Actividad 7: Certificados digitales

Seguridad Informática

06/11/2014

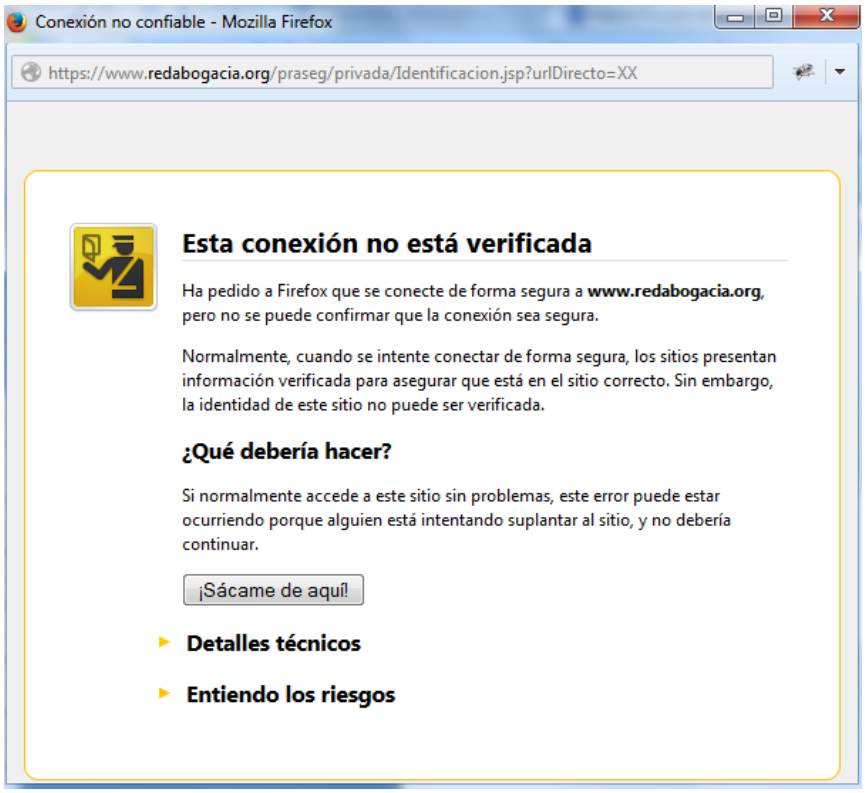
Brais López Yáñez

ÍNDICE

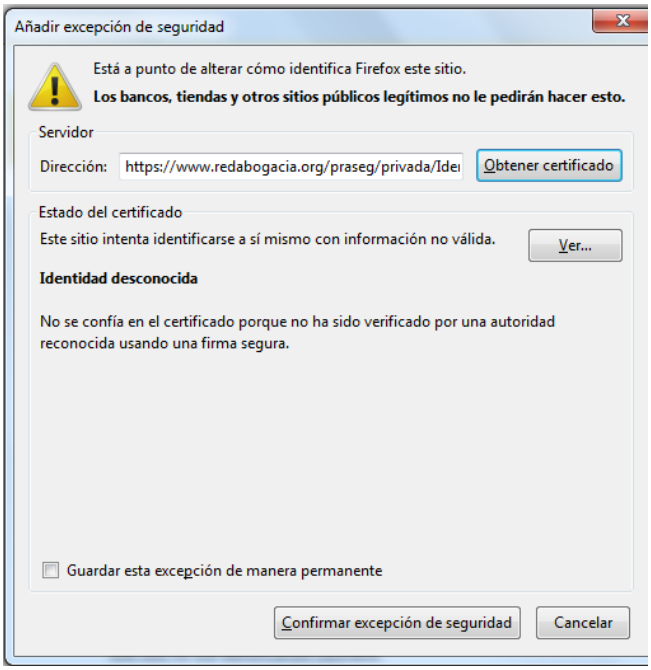
CERTIFICADOS DIGITALES Y CERTIFICADOS RAÍZ

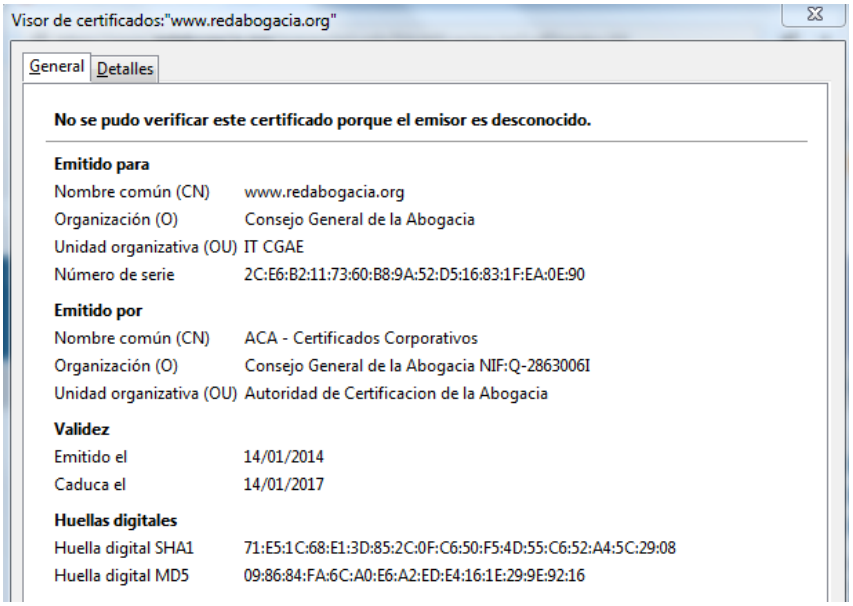
1. Id al sitio web de la Abogacía Española: http://www.abogacia.es/

2. Acceded a los "Servicios Telemáticos" (en el panel de la derecha). ¿Aparece