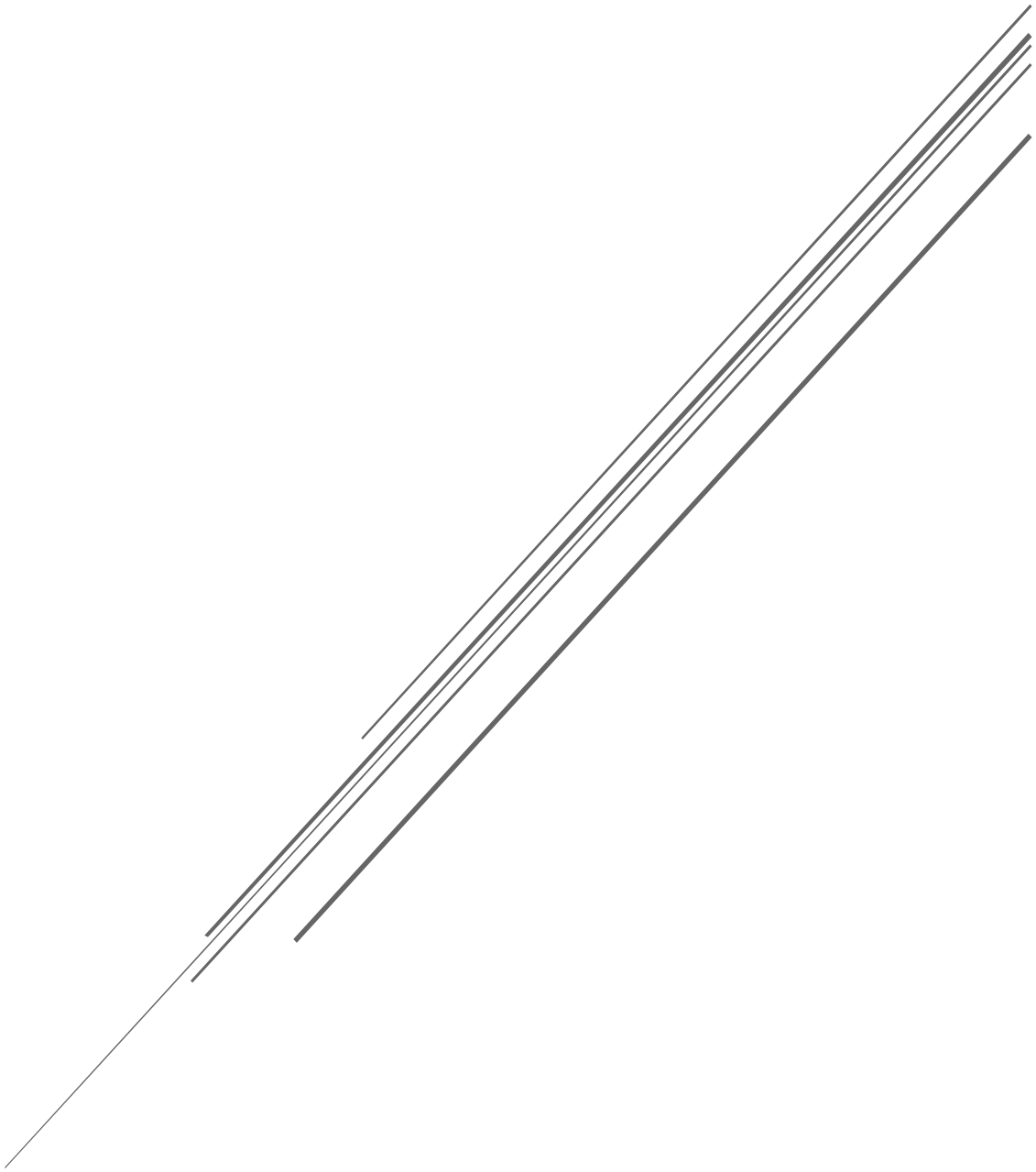
ACTIVIDAD 7: CREACIÓN DE CERTIFICADOS CON OPENSSL

Seguridad Informática



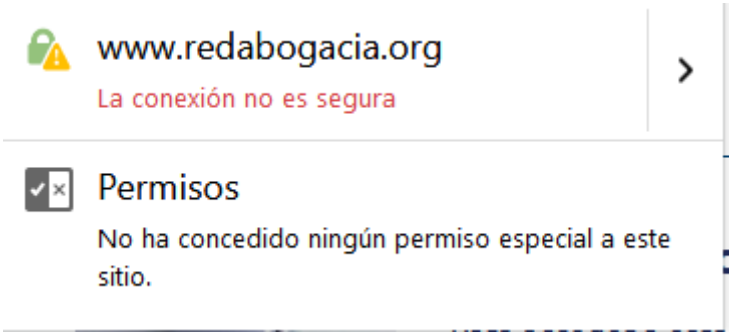
Escuela Técnica Superior de Ingeniería
Grado en Ingeniería Informática

