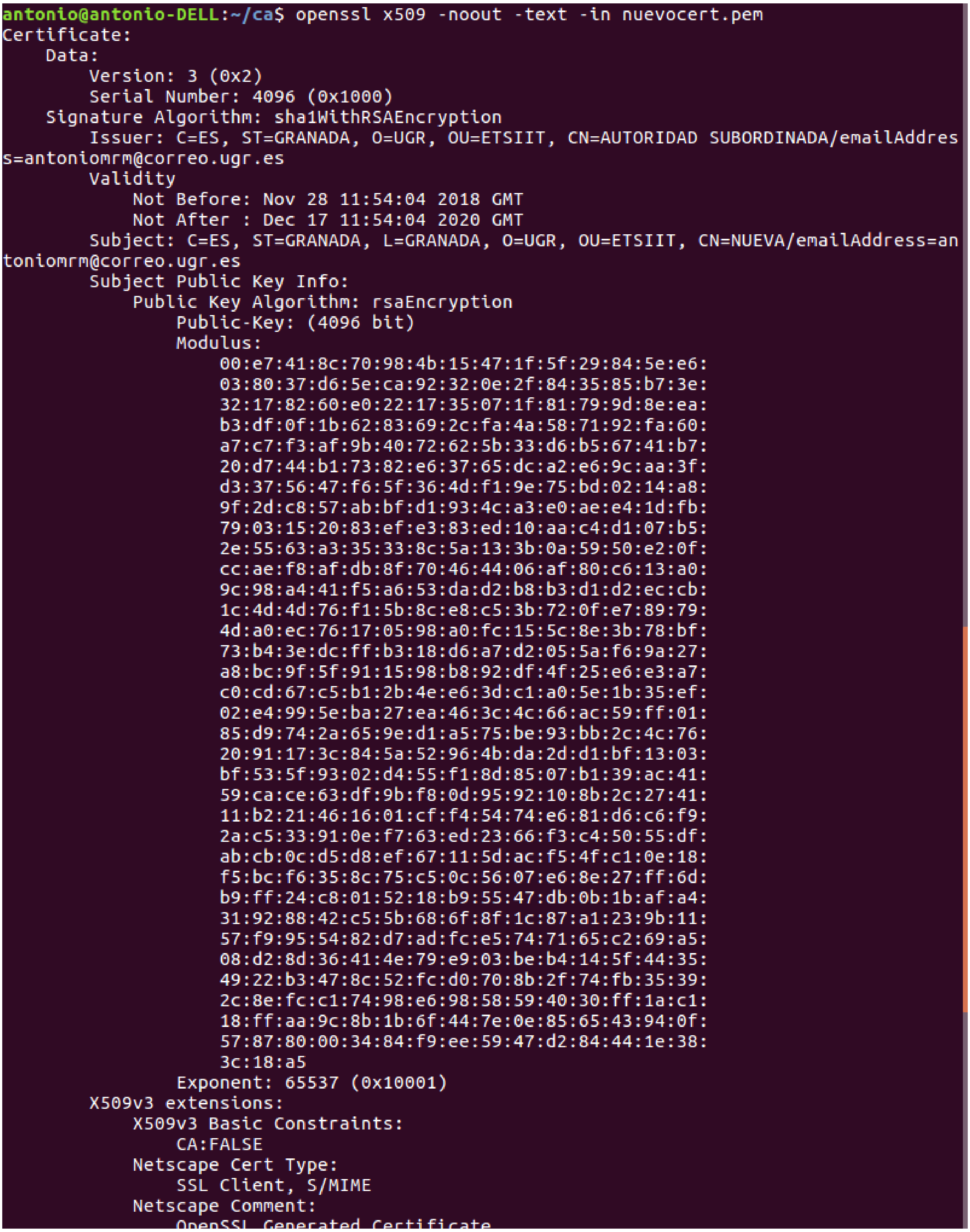
Como hicimos antes con la CA raíz, ahora nos tocará firmar con la CA subordinada en nombre de la raíz.

Usaremos el comando de openssl ca. Como antes le pasamos el archivo de configuración con la opcion -config, muy importante pasarle la de CA Subordinada.
La extesión con -extension, esta vez será usr_cert que indica que será emitido para un usuario y el tiempo antes de que expire con -days.
Después le pasaremos la solicitud de certificado a firmar y el nombre del certificado final firmado.