un mensaje de error? ¿Cuál es el motivo? Solucionadlo añadiendo una excepción.

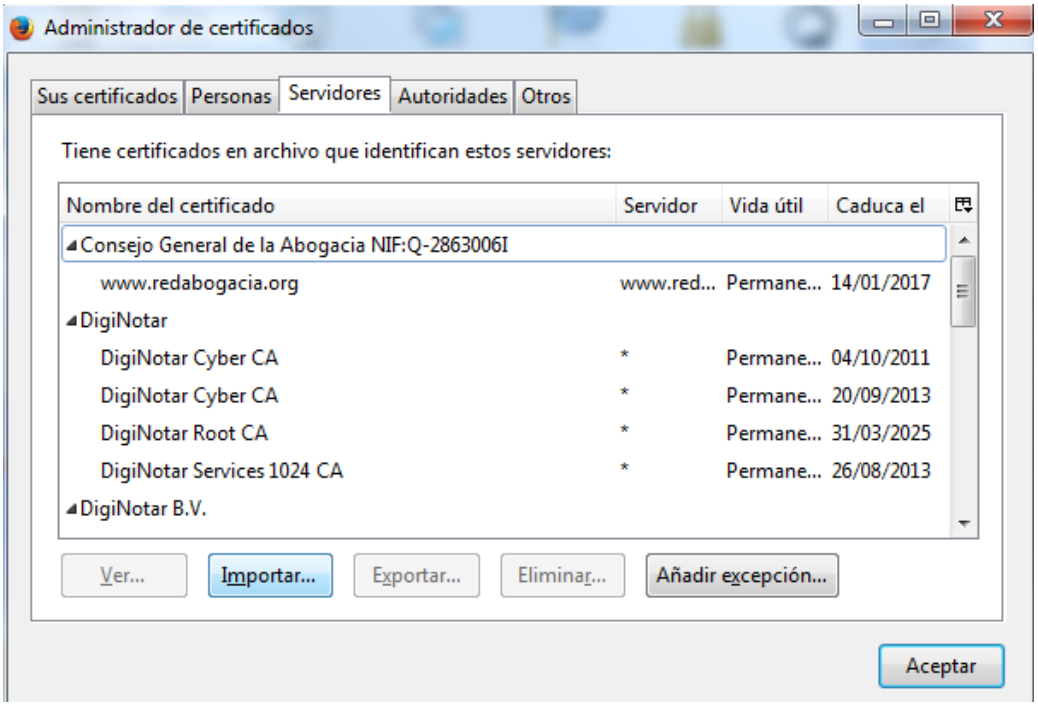


No tenemos el certificado necesario, para conectarnos, si le damos a entender los riesgos, podemos acceder a la obtención del certificado.





3. Una vez resuelto el problema, buscad el certificado en el navegador. ¿En qué apartado está? ¿Para qué usos puede emplearse este certificado?

