

Práctica 3: Creación de un certificado SSL/TLS multisite

Objetivos

- Crear una Autoridad de Certificación (AC) para firma de certificados.
- Crear una solicitud de firma de certificado (CSR) para un servidor web que funcionará en varios dominios.
- Instalar el certificado generado en un servidor web.

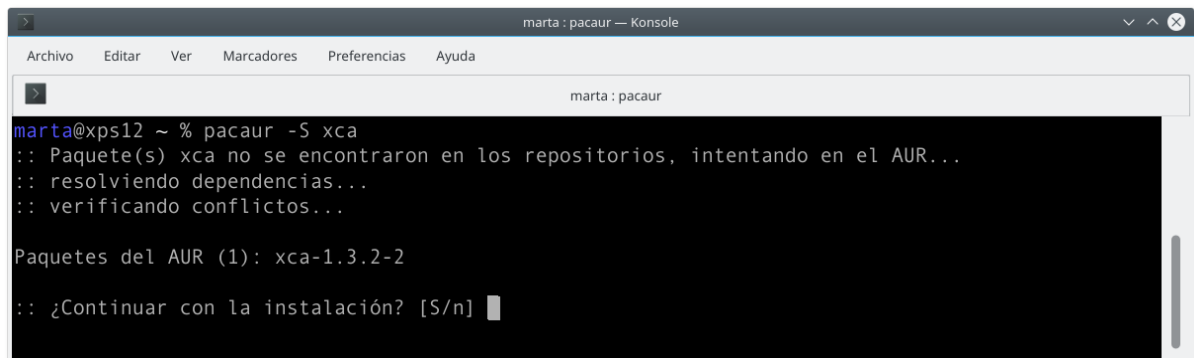
Preparación

Se necesita la herramienta de creación, revocación y almacenamiento de certificados digitales **XCA**, disponible en los repositorios de muchas distribuciones GNU/Linux y también para Windows.

Necesitarás tener instalado un servidor Apache. En principio también podría ser en Windows, aunque yo lo he probado en Linux.

Enunciado

1. Instala la aplicación XCA en la distribución de tu preferencia (este software ha sido probado en Arch, Debian, Ubuntu y Fedora) y ejecútala.



