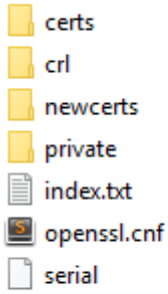
Seguridad y Protección de Sistemas Informáticos Práctica 4

Miguel Morales Castillo

1. Cread una autoridad certificadora. En este caso se premiará el uso de openssl ca frente a CA.pl, aunque este último comando es admisible.

   Para crear la autoridad certificadora primero creamos la estructura de carpetas y archivos siguientes:

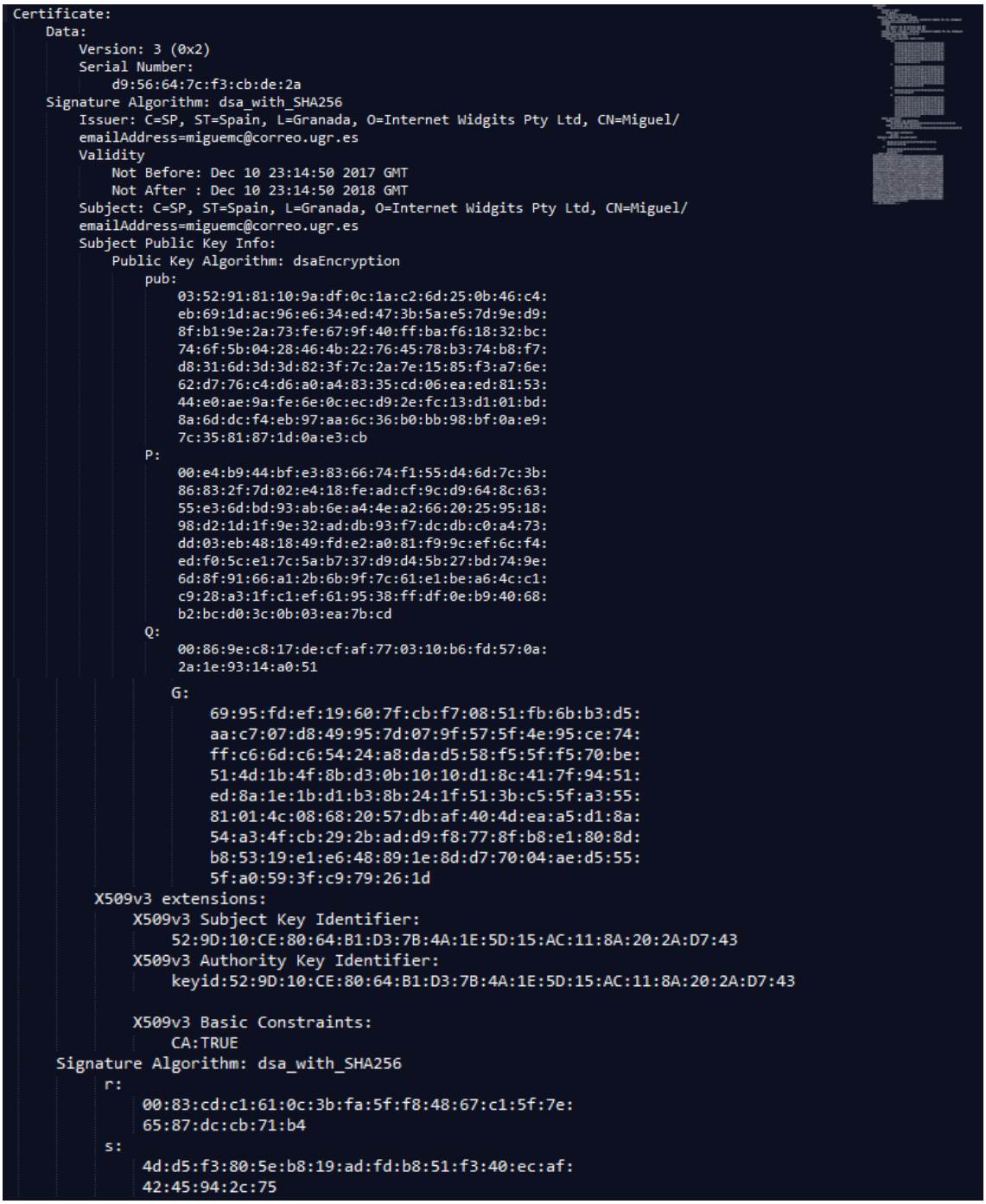


   En cada carpeta se guarda lo que su propio nombre indica intuitivamente. Index.txt llevara un control de las firmas realizadas por la CA y en openssl.cnf se encuentra la configuración de la CA, que hemos modificado del archivo por defecto de OpenSSL para meter nuestros datos y ruta de la CA.