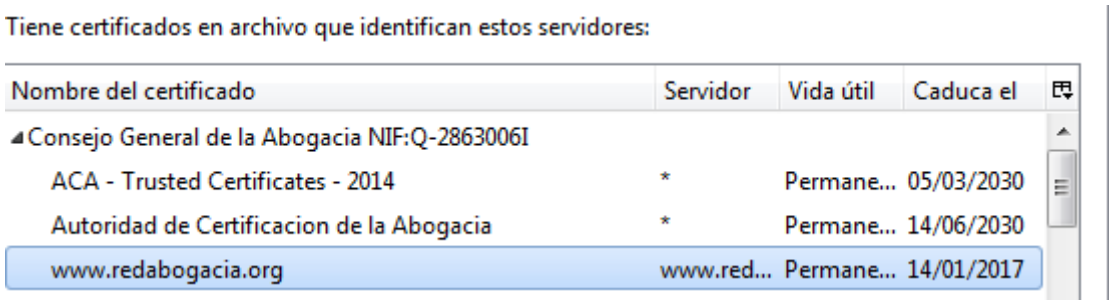


Firefox-->Opciones-->Avanzado-->Certificados-->Ver Certificados--> Servidores

Este certificado trata de validar la conexión www.redabogacia.ort y los diferentes usuarios del sistema.

4. Eliminad el certificado de servidor, e instalad el certificado raíz de la autoridad certificadora correspondiente (DESCARGA SOFTWARE DE ACA).

Accedemos a la sección de descargas de la página abogacia.es y descargamos el certificado correspondiente. Luego importamos el certificado en el apartado de Ver Certificados-->Servidores.



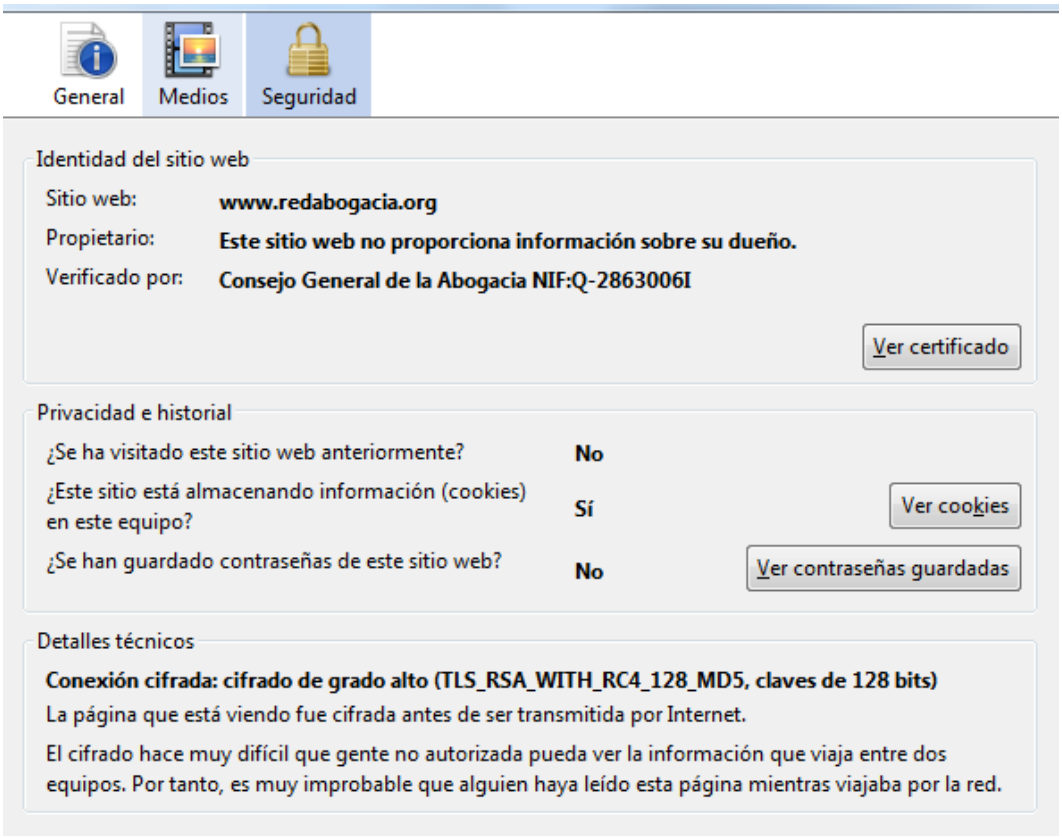
5. Acceded de nuevo a los Servicios Telemáticos. Incluso aunque el certificado raíz sea reconocido por el navegador, ¿podéis acceder al sitio? ¿Qué necesitaríais para ello?

No podemos acceder al servicio web.