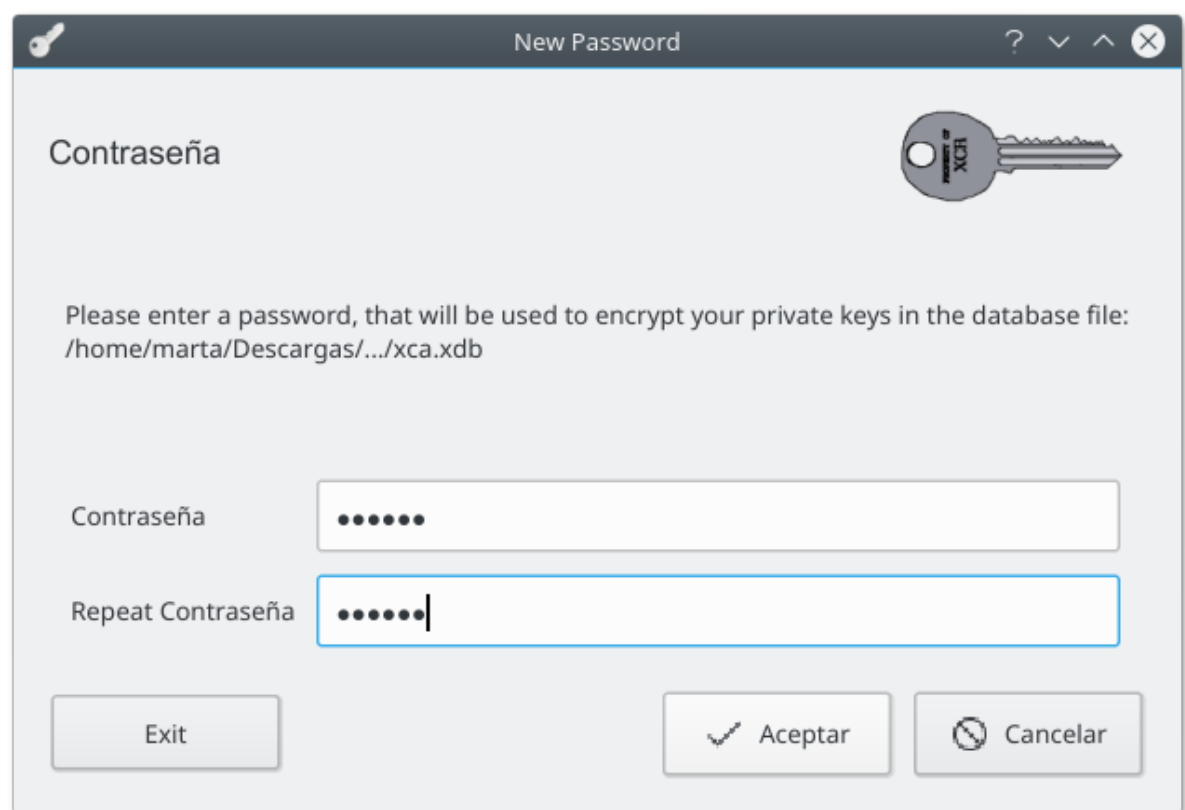
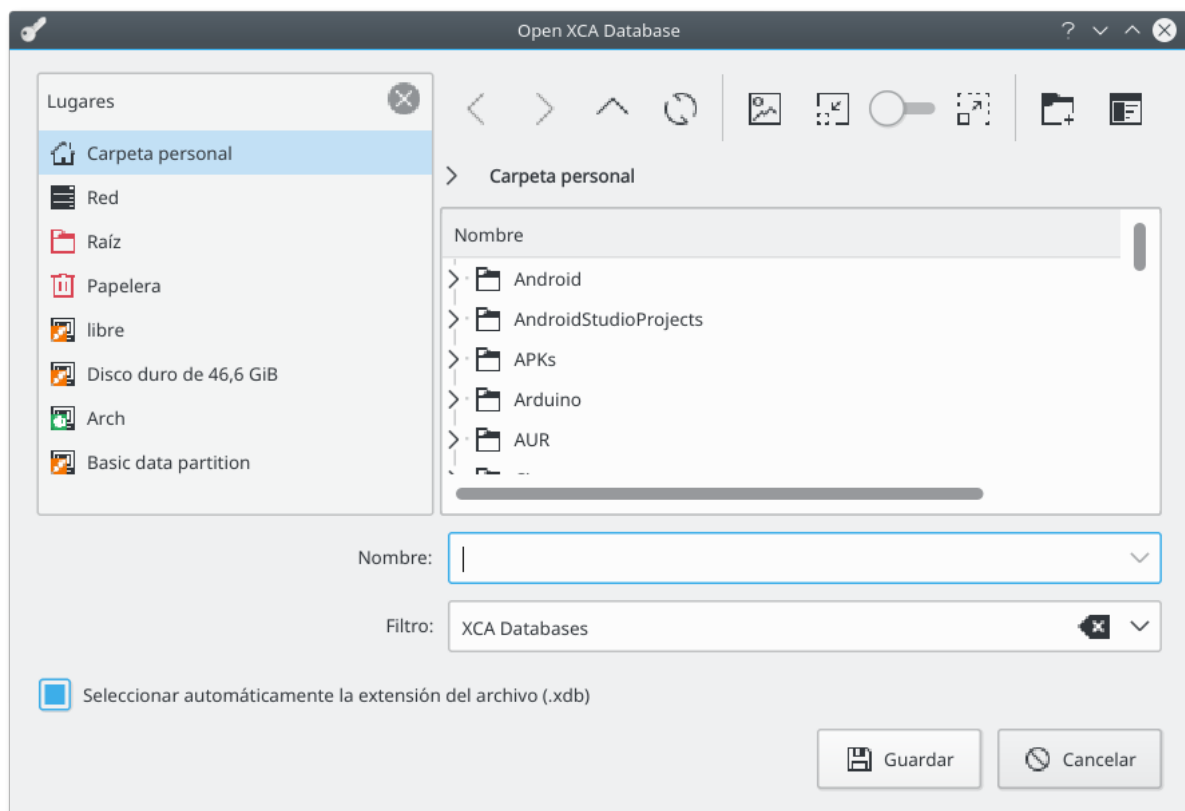
```
marta : pacaaur — Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
marta : pacaaur
marta@xps12 ~ % pacaaur -S xca
:: Paquete(s) xca no se encontraron en los repositorios, intentando en el AUR...
:: resolviendo dependencias...
:: verificando conflictos...

Paquetes del AUR (1): xca-1.3.2-2

:: ¿Continuar con la instalación? [S/n]
```

(Ejemplo en Arch Linux)

2. Antes de trabajar con el programa, es necesario crear una base de datos donde el programa guardará y gestionará todos los certificados que solicitemos o que creamos. Esto se hace con *File* → *New Database*. Elegimos un nombre y una ruta. Nos pedirá una contraseña para proteger nuestros certificados y las claves privadas de ellos.



- Una vez creada la base de datos ya podemos generar y tramitar certificados. El primer paso es constituirnos como una AC que podrá certificar y validar certificados digitales de otras personas o

servidores web. Para ello ves a la pestaña *Certificates* y pulsas *New Certificate* en el menú de la derecha. En la ventana que aparece, en la pestaña *Source* u *Origen*, debes seleccionar el template *[default] CA* y pulsar *Apply All*. La aplicación XCA dispone de una serie de plantillas (templates) para configurar parámetros por defecto en función del uso del certificado. En este caso, ya que vamos a crear nuestra propia Autoridad de Certificación, debemos seleccionar ese template. Como vamos a crear una AC raíz, deja marcado *Create a self signed certificate with the serial* y elegimos SHA 256 como algoritmo de firma. Recordemos que ni MD5 ni SHA 1 se recomiendan por seguridad. Recuerda pulsar *Apply All*:

The screenshot shows the 'Create x509 Certificate' dialog box in the XCA application. The 'Source' tab is active. In the 'Signing request' section, the 'Copy extensions from the request' checkbox is checked. In the 'Signing' section, the radio button for 'Create a self signed certificate with the serial' is selected, with the serial number '1' entered in the adjacent field. The 'Firma' (Signature) dropdown menu is set to 'SHA 256'. In the 'Template for the new certificate' section, '[default] CA' is selected from the dropdown. Below this, the 'Apply all' button is highlighted in blue, while 'Apply extensions' and 'Apply subject' are in grey. At the bottom right, there are 'Aceptar' (Accept) and 'Cancelar' (Cancel) buttons.