```
antonio@antonio-DELL:~/ca$ openssl ca -config intermediate/openssl.cnf -extensions usr_cert -days
750 -notext -in csr/nuevocsr.pem -out nuevocert.pem
Using configuration from intermediate/openssl.cnf
Enter pass phrase for /home/antonio/ca/intermediate/private/intermediatekey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Nov 28 11:54:04 2018 GMT
            Not After : Dec 17 11:54:04 2020 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = GRANADA
            localityName              = GRANADA
            organizationName          = UGR
            organizationalUnitName    = ETSIIT
            commonName                = NUEVA
            emailAddress              = antoniomrm@correo.ugr.es
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                70:7E:F3:5B:B2:9F:4C:4A:F5:82:80:97:37:A0:62:AE:C5:F7:5B:62
            X509v3 Authority Key Identifier:
                keyid:3F:0C:5E:C1:FA:3A:74:2B:8D:52:C3:5B:73:8E:A3:75:B5:9F:38:16

Certificate is to be certified until Dec 17 11:54:04 2020 GMT (750 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
```

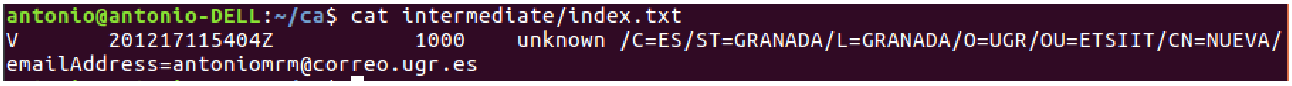
A continuación vamos a ver algo de información del nuevo certificado.



```
antonio@antonio-DELL:~/ca$ openssl x509 -noout -text -in nuevocert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=ES, ST=GRANADA, O=UGR, OU=ETSIIT, CN=AUTORIDAD SUBORDINADA/emailAddres
s=antoniomrm@correo.ugr.es
        Validity
            Not Before: Nov 28 11:54:04 2018 GMT
            Not After : Dec 17 11:54:04 2020 GMT
        Subject: C=ES, ST=GRANADA, L=GRANADA, O=UGR, OU=ETSIIT, CN=NUEVA/emailAddress=an
toniomrm@correo.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:e7:41:8c:70:98:4b:15:47:1f:5f:29:84:5e:e6:
                    03:80:37:d6:5e:ca:92:32:0e:2f:84:35:85:b7:3e:
                    32:17:82:60:e0:22:17:35:07:1f:81:79:9d:8e:ea:
                    b3:df:0f:1b:62:83:69:2c:fa:4a:58:71:92:fa:60:
                    a7:c7:f3:af:9b:40:72:62:5b:33:d6:b5:67:41:b7:
                    20:d7:44:b1:73:82:e6:37:65:dc:a2:e6:9c:aa:3f:
                    d3:37:56:47:f6:5f:36:4d:f1:9e:75:bd:02:14:a8:
                    9f:2d:c8:57:ab:bf:d1:93:4c:a3:e0:ae:e4:1d:fb:
                    79:03:15:20:83:ef:e3:83:ed:10:aa:c4:d1:07:b5:
                    2e:55:63:a3:35:33:8c:5a:13:3b:0a:59:50:e2:0f:
                    cc:ae:f8:af:db:8f:70:46:44:06:af:80:c6:13:a0:
                    9c:98:a4:41:f5:a6:53:da:d2:b8:b3:d1:d2:ec:cb:
                    1c:4d:4d:76:f1:5b:8c:e8:c5:3b:72:0f:e7:89:79:
                    4d:a0:ec:76:17:05:98:a0:fc:15:5c:8e:3b:78:bf:
                    73:b4:3e:dc:ff:b3:18:d6:a7:d2:05:5a:f6:9a:27:
                    a8:bc:9f:5f:91:15:98:b8:92:df:4f:25:e6:e3:a7:
                    c0:cd:67:c5:b1:2b:4e:e6:3d:c1:a0:5e:1b:35:ef:
                    02:e4:99:5e:ba:27:ea:46:3c:4c:66:ac:59:ff:01:
                    85:d9:74:2a:65:9e:d1:a5:75:be:93:bb:2c:4c:76:
                    20:91:17:3c:84:5a:52:96:4b:da:2d:d1:bf:13:03:
                    bf:53:5f:93:02:d4:55:f1:8d:85:07:b1:39:ac:41:
                    59:ca:ce:63:df:9b:f8:0d:95:92:10:8b:2c:27:41:
                    11:b2:21:46:16:01:cf:f4:54:74:e6:81:d6:c6:f9:
                    2a:c5:33:91:0e:f7:63:ed:23:66:f3:c4:50:55:df:
                    ab:cb:0c:d5:d8:ef:67:11:5d:ac:f5:4f:c1:0e:18:
                    f5:bc:f6:35:8c:75:c5:0c:56:07:e6:8e:27:ff:6d:
                    b9:ff:24:c8:01:52:18:b9:55:47:db:0b:1b:af:a4:
                    31:92:88:42:c5:5b:68:6f:8f:1c:87:a1:23:9b:11:
                    57:f9:95:54:82:d7:ad:fc:e5:74:71:65:c2:69:a5:
                    08:d2:8d:36:41:4e:79:e9:03:be:b4:14:5f:44:35:
                    49:22:b3:47:8c:52:fc:d0:70:8b:2f:74:fb:35:39:
                    2c:8e:fc:c1:74:98:e6:98:58:59:40:30:ff:1a:c1:
                    18:ff:aa:9c:8b:1b:6f:44:7e:0e:85:65:43:94:0f:
                    57:87:80:00:34:84:f9:ee:59:47:d2:84:44:1e:38:
                    3c:18:a5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: 
                CA:FALSE
            Netscape Cert Type: 
                SSL Client, S/MIME
            Netscape Comment: 
                OpenSSL Generated Certificate
```

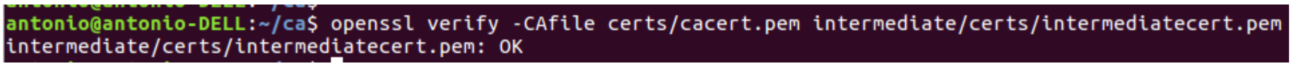
Como vemos ahora el emisor es la autoridad subordinada.

Vemos en index.txt de la CA intermedia para mirar la firma emitida.



```
antonio@antonio-DELL:~/ca$ cat intermediate/index.txt
V       201217115404Z           1000    unknown /C=ES/ST=GRANADA/L=GRANADA/O=UGR/OU=ETSIIT/CN=NUEVA/
emailAddress=antoniomrm@correo.ugr.es
```

Para verificar el certificado de la CA subordinada con el de la CA raíz:

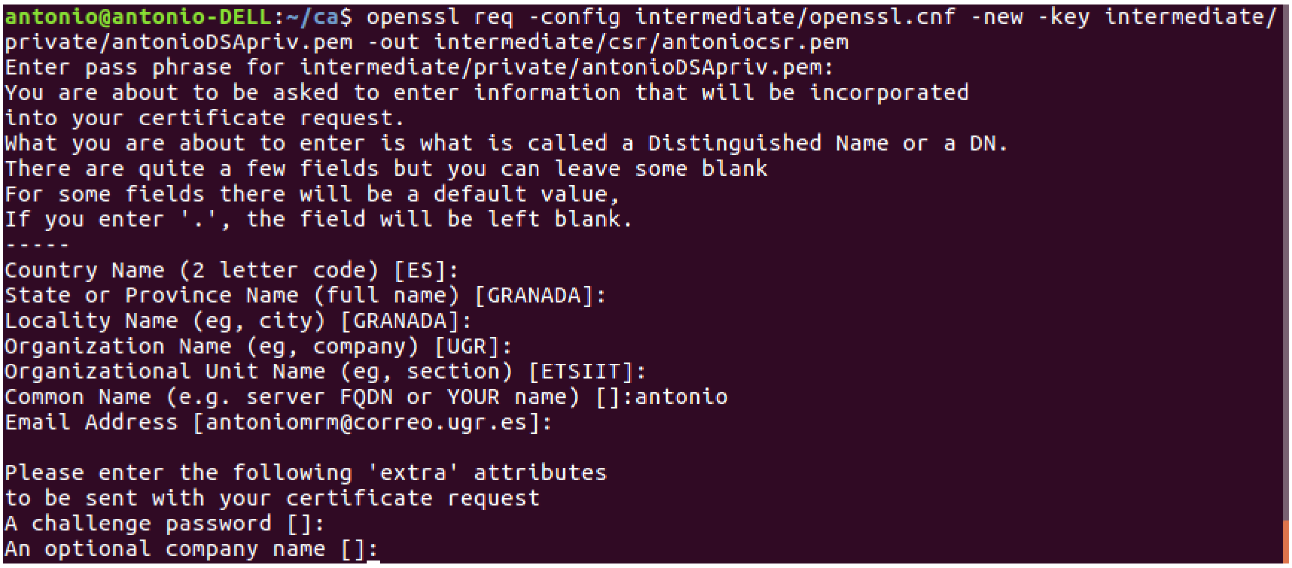


```
antonio@antonio-DELL:~/ca$ openssl verify -CAfile certs/cacert.pem intermediate/certs/intermediatecert.pem
intermediate/certs/intermediatecert.pem: OK
```

La validación es correcta, esto indica que la cadena de confianza está intacta.