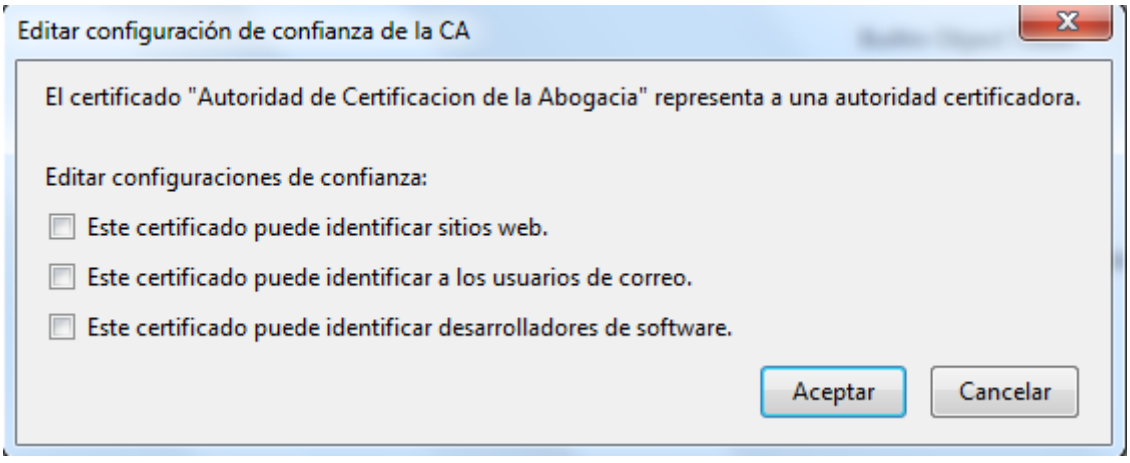
Para poder acceder al sitio, deberíamos ser usuarios registrados de la página, y así poder tener acceso al lugar deseado.

6. Verificad las propiedades de la conexión SSL: identificad los algoritmos de cifrado simétrico y asimétrico, y la función hash. ¿Quién firma el certificado?

Lo firma el consejo general de abogacia NIF:Q-2863006I



7. Editad la confianza en el certificado, y desmarcad el permiso para identificar sitios web. Intentad acceder de nuevo a los Servicios Telemáticos, y comprobad que se muestra de nuevo el mensaje de error.



Se vuelve a mostar el mensaje de error inicial.

CREACIÓN DE UNA NUEVA CA

1. Si estáis usando un PC del aula: copiar el fichero /etc/ssl/openssl.cnf a vuestro home de usuario, para poder editarlo.

```
computer@Computer:~$ cp /etc/ssl/openssl.cnf ./Seguridad7
computer@Computer:~$ cd Seguridad7
computer@Computer:~/Seguridad7$ ls
openssl.cnf
computer@Computer:~/Seguridad7$
```

2. Hacer que la variable "dir" apunte al directorio donde vamos a crear la CA (el nombre por defecto es demoCA, pero podéis cambiarlo). Otra modificación para evitar problemas es descomentar la línea "unique_subject = no".

```
dir             = /home/computer/Seguridad7
certs           = $dir/certs            # Wh
crl_dir         = $dir/crl              # Wh
database        = $dir/index.txt        # da
unique_subject  = no                    # Se
```

3. Crear el directorio (demoCA o el nombre que hayamos elegido) y en su interior, la siguiente estructura de ficheros y carpetas:

```
computer@Computer:~/Seguridad7$ mkdir demoCA
computer@Computer:~/Seguridad7$ cd demoCA/
computer@Computer:~/Seguridad7/demoCA$ mkdir certs
computer@Computer:~/Seguridad7/demoCA$ mkdir crl
computer@Computer:~/Seguridad7/demoCA$ mkdir newcerts
computer@Computer:~/Seguridad7/demoCA$ mkdir private
computer@Computer:~/Seguridad7/demoCA$ >index.txt
computer@Computer:~/Seguridad7/demoCA$ >serial
computer@Computer:~/Seguridad7/demoCA$ ls
certs  crl  index.txt  newcerts  private  serial
```

4. El fichero index.txt debe estar vacío (0 bytes). Podéis crearlo usando >touch index.txt. El fichero serial contendrá la cadena "01" seguida de un retorno de carro. Cuando se firman nuevos certificados, el fichero index.txt se actualiza automaticamente con una lista de los certificados emitidos, y el contenido del fichero serial cambia incrementalmente al siguiente número de serie disponible.