4. Observa que una vez seleccionado el template default CA, en la pestaña *Extensions*, se ha marcado *Certification Authority* como tipo de Certificado y con una validez de 10 años. Esto es así porque en la plantilla por defecto se ha definido esa validez. El programa te permite generar otra plantilla personalizada con distintos parámetros, como por ejemplo los años de validez. Por ejemplo, hay algunas AC como la GVA o la FNMT que tienen 20 de años de validez en sus certificados. Observa también que en la pestaña *Key Usage* (utilización de la clave), se ha marcado *Certificate Sign* y *CRL Sign*. Esto es así porque éste es el uso habitual de un certificado de una CA: firmar y revocar otros certificados.

X Certificate and Key management <2>

?

^

^

×

Create x509 Certificate

Source

Sujeto

Extensions

Key usage

Netscape

Advanced

X509v3 Basic Constraints

Type

Certification Authority

Path length

☒ Critical

Key identifier

☒ Subject Key Identifier

☐ Authority Key Identifier

Validez

No antes de

2017-06-27 16:27 GMT

No después de

2027-06-27 16:27 GMT

Rango de tiempo

10

Años

Aplicar

☐ Medianoche

☐ Local time

☐ No well-defined expiration

X509v3 Subject Alternative Name

Edit

X509v3 Issuer Alternative Name

Edit

X509v3 CRL Distribution Points

Edit

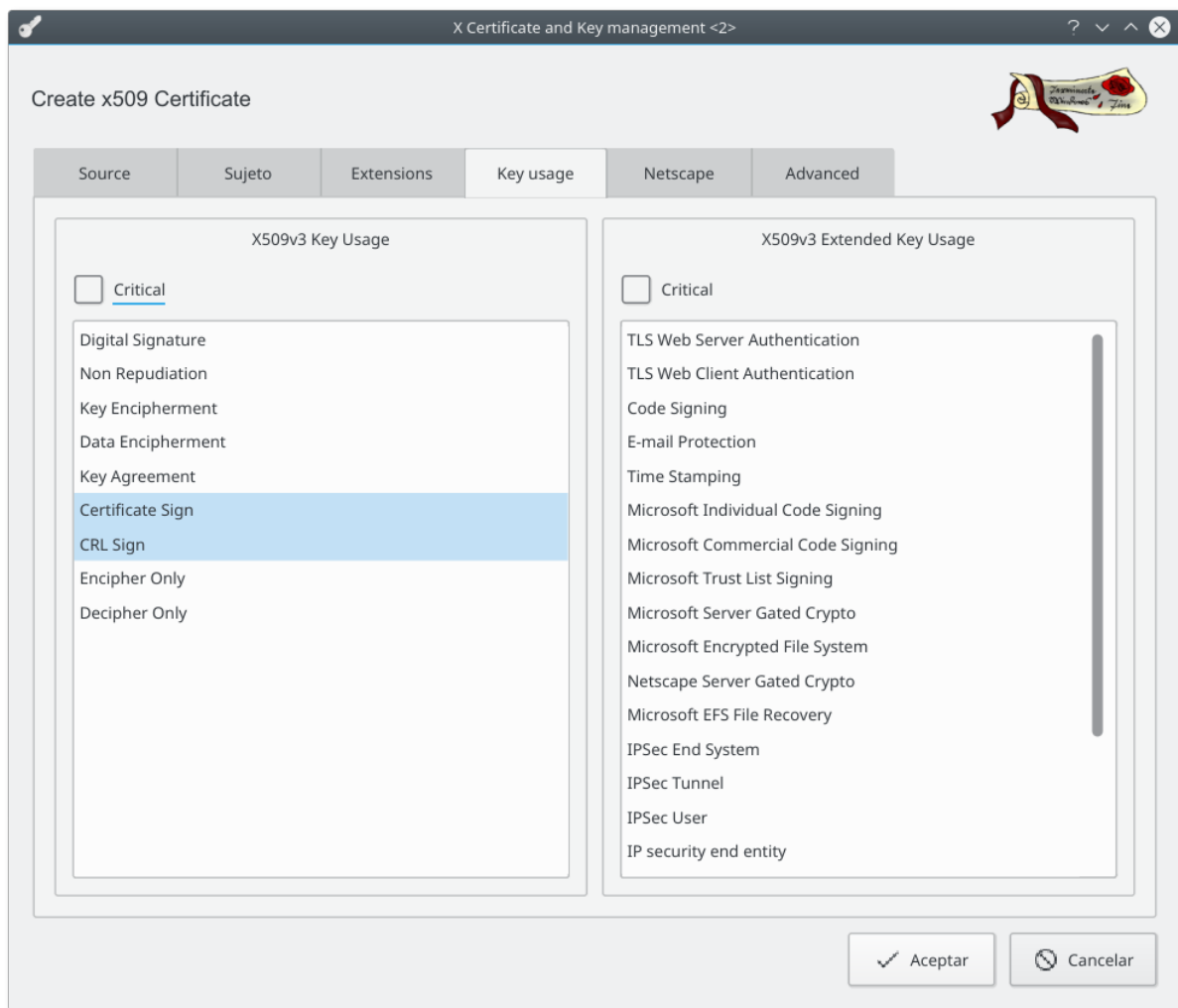
Authority Information Access

OCSP

Edit

✓ Aceptar

⊗ Cancelar



5. En la pestaña *Sujeto* o *Subject* tienes que escribir los campos que te identificarán como AC. En la siguiente pantalla hay un ejemplo de los valores que puedes poner. Cámbialos personalizándolo a tu nombre y evita usar acentos. Puedes cambiar los campos de Organización, unidad organizativa, Common name, etc. a tu gusto, pero que sean valores que tengan sentido como si fueran para una Autoridad Certificadora real:

X Certificate and Key management <2>

Create x509 Certificate

Source | **Sujeto** | Extensions | Key usage | Netscape | Advanced

Distinguished name

Nombre interno	AC Marta	organizationName	Mi Empresa
countryName	ES	organizationalUnitName	Mi Departamento
stateOrProvinceName	Castellon	commonName	AC Marta
localityName	La Vall d'Uixo	emailAddress	

Type	Content
------	---------

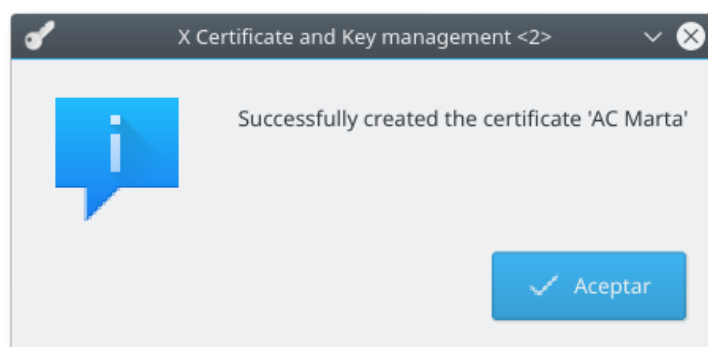
Add
Eliminar

Exponente secreto

AC Marta (RSA:2048 bit) ☐ Used keys too [Generate a new key](#)

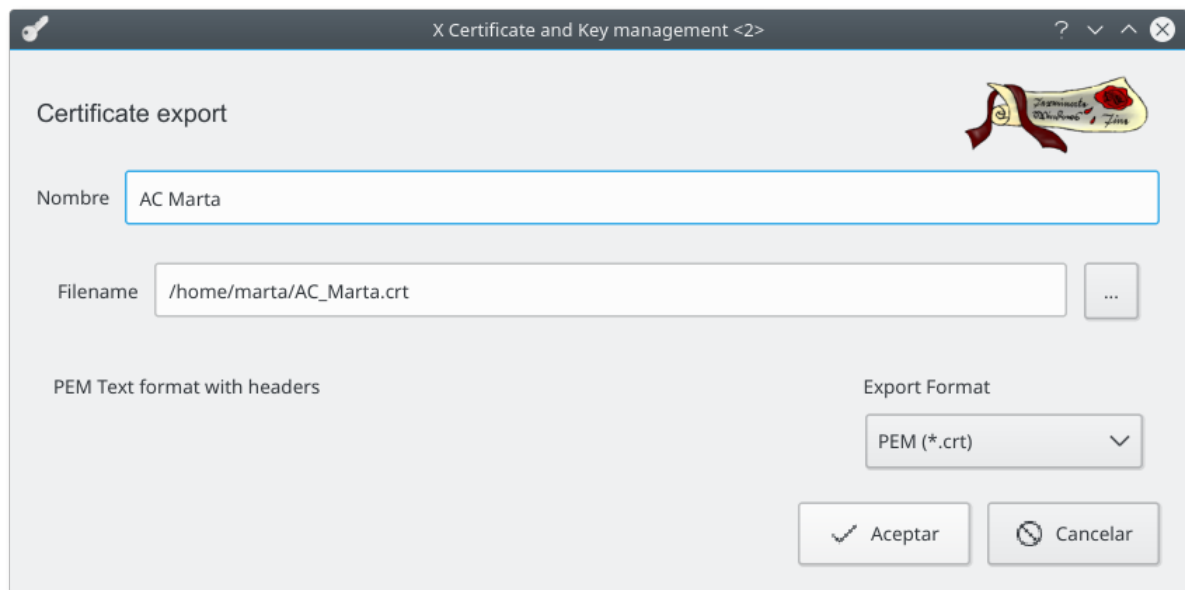
✓ Aceptar Cancelar

Tienes que crear una nueva clave privada para usar en el certificado de la AC. Recuerda que los certificados digitales utilizan la criptografía asimétrica o de clave pública y por tanto todo certificado va asociado a un par de claves. Pulsa en *Generate a new key* y selecciona RSA de 2048 bits, que es una buena longitud de clave. Después de esto, ya puedes pulsar *Aceptar* y se habrá generado tu certificado de AC.