CONTENIDO

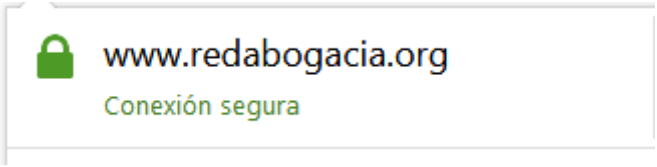
1. CERTIFICADOS DIGITALES Y CERTIFICADOS RAÍZ

Para empezar la sesión, se ha accedido a través de Firefox al sitio web de la Abogacía Española. Una vez allí, se ha procedido a acceder a "Acceso a servicios con certificado ACA". Sin embargo, se produjo un error debido a una mala configuración por parte del propietario de www.redabogacia.org, ya que utiliza un certificado de seguridad no válido, debido a que el emisor era desconocido para el navegador, lo que causaba que la conexión no fuera segura. Para arreglarlo, se decidió añadir una excepción de seguridad con el certificado.

A continuación, se procedió a buscar el certificado añadido a través del administrador de certificados. El certificado se encontró en el apartado de *servidores*. Este certificado permite mantener comunicación cifrada y garantiza que no puedan acceder terceros a la información. Sin embargo, puesto que es una excepción añadida por el usuario, el navegador sigue avisando de que la conexión no es segura:



A continuación, se eliminó el servició de servidor y se instaló el certificador raíz de la autoridad certificadora. Al acceder de nuevo a los servicios telemáticos, el mensaje de aviso de seguridad desapareció:



Sin embargo, aún el acceso al sitio web siguió sin ser posible, puesto que para ello es necesario presentar certificado de cliente.

A continuación, se verificaron las propiedades de la conexión SSL, identificando los algoritmos de cifrado simétrico y asimétrico y las funciones hash. El cifrado simétrico es 3DES EDE CBC, con claves de 112 bits, el cifrado asimétrico se consigue con RSA y la función hash utilizada SHA256. Este certificado está emitido por:

Nombre común	ACA CA3
Organización	CONSEJO GENERAL DE LA ABOGACIA
Unidad Organizativa	AUTORIDAD DE CERTIFICACION DE LA ABOGACIA

Se observó el valor del campo que hacía referencia a los puntos de distribución de CRL, tenía el siguiente contenido:

```
No es crítico
URI: http://www.acabogacia.org/crl/aca_ca3.crl
```

A continuación, se editó la confianza del certificado y se desmarcó el permiso para identificar sitios web por lo que al intentar acceder otra vez a los servicios telemáticos se produjo el mensaje de error del principio de la práctica.

2. CREACIÓN DE CERTIFICADOS CON OPENSSL

a. CREACIÓN DE UNA AUTORIDAD CERTIFICADORA

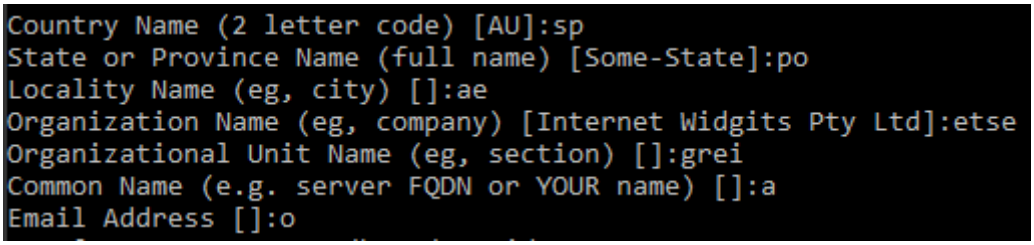
Para la creación de una autoridad certificadora, se realizaron cambios en el fichero openssl.conf y se crearon una serie de directorios para la entidad certificadora.

b. CREACIÓN DE UN CERTIFICADO RAÍZ (AUTOFIRMADO)

El primer paso fue generar un certificado autofirmado. En primer lugar, se generó la clave privada para la autoridad certificadora, luego proporcionar los datos para acompañar a la clave y a continuación se utilizó la clave privada para firmar los datos, creando el certificado. Para ello se utilizó el siguiente comando, que permite crear la clave privada y el certificado raíz:

```
openssl req -x509 -newkey rsa:1024 -
keyout ./demoCA/private/privadaCA.pem -out ./demoCA/raizCA.pem
```