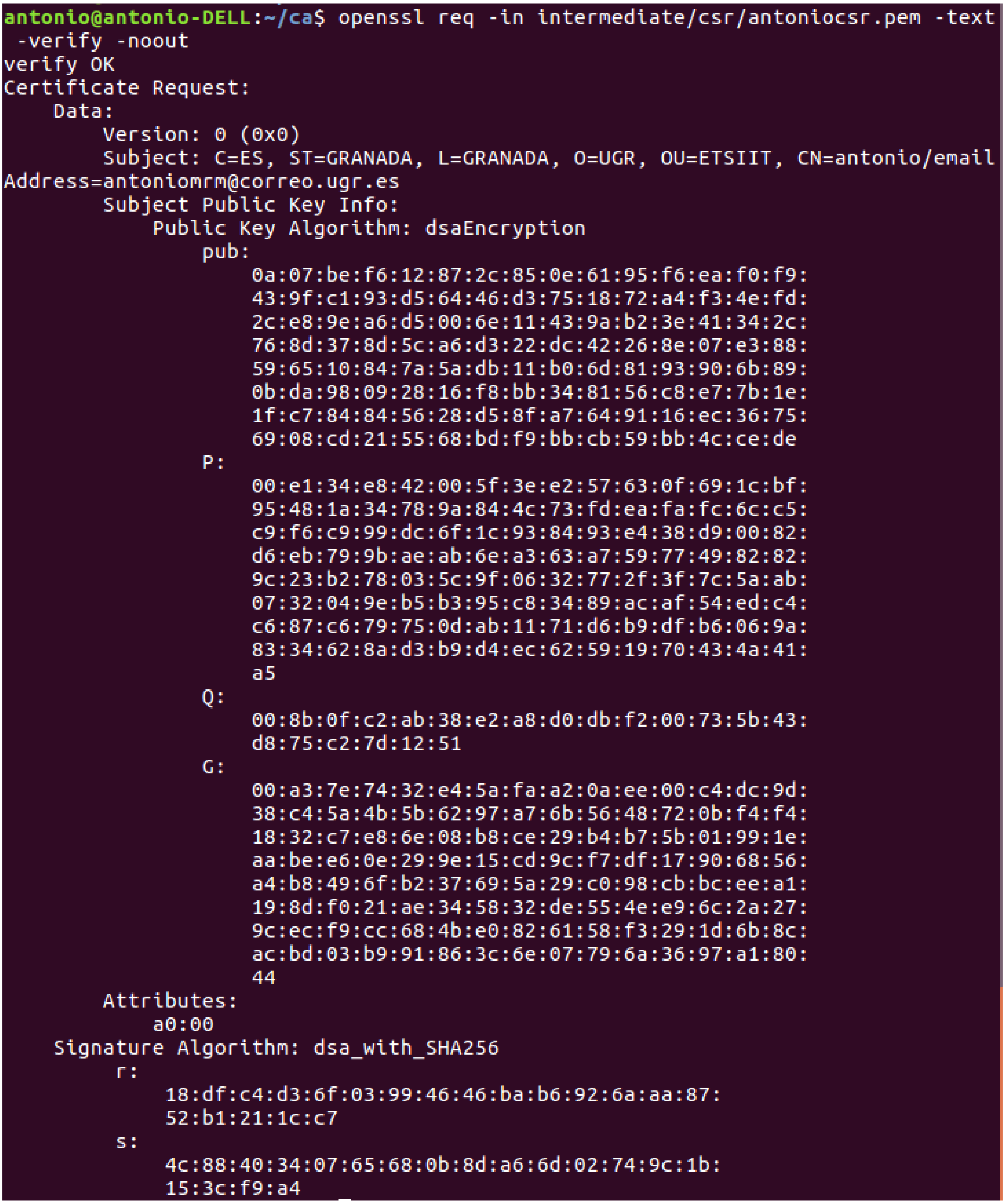
5. Cread una solicitud de certicado para cualquiera de las claves que habeis generado en las practicas anteriores, excepto las RSA. Mostrad el archivo y el valor de la solicitud.

Creamos la solicitud de certificado con req pasandole el archivo openssl.cnf de la subordinada y la clave privada DSA de la práctica anterior.