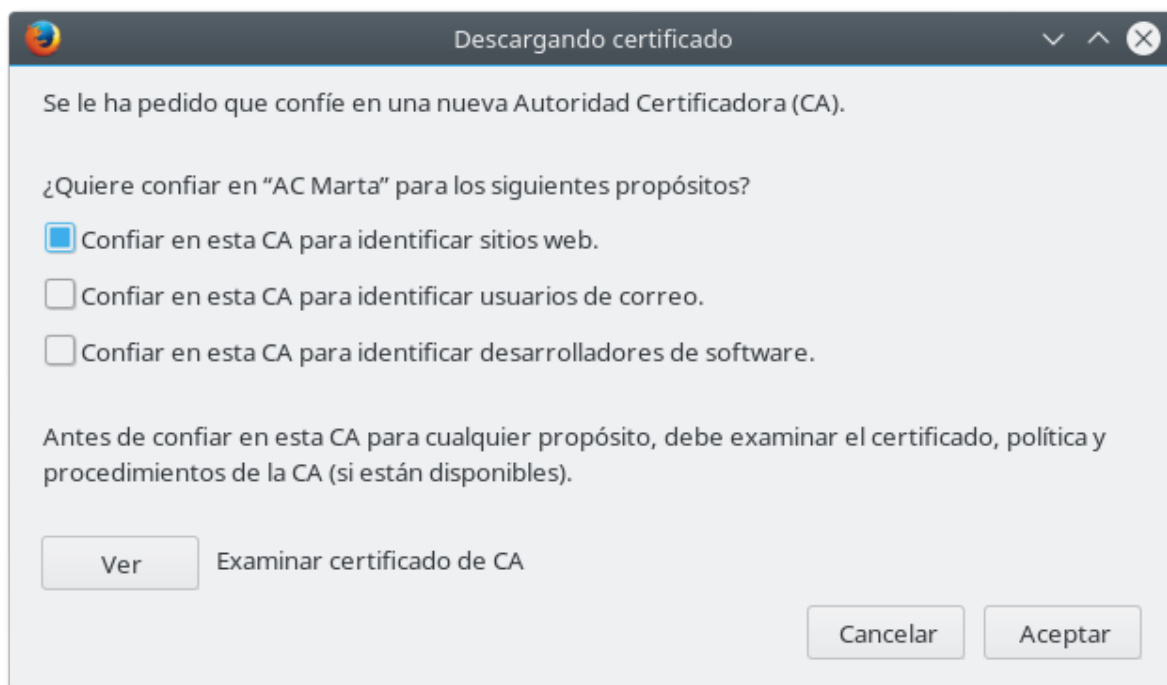


Nombre interno	commonName	CA	Número de serie	Expiry date	CRL Expiration
 AC Marta	AC Marta	Yes	01	2027-06-27	

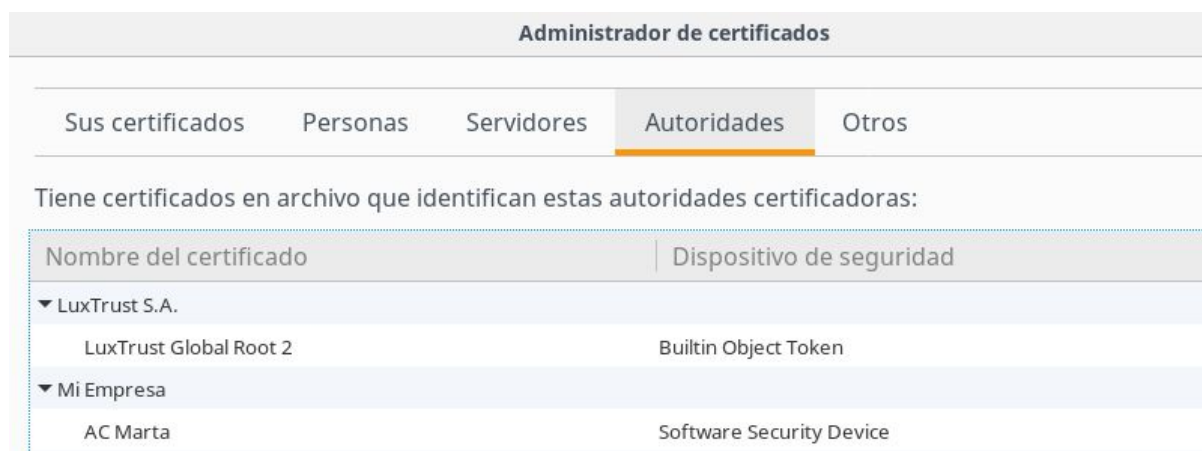
6. Llegamos a este punto ya tenemos la AC constituida. Esta AC la exportaremos a un fichero .crt en formato PEM (codificado en base64) para poder importarlo en la lista de AC's autorizadas y confiables de nuestro navegador. Para ello selecciona el certificado creado y pulsa Export. Una vez exportado, lo puedes importar en tu navegador. Por ejemplo, desde Firefox, esta tarea se realiza desde *Preferencias -> Avanzado -> Certificados -> Ver certificados -> Autoridades -> Importar*. Después marca como mínimo *Confiar en esta CA para identificar sitios web*:



La importamos en Firefox:



En la pestaña *Autoridades* puedes buscar el certificado importado buscando por el nombre de organización (Mi empresa en el ejemplo que os estoy poniendo; espero que hayáis sido más originales que yo):



- Llegados a este punto, vamos a simular que somos una organización con presencia en Internet y que necesitamos un certificado digital de servidor web para el sitio web de la organización y que responde a varios dominios simultáneamente. Como ejemplo se proponen los nombres de servidor siguientes: `www.cursoseguridad.com`, `www.cursoseg.com`, `www.cursoseguridad.es` y `www.cursoseg.es`. A continuación debes ir a la pestaña *Certificate Signing Request* y pulsar *New Request*. Selecciona el template *[default] HTTPS_server* y SHA 256 como firma y pulsa *Apply*, de esta forma se ajustan los parámetros para un certificado de servidor web seguro. Los atributos `unstructuredName` y `challengePassword` no se suelen usar aunque algunas AC's lo pueden solicitar, para la práctica no hace falta.