   El certificado raíz de la CA se crea usando el siguiente comando:

```
req -config openssl.cnf \
-key private/ca.key.pem \
-new -x509 -days 365 -sha256 -extensions v3_ca \
-out certs/ca.cert.pem
```

   Como key hemos usado una clave DSA de la práctica 3, la salida es la siguiente:



2. Cread una solicitud de certificado que incluya la generación de claves en la misma.

Para realizar esto, ejecutamos el siguiente comando:

```
openssl req -newkey rsa:1024 -keyout key.pem -out reqRSA.pem
```

Tras rellenar las preguntas del DN, la salida es la siguiente:

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SP, ST=Spain, L=Granada, O=Internet Widgits Pty Ltd, CN=Miguel/
        emailAddress=miguemc@correo.ugr.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:de:9d:9d:61:f1:d2:04:c7:60:3e:34:9f:b3:a9:
                    34:43:ab:5a:d5:4d:df:97:ae:68:61:46:76:03:da:
                    13:4a:d7:b7:9f:1b:8c:36:b8:b7:89:ea:5e:0c:c9:
                    2b:55:0c:47:4e:7a:39:63:40:0e:4d:f9:bd:56:3e:
                    f8:dd:ef:13:8e:52:06:51:87:b9:27:d0:65:09:2a:
                    f0:87:99:f3:3a:35:61:4f:4b:f7:91:f7:ea:5e:98:
                    04:18:36:f4:29:c1:3e:66:80:e9:b5:c3:28:eb:56:
                    01:bd:ab:75:c7:00:88:65:01:93:3a:f9:14:60:52:
                    62:a8:86:29:9c:89:f4:b3:6b
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :0123456789
    Signature Algorithm: sha256WithRSAEncryption
         a5:6a:43:f6:2a:7a:61:0d:aa:85:24:f7:8e:06:d1:49:c1:f8:
         c8:8c:9e:68:1d:a1:a8:94:96:5d:a3:da:f1:2b:65:57:6d:21:
         b3:1b:f1:80:96:30:a4:ed:80:33:31:99:19:e2:e5:db:dd:31:
         33:5e:28:a4:fb:6d:7f:55:14:0c:40:50:60:49:54:0e:6d:6c:
         3e:b9:61:f7:fc:07:af:8a:23:83:fc:f6:74:ac:49:86:d3:c8:
         66:18:70:f0:4e:5f:c0:09:91:f8:73:bb:a4:66:78:fb:57:11:
         d6:f0:88:51:22:a0:bb:ca:27:66:b2:27:e3:27:38:45:99:e7:
         c7:ce
```

3. Cread un certificado para la solicitud anterior empleando la CA creada en el primer punto

   Para este apartado, lo que nos pide es que nuestra CA firme la solicitud, esto se hace de la siguiente forma:

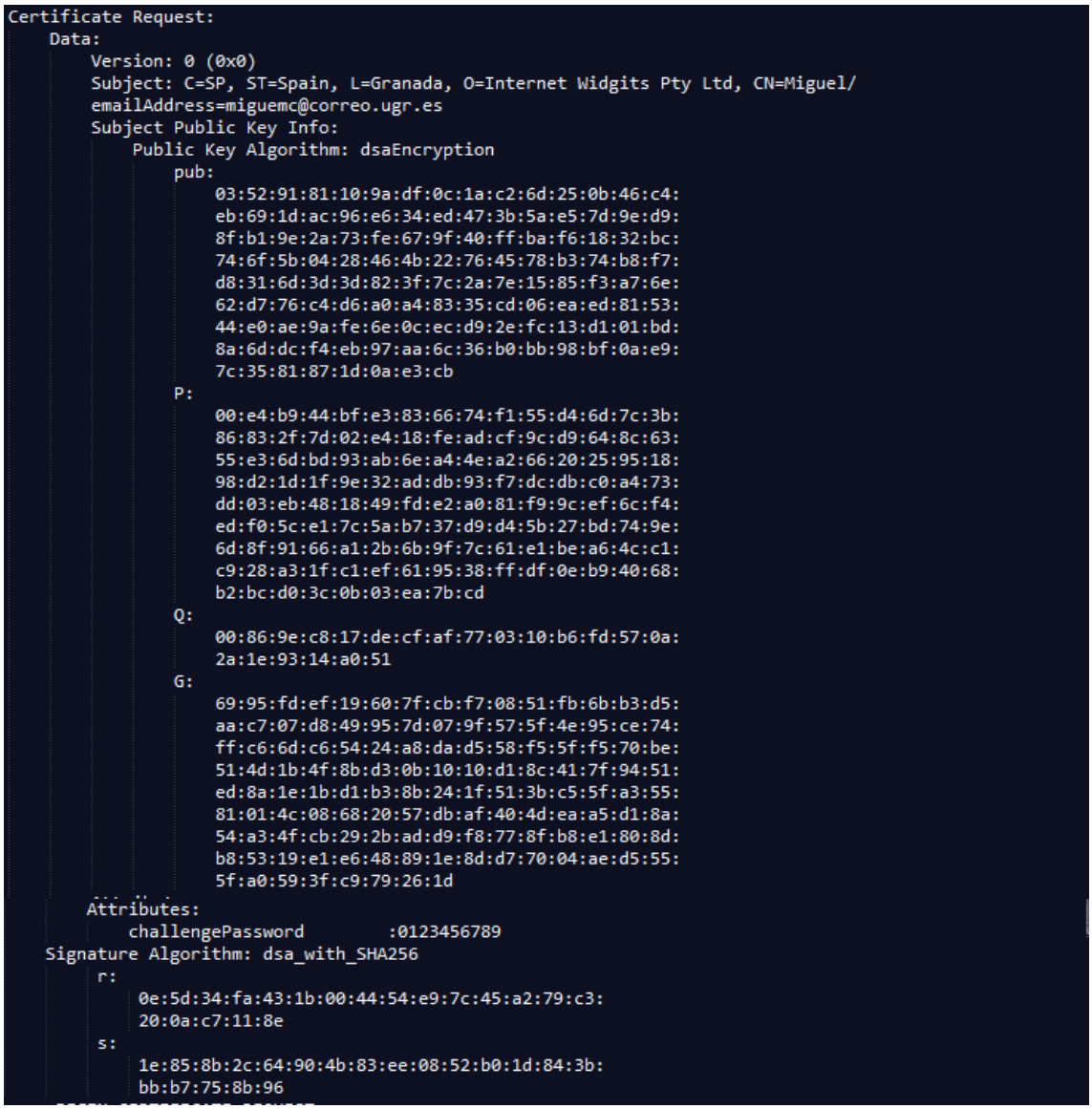
```
OpenSSL> ca -config "C:\Users\Miguemc\Desktop\ca\openssl.cnf" -in  "C:\Users\Miguemc\
Desktop\ca\reqRSA.pem" -out "C:\Users\Miguemc\Desktop\ca\certs\newcertRSA.pem"
Using configuration from C:\Users\Miguemc\Desktop\ca\openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Dec 10 23:20:10 2017 GMT
            Not After : Dec 10 23:20:10 2018 GMT
        Subject:
            countryName               = SP
            stateOrProvinceName       = Spain
            organizationName          = Internet Widgits Pty Ltd
            commonName                = Miguel
            emailAddress              = miguemc@correo.ugr.es
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                E6:0D:A5:0E:36:11:12:50:90:4C:7B:87:A4:14:26:92:AA:94:26:8A
            X509v3 Authority Key Identifier:
                keyid:52:9D:10:CE:80:64:B1:D3:7B:4A:1E:5D:15:AC:11:8A:20:2A:D7:43