```
antonio@antonio-DELL:~/ca$ openssl req -config intermediate/openssl.cnf -new -key intermediate/
private/antonioDSApriv.pem -out intermediate/csr/antoniocsr.pem
Enter pass phrase for intermediate/private/antonioDSApriv.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 (full name) [GRANADA]:
Locality Name (eg, city) [GRANADA]:
Organization Name (eg, company) [UGR]:
Organizational Unit Name (eg, section) [ETSIIT]:
Common Name (e.g. server FQDN or YOUR name) []:antonio
Email Address [antoniomrm@correo.ugr.es]:

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

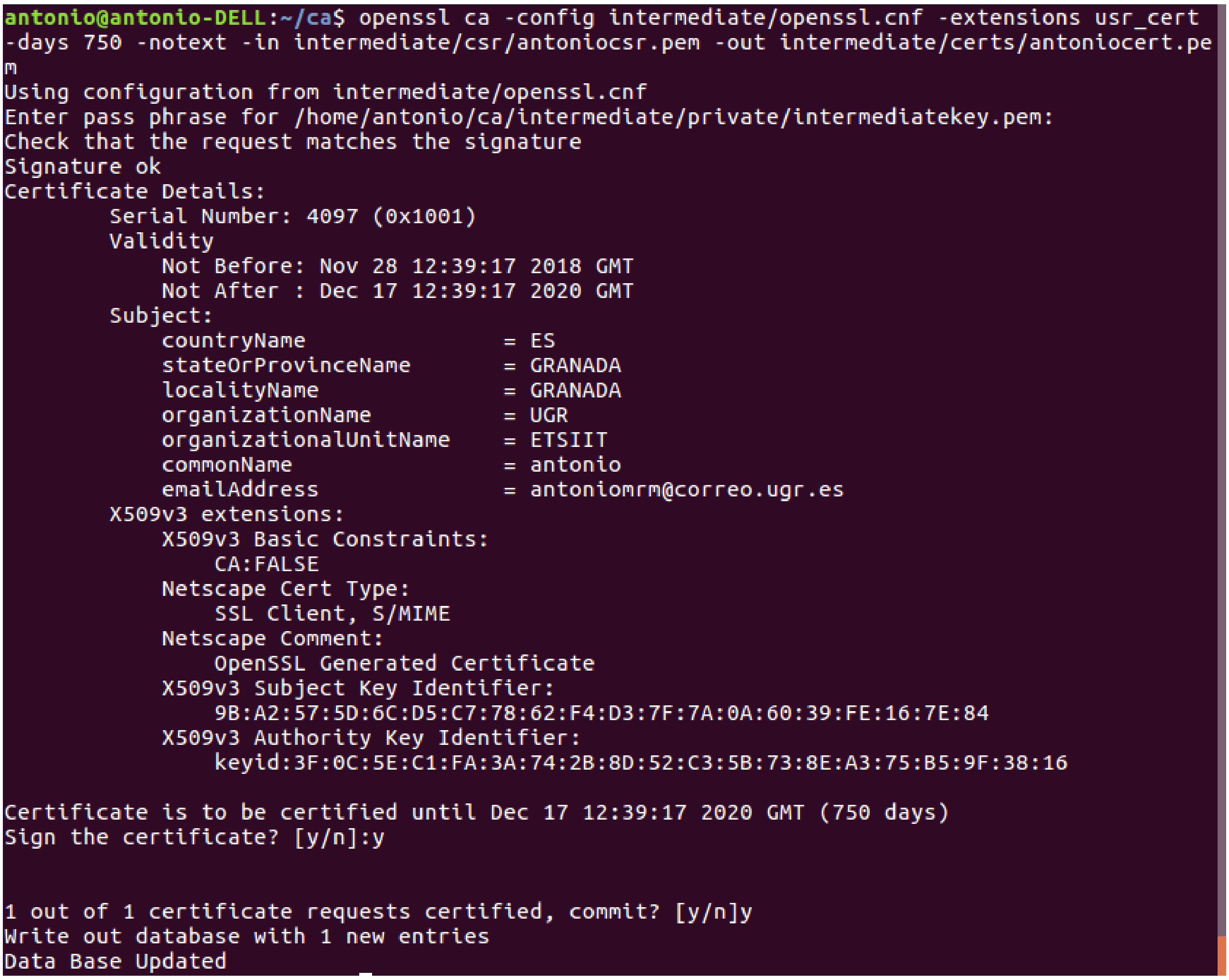
Vemos mas información de la solicitud de firma del certificado y sus atributos.