X Certificate and Key management <2>

Create Certificate signing request

Source Sujeto Extensions Key usage Netscape Advanced

Distinguished name

Nombre interno	Servidor seguro cursoseg	organizationName	Mi empresa, S.L.
countryName	ES	organizationalUnitName	Mi departamento
stateOrProvinceName	Castellon	commonName	www.cursoseguridad.com
localityName	La Vall d'Uixo	emailAddress	info@cursoseguridad.com

Type	Content

Add
Eliminar

Exponente secreto

Servidor seguro cursoseg (RSA:2048 bit) ☒ Used keys too [Generate a new key](#)

✓ Aceptar ☐ Cancelar

8. En la pestaña *Sujeto* o *Subject* tienes que escribir los campos que te identificarán como servidor web, ya que el uso que le vas a dar al certificado que estás solicitando. En la siguiente pantalla hay un ejemplo de los valores que puedes poner. Cámbialos personalizándolo al dominio de tu servidor y evita usar acentos. Es fundamental que el *Common Name* lo pongas correctamente y debe ser el FQDN (nombre de dominio completo) que usará tu servidor en Internet:

Create Certificate signing request

Source Sujeto Extensions Key usage Netscape Advanced

Distinguished name

Nombre interno: Servidor seguro cursoseg organizationName: Mi empresa, S.L.

countryName: ES organizationalUnitName: Mi departamento

stateOrProvinceName: Castellon commonName: www.cursoseguridad.com

localityName: La Vall d'Uixo emailAddress: info@cursoseguridad.com

Type	Content

Exponente secreto

Servidor seguro cursoseg (RSA:2048 bit) ☐ Used keys too [Generate a new key](#)

☒ Aceptar ☐ Cancelar

9. A continuación vamos a añadir los nombres de dominio adicionales en la pestaña *Extensions*. Pulsa el botón Editar situado al lado del campo *subject alternate name* y en la ventana que aparece introduce todos los nombres adicionales del tipo DNS, como en el siguiente ejemplo. Observa que puedes introducir * como prefijo en los nombres (nota: no vale algo como *.dominio.*):

☒ Critical



	Type	Content
0	DNS	www.cursoseguridad.com
1	DNS	www.cursoseg.com
2	DNS	www.cursoseg.es
3	DNS	*,cursoseguridad.com

[Add](#) [Eliminar](#)

[Aplicar](#) [Validate](#) [Cancelar](#)

10. Pulsa *Aplicar* y *Aceptar* y aparecerá la nueva CSR en la pestaña de Certificate signing requests, pero pendiente de firma. En un escenario real, deberías exportar este CSR y enviarlo a una AC para que una vez validado el dominio y la organización, proceda a firmar digitalmente tu CSR y convertirla en un certificado digital de servidor listo para usar. En nuestra práctica, como nosotros mismo somos la AC, procedemos a firmar la CSR seleccionándola y pulsando *Firma* en el menú contextual que aparece al hacer clic en el botón derecho del ratón. En el procedimiento de firma, aplicamos el template de HTTPS_server, seleccionaremos SHA 256 como algoritmo de firma y seleccionamos nuestra AC para firmar en la lista desplegable *Use this Certificate for signing*:

11. Asegúrate que está marcado *Copy extensions from the request* para que se copien las extensiones adicionales como Subject Alternate Names del CSR original al certificado que se va a crear. Para evitar que haya extensiones duplicadas al copiarlas desde la CSR y se produzca un error, en la pestaña *Extensions* selecciona como tipo Not defined. Después en la pestaña *Key Usage*, desmarca las tres opciones marcadas bajo *Key Usage*. En la pestaña *Netscape*, elimina la opción *SSL Server* y el comentario. Finalmente pulsa *Aceptar* y el certificado aparecerá generado colgando del certificado de tu AC en la jerarquía de certificados:

Private Keys		Certificate signing requests		Certificates	Templates	Revocation lists
Nombre interno	commonName	CA	Número de serie	Expiry date	CRL Expiration	
✓  AC Marta	AC Marta	✓ Yes	01	2027-06-27		
 Servi...	www.cursose...	No	02	2018-06-27		