Para el certificado raíz. A continuación, fue necesaria introducir una contraseña y datos informativos sobre el certificado a emitir:



c. CREACIÓN DE PETICIONES DE CERTIFICADO (POR PARTE DE USUARIO) Y FIRMA DE CERTIFICADOS (POR PARTE DE LA CA)

Al ejecutar ejecutar el comando:

```
Openssl x509 -in raizCA.pem -text
```

Se obtuvo la siguiente información:

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 18258673991942455808 (0xfd63d741cf64c200)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=sp, ST=po, L=ae, O=etse, OU=grei, CN=a/emailAddress=o
Validity
Not Before: Nov  6 00:41:12 2017 GMT
Not After : Dec  6 00:41:12 2017 GMT
Subject: C=sp, ST=po, L=ae, O=etse, OU=grei, CN=a/emailAddress=o
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (1024 bit)
```

```
Modulus:
00:93:e4:5c:9d:23:27:96:8c:8c:8a:eb:66:ec:d8:
39:a2:d5:6f:9e:cb:15:e3:1a:94:5b:eb:61:e2:24:
90:d4:aa:9a:67:fa:75:ac:eb:3b:47:2a:cb:ff:2b:
08:2a:50:0d:ad:34:28:77:80:3f:9a:f7:e4:c8:f1:
39:b0:f0:7e:4c:16:83:92:7e:23:9e:8a:c5:56:64:
bb:87:60:86:78:f5:cf:32:a4:1b:90:48:92:5c:5e:
0e:52:8e:8e:13:10:59:6c:1e:7d:19:e2:e7:8a:52:
2a:e9:15:9a:12:9e:e3:70:f9:c7:73:77:14:b8:02:
5f:bf:d8:08:a9:fd:bd:2a:19
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
7A:05:5D:BB:F1:DF:6E:8A:29:41:04:EB:37:52:62:74:AA:BE:35:BA
X509v3 Authority Key Identifier:
keyid:7A:05:5D:BB:F1:DF:6E:8A:29:41:04:EB:37:52:62:74:AA:BE:35:BA
X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
43:71:a5:31:a7:ac:02:19:6b:5b:56:77:d6:bd:b3:2e:6c:7d:
70:61:80:4c:d5:55:00:91:99:d5:2e:f5:0d:67:f9:21:76:18:
4b:1b:69:83:2d:39:3c:31:e4:61:fc:19:4c:fb:4d:fd:a1:6a:
e1:17:62:2c:41:8e:a5:2e:0d:27:22:28:b4:dc:8d:e0:c8:b3:
18:3a:c8:d0:aa:81:80:79:20:6c:7e:91:e9:8c:db:9c:9b:e3:
1e:6c:df:6e:8e:aa:57:1e:9d:03:cb:de:38:29:f6:fe:27:dc:
67:2b:b3:7b:38:eb:02:85:2c:02:a3:91:3c:b9:1f:5b:b5:13:
a8:23
-----BEGIN CERTIFICATE-----
MIIClDCCAf2gAwIBAgIJAP1j10HPZMIAMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNV
BAYTAnNwMQswCQYDVQQIDAJwbzELMAkGA1UEBwwCYWUxDTALBgNVBAoMBGV0c2Ux
DTALBgNVBAsMBGdyZWkxCjAIBgNVBAMMAWExEDAOBgkqhkiG9w0BCQEWAW8wHhcN
MTcxMTA2MDA0MTEyWhcNMTcxMjA2MDA0MTEyWjBjMQswCQYDVQQGEwJzcDELMAkG
A1UECAwCcG8xCzAJBgNVBAcMAmFlMQ0wCwYDVQQKDARldHNlMQ0wCwYDVQQLDARn
cmVpMQowCAYDVQQDDAFhMRAwDgYJKoZIhvcNAQkBFgFvMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQCT5FydIyeWjIyK62bs2Dmi1W+eyxXjGpRb62HiJJDUqppn
+nWs6ztHKsv/KwgqUA2tNCh3gD+a9+TI8Tmw8H5MFoOSfiOeisVWZLuHYIZ49c8y
pBuQSJJcXg5Sjo4TEFlsHn0Z4ueKUirpFZoSnuNw+cdzdxS4Al+/2Aip/b0qGQID
AQABo1AwTjAdBgNVHQ4EFgQUegVdu/HfboopQQTrN1JidKq+NbowHwYDVR0jBBgw
FoAUegVdu/HfboopQQTrN1JidKq+NbowDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOBgQBDcaUxp6wCGWtbVnfWvbMubH1wYYBM1VUAkZnVLvUNZ/khdhhLG2mD
LTk8MeRh/BlM+039oWrhF2IsQY6lLg0nIii03I3gyLMYOsjQqoGAeSBsfpHpjNuc
m+MebN9ujqpXHp0Dy944Kfb+J9xnK7N7OOsChSwCo5E8uR9btROoIw==
```

d. EMISIÓN DE CERTIFICADOS DE USUARIO

A continuación, se creó una petición de certificado para la autoridad certificadora, a través del siguiente comando:

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

Fue necesario rellenar los mismos campos que en el caso de la creación de la autofirma y dos campos más: *A challenge password* y *An optional company name*.

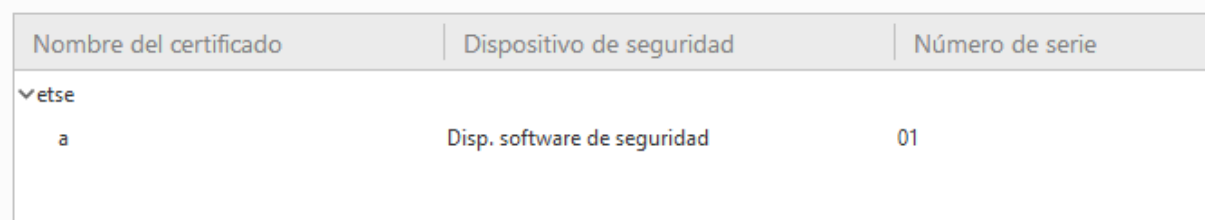
Cuando se recibe una petición, es posible, tras haber verificado los datos, firmar los datos con el siguiente comando:

```
openssl ca -in req.pem -out certificado_usuario.pem
```

Este certificado caduca en 365 días. A continuación, se realizó una conversión del certificado a extensión .p12, con la contraseña abcd, con el siguiente comando:

```
openssl pkcs12 -export -in certificado_usuario.pem -inkey
miclaveprivada.pem -out cert_usuario.p12
```

Finalmente, se ha añadido este certificado al navegador:

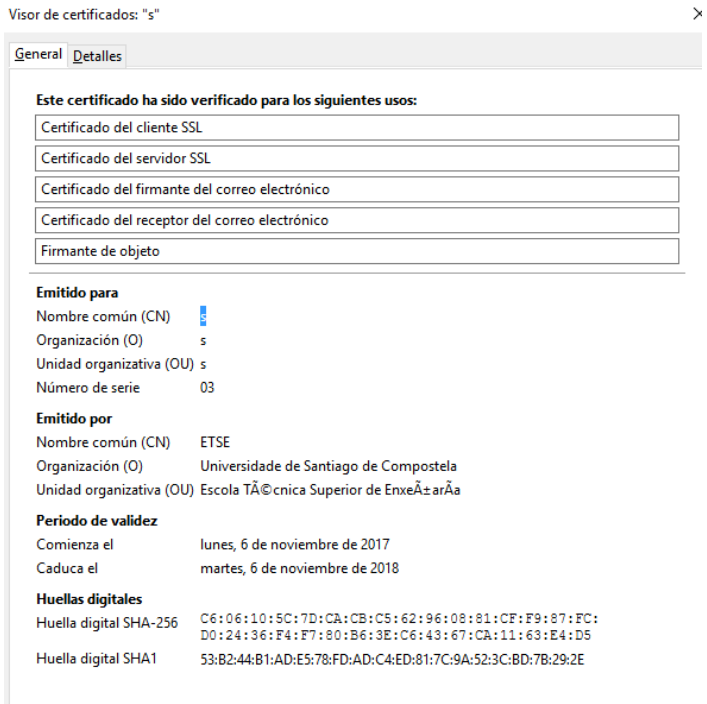


e. POR PAREJAS

A continuación, se envió una petición de certificado a un compañero. Así mismo se recibió una petición por parte del compañero y se procedió a aprobarla con el comando:

```
openssl ca -in req.pem -out certificado_prueba.pem
```

Que fue utilizado previamente. Se procedió a enviar este certificado y el compañero al que se le envió la petición también envió un certificado. A continuación, se convirtió el certificado a .p12, con el fin de añadirlo al navegador. También fue necesario añadir el certificado raíz de la autoridad certificadora del compañero a la lista de CAs, con el fin de que fuera de confianza para el navegador.



Para poder enviar mensajes cifrados a otras personas, sería necesario añadir sus certificados personales al navegador, para ello sería necesario que nos enviara el certificado en .pem, puesto que así únicamente enviaría su clave pública.