For the CA policy

[policy_match]

countryName = match

stateOrProvinceName = optional

organizationName = optional

organizationalUnitName= optional

commonName = supplied

emailAddress = optional

También debemos indicar la función de resumen (message digest) que se utilizará:

default_md = md5

CREACIÓN DE UN CERTIFICADO RAÍZ (AUTOFIRMADO)

El primer paso será generar la clave privada para la CA, luego proporcionar los datos para la autoridad certificadora, y a continuación usar la clave privada generada para firmar esos datos.

El siguiente comando permite crear el par clave privada + certificado raíz con los nombres que hayamos especificado en el fichero openssl.cnf para las variables private_key (cakey.pem por defecto) y certificate (cacert.pem por defecto). Cambiad los nombres en el fichero de configuración si queréis usar nombres de fichero diferentes, como en este ejemplo:

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

Se crea una clave privada RSA de 1024 bits para la CA, que se almacena en el fichero privadaCA.pem dentro de la carpeta private. Esta clave privada se usa para firmar un certificado raíz para la CA (que se guarda en el fichero raizCA.pem). Este certificado raíz contiene la clave pública y los datos introducidos para la CA, firmados por la propia CA.

```
computer@Computer:~/Seguridad7$ openssl req -x509 -newkey rsa:1024 -keyout ./demoCA/private/private
CA.pem -out ./demoCA/raizCA.pem -config openssl.cnf
Generating a 1024 bit RSA private key
...++++++
.........................................++++++
writing new private key to './demoCA/private/privateCA.pem'
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]:Spain
string is too long, it needs to be less than  2 bytes long
Country Name (2 letter code) [AU]:Spain
string is too long, it needs to be less than  2 bytes long
Country Name (2 letter code) [AU]:SP
State or Province Name (full name) [Some-State]:Pontevedra
Locality Name (eg, city) []:VIgo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Mar de Arousa
Organizational Unit Name (eg, section) []:Mar de Arousa
Common Name (e.g. server FQDN or YOUR name) []:MA
Email Address []:info@ma.es
```

Creación de peticiones de certificado (por parte de un usuario) y firma de certificados (por parte de la CA)

Ya tenemos un certificado autofirmado (certificado raíz raizCA.pem) para nuestra propia CA. Con este certificado podemos procesar peticiones de certificado de otros usuarios y firmarlas.

En primer lugar, comprobamos los campos del certificado raíz en modo texto, usando el comando openssl x509:

openssl x509 -in raizCA.pem –text

```
computer@Computer:~/Seguridad7$ openssl x509 -in raizCA.pem -text
Error opening Certificate raizCA.pem
3074459848:error:02001002:system library:fopen:No such file or directory:bss_file.c:398:fopen('raiz
CA.pem','r')
3074459848:error:20074002:BIO routines:FILE_CTRL:system lib:bss_file.c:400:
unable to load certificate
computer@Computer:~/Seguridad7$ ls
demoCA  openssl.cnf  openssl.cnf~
computer@Computer:~/Seguridad7$ cd demoCA/
computer@Computer:~/Seguridad7/demoCA$ ls
certs  crl  index.txt  newcerts  private  raizCA.pem  serial
computer@Computer:~/Seguridad7/demoCA$ openssl x509 -in raizCA.pem -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            ed:b2:58:d4:52:60:d7:90
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=SP, ST=Pontevedra, L=VIgo, O=Mar de Arousa, OU=Mar de Arousa, CN=MA/emailAddress=
info@ma.es
        Validity
            Not Before: Oct 29 18:40:56 2014 GMT
            Not After : Nov 28 18:40:56 2014 GMT
        Subject: C=SP, ST=Pontevedra, L=VIgo, O=Mar de Arousa, OU=Mar de Arousa, CN=MA/emailAddress
=info@ma.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
```

Podemos ver también el contenido del certificado si lo instalamos en el navegador o en un gestor de correo. Verificad que el receptor (subject) y el emisor (issuer) en el certificado son la misma entidad.

EMISIÓN DE CERTIFICADOS DE USUARIO

Antes de que una CA pueda firmar un certificado personal, debe existir un proceso mediante el cual la CA pueda verificar de alguna forma toda la información almacenada en el certificado. Por ejemplo, para los certificados emitidos por la FNMT, se verifica el nombre y NIF (campo CN en el subject), pero no se verifica la dirección de correo electrónico (campo E). Por otro lado, en el caso de certificados de correo electrónico, el nombre del usuario no es verificado generalmente (por ejemplo, CAcert no verifica el nombre, sólo la dirección de correo).