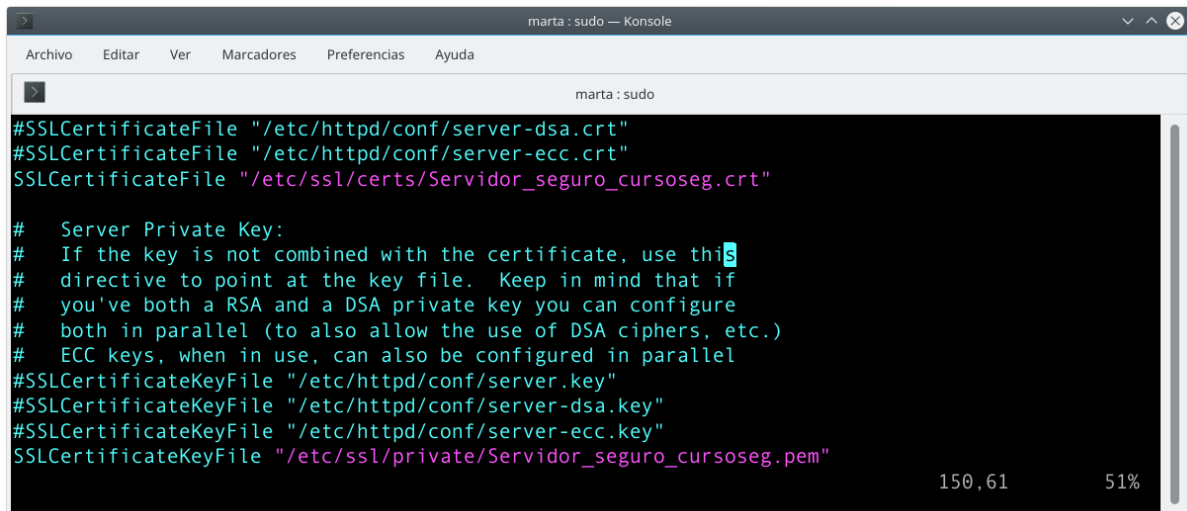
12. En este momento, ya puedes exportar tanto el certificado del servidor web recién generado, como la clave privada asociada, ambos en formato PEM. Normalmente desde xca el certificado se exporta con extensión .crt y la clave privada con extensión .pem, aunque a la hora de instalarlos en un servidor web como Apache, es indiferente la extensión que tenga. Copia tanto el certificado como clave privada en el directorio habitual de tu distribución GNU/Linux, como por ejemplo */etc/ssl/certs* para certificados y */etc/ssl/private* para claves privadas en el caso de Debian y derivadas o */etc/pki/tls/certs* para Red Hat, CentOS o Fedora, y asegurándote de que la clave privada tiene permisos 600 y es propietario root únicamente, para que nadie excepto root tenga acceso a la clave privada.

```

130 marta@xps12 ~ % sudo cp Servidor_seguro_cursoseg.crt /etc/ssl/certs/
[sudo] contrasena per a marta:
marta@xps12 ~ % sudo cp Servidor_seguro_cursoseg.pem /etc/ssl/private
marta@xps12 ~ %

```

- Configura tu servidor Apache para que funcione con SSL/TLS usando cualquier guía de Internet. Básicamente se trata de cargar el módulo `mod_ssl` (puede que no esté instalado), de que escuche en el puerto 443 y de indicar la ruta al certificado y clave privada en la configuración de Apache. Se deben usar las directivas **SSLEngine**, **SSLCertificate** y **SSLCertificateKeyFile**.



```

marta : sudo — Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

marta : sudo
#SSLCertificateFile "/etc/httpd/conf/server-dsa.crt"
#SSLCertificateFile "/etc/httpd/conf/server-ecc.crt"
SSLCertificateFile "/etc/ssl/certs/Servidor_seguro_cursoseg.crt"

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
#   ECC keys, when in use, can also be configured in parallel
#SSLCertificateKeyFile "/etc/httpd/conf/server.key"
#SSLCertificateKeyFile "/etc/httpd/conf/server-dsa.key"
#SSLCertificateKeyFile "/etc/httpd/conf/server-ecc.key"
SSLCertificateKeyFile "/etc/ssl/private/Servidor_seguro_cursoseg.pem"

150,61  51%

```

```

3 marta@xps12 ~ % sudo vi /etc/httpd/conf/extra/httpd-ssl.conf
marta@xps12 ~ % sudo systemctl restart httpd.service
marta@xps12 ~ % sudo systemctl status httpd.service
● httpd.service - Apache Web Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2017-06-27 20:20:37 CEST; 2s ago
     Process: 16731 ExecStop=/usr/bin/httpd -k graceful-stop (code=exited, status=1/FAILURE)
    Process: 17062 ExecReload=/usr/bin/httpd -k graceful (code=exited, status=0/SUCCESS)
   Main PID: 16815 (httpd)
      Tasks: 6 (limit: 4915)
   CGroup: /system.slice/httpd.service
           └─16815 /usr/bin/httpd -k start -DFOREGROUND
             └─16823 /usr/bin/httpd -k start -DFOREGROUND
               └─16824 /usr/bin/httpd -k start -DFOREGROUND
                 └─16825 /usr/bin/httpd -k start -DFOREGROUND
                   └─16826 /usr/bin/httpd -k start -DFOREGROUND
                     └─16827 /usr/bin/httpd -k start -DFOREGROUND

jun 27 20:20:37 xps12 systemd[1]: Started Apache Web Server.
marta@xps12 ~ %

```

- Una vez configurado y reiniciado Apache, vamos a simular que los dominios que has añadido como nombres alternativos, se resuelven en Internet. Para ello lo más fácil es editar el fichero `hosts` de tu sistema e indicarle que todos esos dominios se sirven en `localhost` (127.0.0.1):





```





127.0.0.1    localhost www.cursoseguridad.com www.cursoseguridad.es
www.cursoseg.comwww.cursoseg.es

```

15. Comprueba ahora que conectándote por https a cualquiera de estos dominios, se muestra la página por defecto de tu servidor web usando TLS y sin mostrar ninguna alerta de seguridad, ya que el certificado incluye todos esos nombres DNS. Haz la prueba añadiendo algún dominio no incluido en el certificado y mostrando una alerta de seguridad del navegador al no corresponder el dominio con el certificado.