Certificate is to be certified until Dec 10 23:20:10 2018 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
OpenSSL>
```

4. Cread una solicitud de certificado para cualquiera de las claves que habéis generado en las prácticas anteriores, excepto las RSA.

Repetimos el proceso del apartado 2 pero cambiando el flag correspondiente a la key. La key usada es miguelDSA.pem de la práctica 3, el comando quedaría así:

openssl req -config openssl.cnf –key miguelDSA.pem -text -new -out req.pem

La salida producida es la siguiente:



5. Cread un certificado para la solicitud anterior utilizando la CA creada.

Repetimos el proceso del apartado 3.

```
OpenSSL> ca -config "C:\Users\Miguemc\Desktop\ca\openssl.cnf" -in  "C:\Users\Miguemc\
Desktop\ca\req.pem" -out "C:\Users\Miguemc\Desktop\ca\certs\newcert.pem"
Using configuration from C:\Users\Miguemc\Desktop\ca\openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Dec 10 23:15:17 2017 GMT
            Not After : Dec 10 23:15:17 2018 GMT
        Subject:
            countryName               = SP
            stateOrProvinceName       = Spain
            organizationName          = Internet Widgits Pty Ltd
            commonName                = Miguel
            emailAddress              = miguemc@correo.ugr.es
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                52:9D:10:CE:80:64:B1:D3:7B:4A:1E:5D:15:AC:11:8A:20:2A:D7:43
            X509v3 Authority Key Identifier:
                keyid:52:9D:10:CE:80:64:B1:D3:7B:4A:1E:5D:15:AC:11:8A:20:2A:D7:43

Certificate is to be certified until Dec 10 23:15:17 2018 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
OpenSSL>
```