Ahora vamos a crear una petición de certificado para nuestra propia CA, usando el comando req:

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

Se crea una clave RSA de 1024 bits para el usuario, y se almacena en el fichero miclaveprivada.pem. Se crea otro fichero, req.pem, que contiene la clave pública correspondiente a esa clave privada, y los datos personales del usuario. Este fichero constituye la petición que el usuario debe enviar a la CA para que se lo firme y se lo devuelva como certificado de usuario.

```
computer@Computer:~/Seguridad7$ openssl req -newkey rsa:1024 -keyout miclavepriv
ada.pem -out req.pem -config openssl.cnf
Generating a 1024 bit RSA private key
......++++++
.........................................++++++
writing new private key to 'miclaveprivada.pem'
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]:SP
State or Province Name (full name) [Some-State]:Pontevedra
Locality Name (eg, city) []:Marin
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Caimanes SA
Organizational Unit Name (eg, section) []:Caimanes SA
Common Name (e.g. server FQDN or YOUR name) []:Caimanes
```

Cuando la CA recibe la petición, después de verificar los datos, puede firmar dichos datos con el comando ca, que produce como resultado un certificado de usuario en formato .pem:

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

```
computer@Computer:~/Seguridad7$ openssl ca -in req.pem -out certificado_usuario.
pem -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for /home/computer/Seguridad7/demoCA/private/privateCA.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Nov  3 16:14:45 2014 GMT
            Not After : Nov  3 16:14:45 2015 GMT
        Subject:
            countryName               = SP
            stateOrProvinceName       = Pontevedra
            organizationName          = Caimanes SA
            organizationalUnitName    = Caimanes SA
            commonName                = Caimanes
            emailAddress              = info@caimanes.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                51:AF:FB:DC:71:B8:09:E8:F3:E6:53:B9:FA:B8:4B:F6:D8:5A:FA:52
            X509v3 Authority Key Identifier:
                keyid:96:EC:7D:68:E9:8A:22:4D:D0:5E:92:E0:73:48:B7:EA:14:81:8E:B
1

Certificate is to be certified until Nov  3 16:14:45 2015 GMT (365 days)
Sign the certificate? [y/n]:y
```

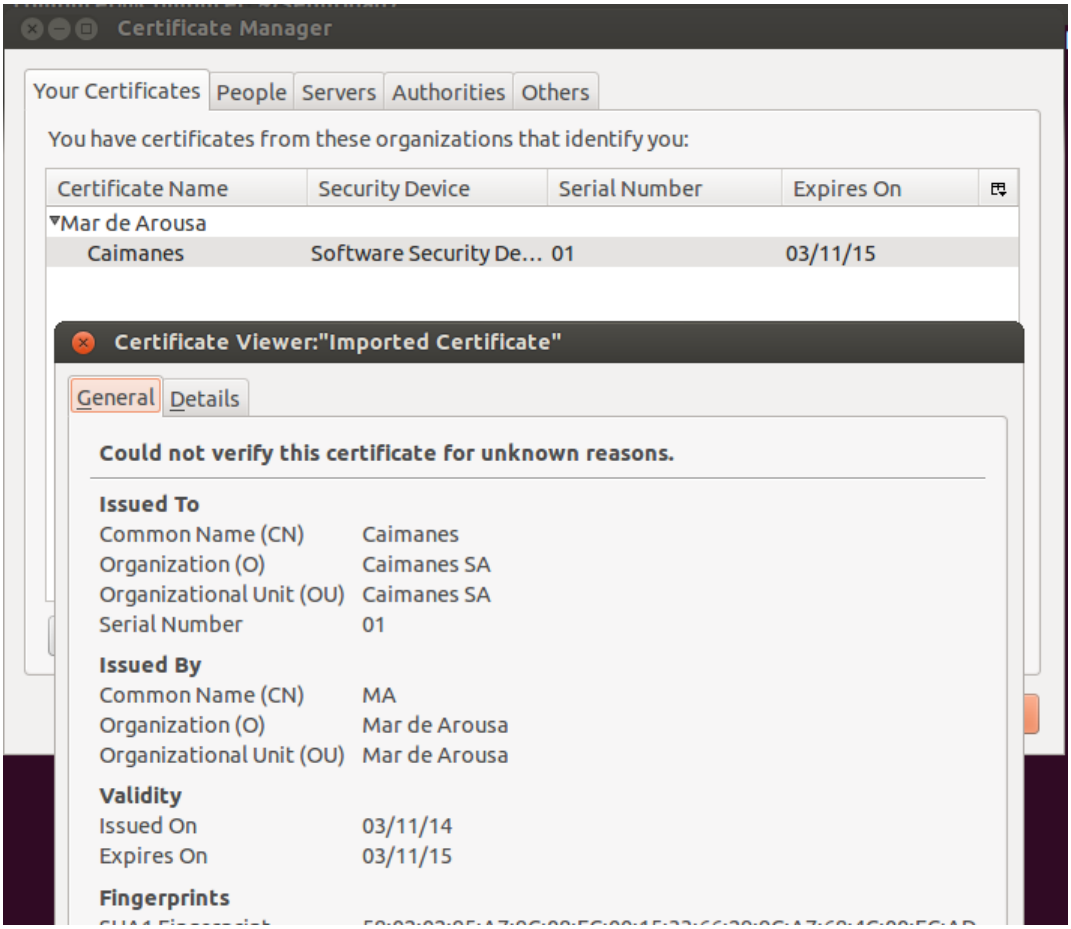
Este certificado contiene la clave pública del usuario, sus datos, y la firma de la CA avalándolos. A partir de este certificado de usuario y de la clave privada del usuario se puede crear un certificado personal en formato pkcs#12 (extensión .p12), que es el formato más ampliamente utilizado en la maioría de aplicaciones (este formato incluye la clave privada dentro del propio certificado, mientras que el formato .pem no). El comando para realizar esta conversión de formatos es:

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

```
computer@Computer:~/Seguridad7$ openssl pkcs12 -export -in certificado_usuario.pem -inkey miclavepriv
ada.pem -out cert_usuario.p12
Enter pass phrase for miclaveprivada.pem:
Enter Export Password:
Verifying - Enter Export Password:
computer@Computer:~/Seguridad7$
```

Un último paso: añadir este certificado personal cert_usuario.p12 al navegador o al gestor de correo, para poder firmar y descifrar información.

En Firefox: Herramientas -> Opciones -> Avanzado -> Ver certificados -> Sus certificados ->

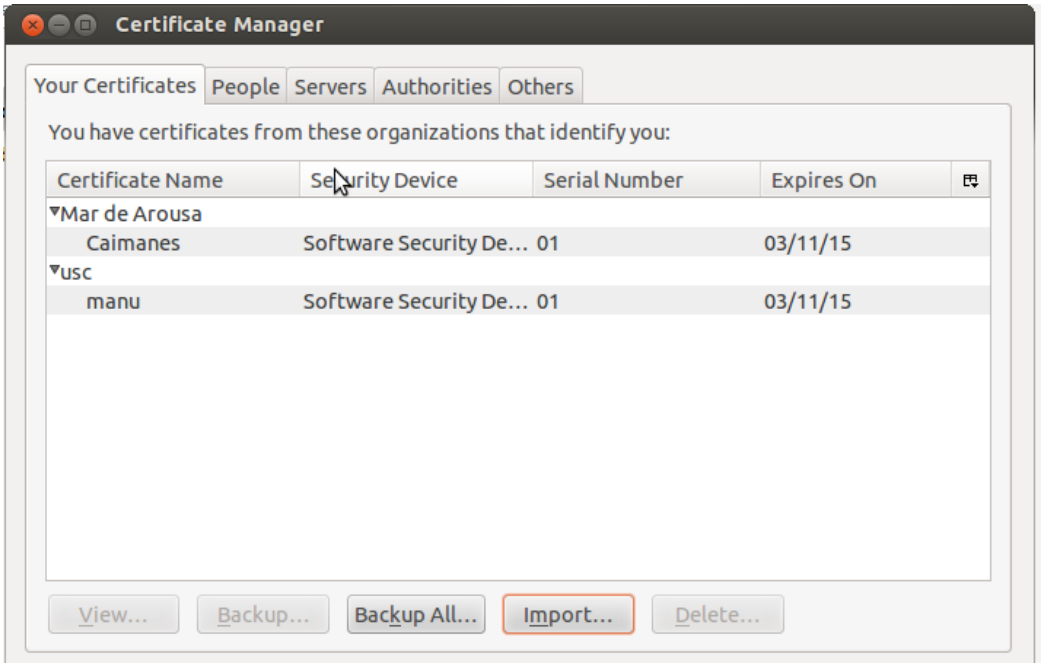


POR PAREJAS

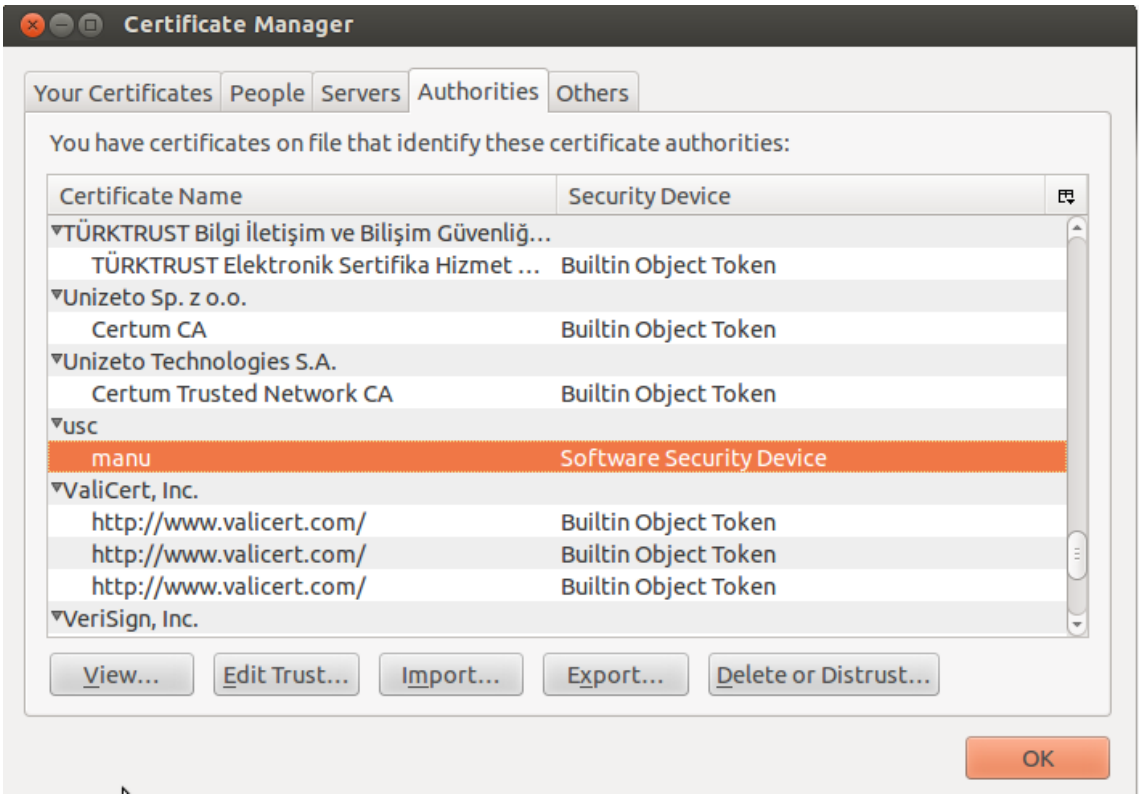
Trabajo realizado junto con Manuel Cascallar Autrán.

Enviad a vuestro compañero una petición de certificado. Vuestro compañero debe procesar la petición y enviaros de vuelta un certificado firmado. Añadid este certificado al navegador, después de convertirlo a formato .p12.

```
computer@Computer:~/Seguridad7$ openssl ca -in reqmanu.pem -out certificado_manu.pem -config openssl.
cnf
Using configuration from openssl.cnf
Enter pass phrase for /home/computer/Seguridad7/demoCA/private/privateCA.pem:
3073644744:error:28069065:lib(40):UI_set_result:result too small:ui_lib.c:869:You must type in 4 to 8
191 characters
Enter pass phrase for /home/computer/Seguridad7/demoCA/private/privateCA.pem:
Check that the request matches the signature
Signature ok
The countryName field needed to be the same in the
CA certificate (SP) and the request (ES)
```



Deberéis añadir también el certificado raíz de la CA del compañero a la lista de CAs del navegador, para que la firma en vuestro certificado sea de confianza para el navegador.



Para poder enviar mensajes cifrados/firmados a otras personas, tendríais que añadir sus certificados personales al gestor de correo, así que pedid a vuestro compañero que os envíe su certificado personal. ¿Tendría que enviar el certificado en formato .pem, o en formato .p12?

Esto va a depender del programa que se utilice. El formato .pem tiene menos funciones que .p12, pero este último aún así tiene las funciones básicas como contener una clave privada dentro de él.