 Información de la página - https://www.cursoseguridad.com/   

 **General**  **Medios**  **Permisos**  **Seguridad**

Identidad del sitio web

Sitio web: **www.cursoseguridad.com**

Propietario: **Este sitio web no proporciona información sobre su dueño.**

Verificado por: **Mi Empresa**

[Ver certificado](#)

Privacidad e historial

¿Se ha visitado este sitio web anteriormente?	No	
¿Este sitio está almacenando información (cookies) en este equipo?	No	Ver cookies
¿Se han guardado contraseñas de este sitio web?	No	Ver contraseñas guardadas

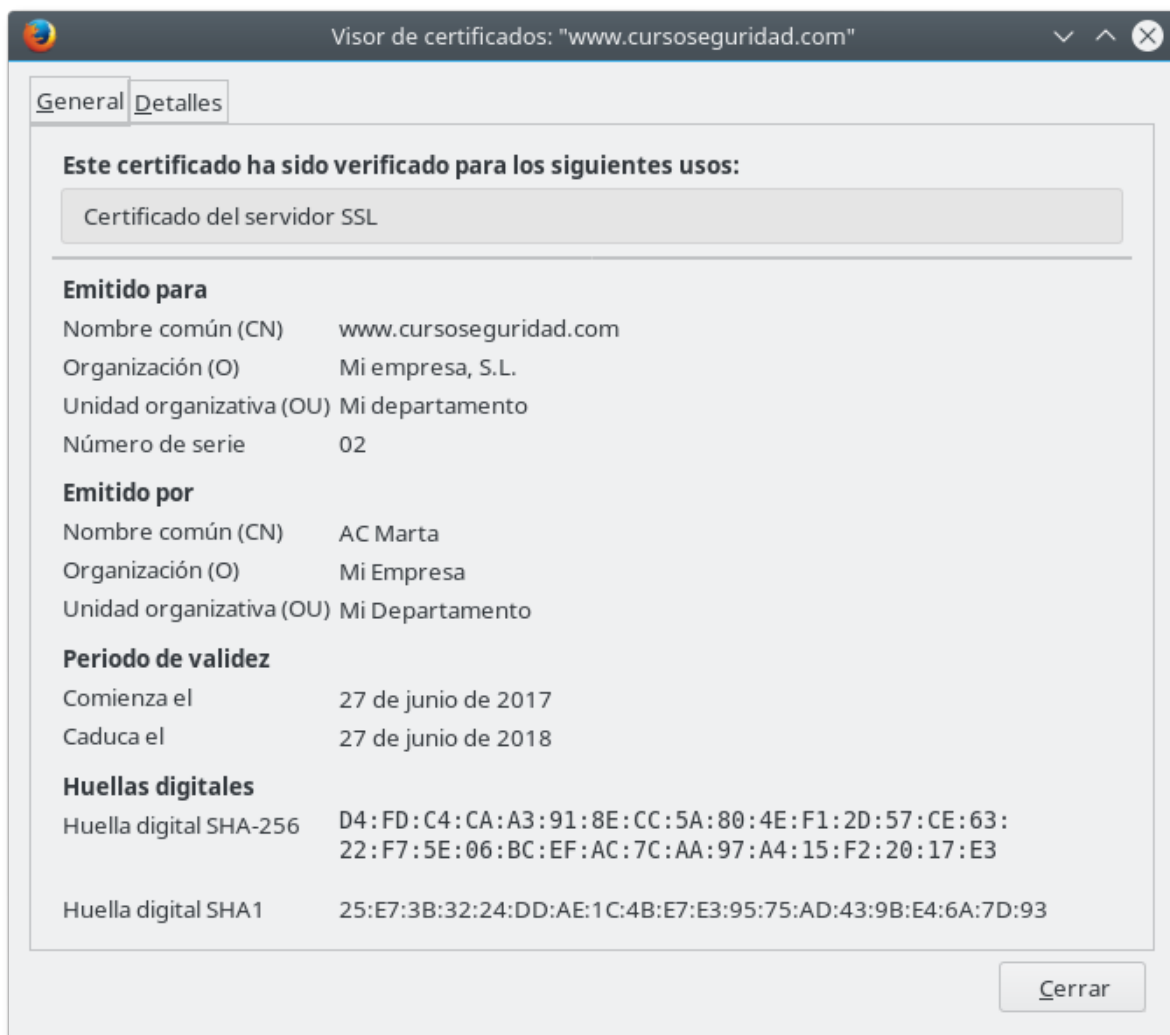
Detalles técnicos

Conexión cifrada (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, claves de 256 bits, TLS 1.2)

La página que está viendo fue cifrada antes de transmitirse por Internet.

El cifrado dificulta que personas no autorizadas vean la información que viaja entre sistemas. Es, por tanto, improbable que nadie lea esta página mientras viajó por la red.

[Ayuda](#)



Sube la memoria al enlace habilitado al efecto.