```
antonio@antonio-DELL:~/ca$ openssl req -in intermediate/csr/antoniocsr.pem -text
 -verify -noout
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=ES, ST=GRANADA, L=GRANADA, O=UGR, OU=ETSIIT, CN=antonio/email
Address=antoniomrm@correo.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: dsaEncryption
                pub:
                    0a:07:be:f6:12:87:2c:85:0e:61:95:f6:ea:f0:f9:
                    43:9f:c1:93:d5:64:46:d3:75:18:72:a4:f3:4e:fd:
                    2c:e8:9e:a6:d5:00:6e:11:43:9a:b2:3e:41:34:2c:
                    76:8d:37:8d:5c:a6:d3:22:dc:42:26:8e:07:e3:88:
                    59:65:10:84:7a:5a:db:11:b0:6d:81:93:90:6b:89:
                    0b:da:98:09:28:16:f8:bb:34:81:56:c8:e7:7b:1e:
                    1f:c7:84:84:56:28:d5:8f:a7:64:91:16:ec:36:75:
                    69:08:cd:21:55:68:bd:f9:bb:cb:59:bb:4c:ce:de
                P:
                    00:e1:34:e8:42:00:5f:3e:e2:57:63:0f:69:1c:bf:
                    95:48:1a:34:78:9a:84:4c:73:fd:ea:fa:fc:6c:c5:
                    c9:f6:c9:99:dc:6f:1c:93:84:93:e4:38:d9:00:82:
                    d6:eb:79:9b:ae:ab:6e:a3:63:a7:59:77:49:82:82:
                    9c:23:b2:78:03:5c:9f:06:32:77:2f:3f:7c:5a:ab:
                    07:32:04:9e:b5:b3:95:c8:34:89:ac:af:54:ed:c4:
                    c6:87:c6:79:75:0d:ab:11:71:d6:b9:df:b6:06:9a:
                    83:34:62:8a:d3:b9:d4:ec:62:59:19:70:43:4a:41:
                    a5
                Q:
                    00:8b:0f:c2:ab:38:e2:a8:d0:db:f2:00:73:5b:43:
                    d8:75:c2:7d:12:51
                G:
                    00:a3:7e:74:32:e4:5a:fa:a2:0a:ee:00:c4:dc:9d:
                    38:c4:5a:4b:5b:62:97:a7:6b:56:48:72:0b:f4:f4:
                    18:32:c7:e8:6e:08:b8:ce:29:b4:b7:5b:01:99:1e:
                    aa:be:e6:0e:29:9e:15:cd:9c:f7:df:17:90:68:56:
                    a4:b8:49:6f:b2:37:69:5a:29:c0:98:cb:bc:ee:a1:
                    19:8d:f0:21:ae:34:58:32:de:55:4e:e9:6c:2a:27:
                    9c:ec:f9:cc:68:4b:e0:82:61:58:f3:29:1d:6b:8c:
                    ac:bd:03:b9:91:86:3c:6e:07:79:6a:36:97:a1:80:
                    44
        Attributes:
            a0:00
    Signature Algorithm: dsa_with_SHA256
         r:
             18:df:c4:d3:6f:03:99:46:46:ba:b6:92:6a:aa:87:
             52:b1:21:1c:c7
         s:
             4c:88:40:34:07:65:68:0b:8d:a6:6d:02:74:9c:1b:
             15:3c:f9:a4
```

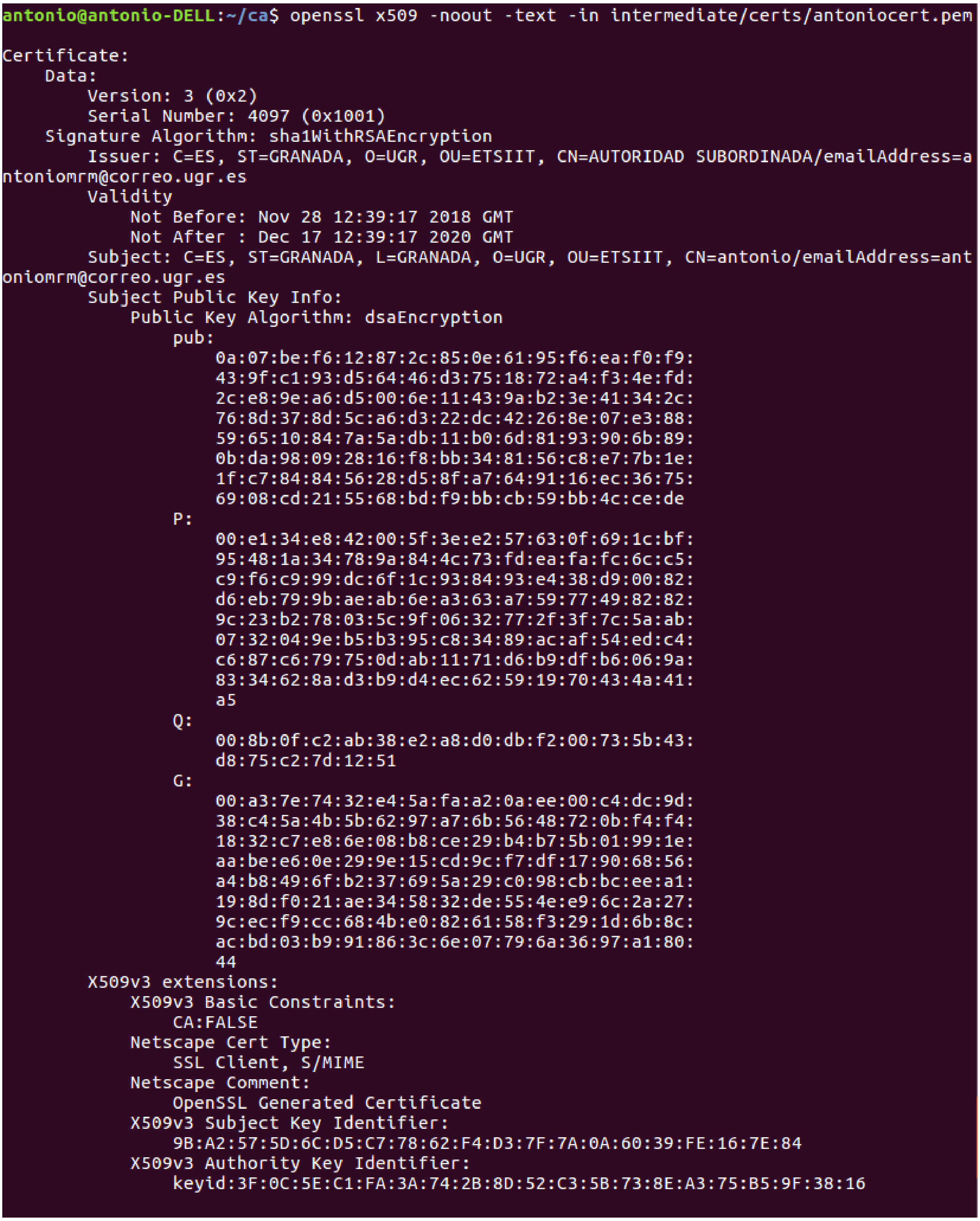
6. Cread un certicado para la solicitud anterior utilizando la CA subordinada. Mostrad el archivo y los valores del certicado

Usaremos el comando de openssl ca. Utilizaremos las mismas opciones que usamos en la pregunta 4.



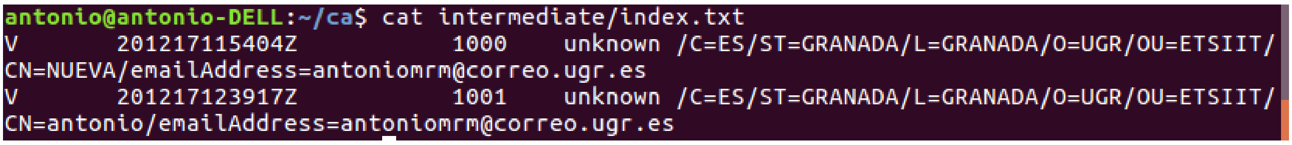
```
antonio@antonio-DELL:~/ca$ openssl ca -config intermediate/openssl.cnf -extensions usr_cert
-days 750 -notext -in intermediate/csr/antoniocsr.pem -out intermediate/certs/antoniocert.pe
m
Using configuration from intermediate/openssl.cnf
Enter pass phrase for /home/antonio/ca/intermediate/private/intermediatekey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Nov 28 12:39:17 2018 GMT
            Not After : Dec 17 12:39:17 2020 GMT
        Subject:
            countryName               = ES
            stateOrProvinceName       = GRANADA
            localityName              = GRANADA
            organizationName          = UGR
            organizationalUnitName    = ETSIIT
            commonName                = antonio
            emailAddress              = antoniomrm@correo.ugr.es
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                9B:A2:57:5D:6C:D5:C7:78:62:F4:D3:7F:7A:0A:60:39:FE:16:7E:84
            X509v3 Authority Key Identifier:
                keyid:3F:0C:5E:C1:FA:3A:74:2B:8D:52:C3:5B:73:8E:A3:75:B5:9F:38:16

Certificate is to be certified until Dec 17 12:39:17 2020 GMT (750 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
```

De nuevo vemos en detalle algunos datos del certificado emitido por la CA subordinada.



```
antonio@antonio-DELL:~/ca$ openssl x509 -noout -text -in intermediate/certs/antoniocert.pem

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4097 (0x1001)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=ES, ST=GRANADA, O=UGR, OU=ETSIIT, CN=AUTORIDAD SUBORDINADA/emailAddress=a
ntoniomrm@correo.ugr.es
        Validity
            Not Before: Nov 28 12:39:17 2018 GMT
            Not After : Dec 17 12:39:17 2020 GMT
        Subject: C=ES, ST=GRANADA, L=GRANADA, O=UGR, OU=ETSIIT, CN=antonio/emailAddress=ant
oniomrm@correo.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: dsaEncryption
                pub:
                    0a:07:be:f6:12:87:2c:85:0e:61:95:f6:ea:f0:f9:
                    43:9f:c1:93:d5:64:46:d3:75:18:72:a4:f3:4e:fd:
                    2c:e8:9e:a6:d5:00:6e:11:43:9a:b2:3e:41:34:2c:
                    76:8d:37:8d:5c:a6:d3:22:dc:42:26:8e:07:e3:88:
                    59:65:10:84:7a:5a:db:11:b0:6d:81:93:90:6b:89:
                    0b:da:98:09:28:16:f8:bb:34:81:56:c8:e7:7b:1e:
                    1f:c7:84:84:56:28:d5:8f:a7:64:91:16:ec:36:75:
                    69:08:cd:21:55:68:bd:f9:bb:cb:59:bb:4c:ce:de
                P:
                    00:e1:34:e8:42:00:5f:3e:e2:57:63:0f:69:1c:bf:
                    95:48:1a:34:78:9a:84:4c:73:fd:ea:fa:fc:6c:c5:
                    c9:f6:c9:99:dc:6f:1c:93:84:93:e4:38:d9:00:82:
                    d6:eb:79:9b:ae:ab:6e:a3:63:a7:59:77:49:82:82:
                    9c:23:b2:78:03:5c:9f:06:32:77:2f:3f:7c:5a:ab:
                    07:32:04:9e:b5:b3:95:c8:34:89:ac:af:54:ed:c4:
                    c6:87:c6:79:75:0d:ab:11:71:d6:b9:df:b6:06:9a:
                    83:34:62:8a:d3:b9:d4:ec:62:59:19:70:43:4a:41:
                    a5
                Q:
                    00:8b:0f:c2:ab:38:e2:a8:d0:db:f2:00:73:5b:43:
                    d8:75:c2:7d:12:51
                G:
                    00:a3:7e:74:32:e4:5a:fa:a2:0a:ee:00:c4:dc:9d:
                    38:c4:5a:4b:5b:62:97:a7:6b:56:48:72:0b:f4:f4:
                    18:32:c7:e8:6e:08:b8:ce:29:b4:b7:5b:01:99:1e:
                    aa:be:e6:0e:29:9e:15:cd:9c:f7:df:17:90:68:56:
                    a4:b8:49:6f:b2:37:69:5a:29:c0:98:cb:bc:ee:a1:
                    19:8d:f0:21:ae:34:58:32:de:55:4e:e9:6c:2a:27:
                    9c:ec:f9:cc:68:4b:e0:82:61:58:f3:29:1d:6b:8c:
                    ac:bd:03:b9:91:86:3c:6e:07:79:6a:36:97:a1:80:
                    44
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                9B:A2:57:5D:6C:D5:C7:78:62:F4:D3:7F:7A:0A:60:39:FE:16:7E:84
            X509v3 Authority Key Identifier:
                keyid:3F:0C:5E:C1:FA:3A:74:2B:8D:52:C3:5B:73:8E:A3:75:B5:9F:38:16
```

Finalmente vemos en index.txt de la CA subordinada las firmas emitidas.



```
antonio@antonio-DELL:~/ca$ cat intermediate/index.txt
V       201217115404Z           1000    unknown /C=ES/ST=GRANADA/L=GRANADA/O=UGR/OU=ETSIIT/
CN=NUEVA/emailAddress=antoniomrm@correo.ugr.es
V       201217123917Z           1001    unknown /C=ES/ST=GRANADA/L=GRANADA/O=UGR/OU=ETSIIT/
CN=antonio/emailAddress=antoniomrm@correo.ugr.es
```

Biografia

[1.] Manual de openssl.
https://www.openssl.org/docs/man1.0.2/apps/

[2.] Creación de autoridad certificadora subordinada.
https://jamielinux.com/docs/openssl-certificate-authority/create-the-intermediate-pair.html

[3.] Creación de autoridad certificadora subordinada.
https://www.linuxarena.net/2017/01/06/172/

[4.] Creación de autoridad certificadora raiz.
https://www.linuxarena.net/2017/01/06/openssl-parte-2-creacion-de-una-autoridad-certificadora/