

Solicitud de Certificados de servidor web

El procedimiento de solicitud de los distintos tipos de certificados que pueden ser expedidos por la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda (FNMT – RCM), en el marco del Convenio FNMT – Junta de Andalucía, se encuentra disponible en el portal de la Oficina Virtual de Soporte a la Administración Electrónica.

El tipo de certificado necesario será el siguiente:

Certificado de F.N.M.T. Clase 2 CA para un servidor web identificado por el nombre del dominio

Este certificado permitirá establecer comunicaciones con sus clientes utilizando la tecnología SSL, el estándar para comunicaciones seguras en la Web. Su servidor se identificará a los clientes con el nombre del dominio donde se encuentra su servicio Web.

A continuación se detalla el proceso para una solicitud de certificado de servidor web de ejemplo.

Para comenzar la solicitud de emisión de certificado es necesario acceder a la página web <http://apus.cert.fnmt.es/PrerregistroSolicitudesComponentes/index.html> y hacer click en el enlace “Solicitar un certificado de F.N.M.T. Clase 2 CA para un servidor web identificado por el nombre del dominio”

SOLICITUDES EN CURSO

Consulte el estado de su solicitud

Nº PETICIÓN:

CIF:

GENERACIÓN DE CLAVES

Si tiene Internet Explorer y desea generar su par de claves, pulse aquí:

ATENCIÓN: El procedimiento habitual para la obtención de un certificado de componente consiste en la generación de una solicitud de certificado (PKCS#10) mediante las herramientas proporcionadas por el software / hardware que va a utilizar el mismo. Si Vd. genera la petición pulsando el botón superior, deberá conocer a priori la forma de importar material criptográfico en su software / hardware.

IMPRESINDIBLE

Para poder utilizar esta aplicación es necesario que tenga habilitadas las cookies en su navegador.

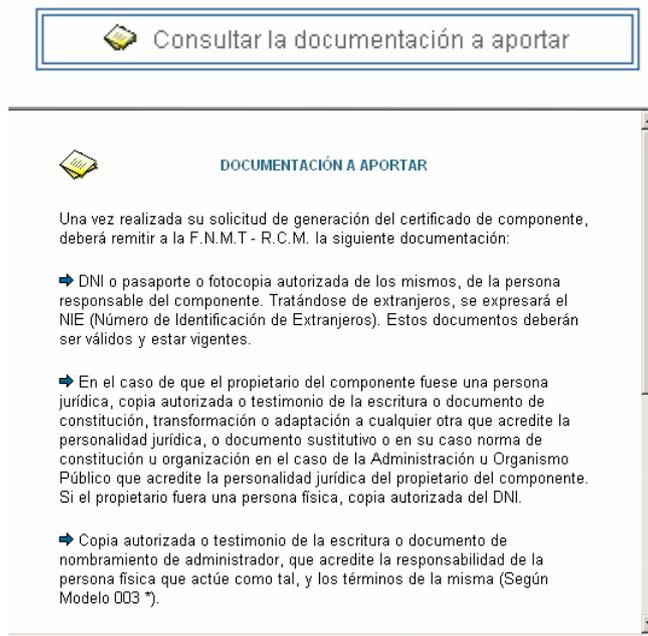
OBTENGA SU CERTIFICADO DE COMPONENTE

Seleccione el tipo de certificado de componente que desee obtener.

- [Solicitar un certificado de F.N.M.T. Clase 2 CA para un servidor web identificado por el nombre del dominio](#)
Este certificado permitirá establecer comunicaciones con sus clientes utilizando la tecnología SSL, el estándar para comunicaciones seguras en la Web. Su servicio se identificará a los clientes con el nombre del dominio donde se encuentra su servicio Web.
- [Solicitar un certificado de F.N.M.T. Clase 2 CA para un servidor web identificado por la dirección IP](#)
Este certificado le permitirá establecer comunicaciones con sus clientes utilizando la tecnología SSL, el estándar para comunicaciones seguras en la Web. Su servicio se identificará a los clientes con la dirección IP donde se encuentra su servicio Web.
- [Solicitar un certificado de F.N.M.T. Clase 2 CA para firma de software](#)
Este Certificado de Firma de Código le permite firmar programas y componentes informáticos acreditando su identidad como autor y realizar de este modo distribuciones seguras a través de Internet.
- [Solicitar un certificado de F.N.M.T. Clase 2 CA para clientes de servicios avanzados](#)
Estos Certificados de Cliente de Servicios Avanzados le permitirán conectar y utilizar los Servicios Avanzados de Certificación de la FNMT.
- [Solicitar un certificado de F.N.M.T. Clase 2 CA para componentes informáticos genéricos](#)
Estos certificados pueden emplearse para establecer conexiones seguras entre componentes informáticos genéricos. Su utilización le permitirá garantizar la integridad y confidencialidad de las comunicaciones de datos entre componentes o servicios.

Hay que tener en cuenta que en la parte final del formulario de solicitud accesible desde el enlace indicado en el párrafo anterior se requiere incluir el PKCS#10 de la solicitud de certificado. Para ello se dispone de la utilidad de generación de claves ubicada bajo el formulario “Solicitudes en curso”.

Junto con el formulario de solicitud es necesario aportar cierta documentación que se describe en la opción “Consultar la documentación a aportar”. Para servidores web que formen parte de dominios de la Junta de Andalucía será necesario aportar únicamente el modelo 003.



NOTA IMPORTANTE:

GENERACIÓN DE CLAVES

Si tiene Internet Explorer y desea generar su par de claves, pulse aquí:

ATENCIÓN: El procedimiento habitual para la obtención de un certificado de componente consiste en la generación de una solicitud de certificado (PKCS#10) mediante las herramientas proporcionadas por el software / hardware que va a utilizar el mismo. Si Vd. genera la petición pulsando el botón superior, deberá conocer a priori la forma de importar material criptográfico en su software / hardware.

El campo de “SOLICITUD DE CERTIFICADO (PKCS#10)*: “ al final de cada plantilla de formulario, debe ser diferente para cada solicitud, y lo más sencillo es generarlo a través de la utilidad que se ofrece para ello en la herramienta.

Ejemplo de solicitud de certificado

Solicitud de Certificado para servidor web, identificado por nombre de dominio

Supongamos para ello que nos han asignado, después de publicar nuestro servidor en Internet, la url "www.servidorAyto.es"

GENERACIÓN DE UN CERTIFICADO DE FNMT CLASE 2 CA PARA UN SERVIDOR WEB IDENTIFICADO POR DNS

FORMULARIO DE DATOS

SUJETO DEL CERTIFICADO	
DATOS IDENTIFICATIVOS DEL SERVIDOR WEB	
DOMINIO*:	www.servidorAyto.es

PROPIETARIO DEL CERTIFICADO	
DATOS DE IDENTIFICACION	
RAZON SOCIAL*:	Ayto Tal
CIF*:	S1234567F
DATOS DOMICILIARIOS	
DIRECCIÓN*:	Avda. tal
LOCALIDAD*:	Sevilla
CODIGO POSTAL*:	41011
PROVINCIA*:	SEVILLA
PAIS*:	ESPAÑA

RESPONSABLE DEL CERTIFICADO	
DATOS DE IDENTIFICACION	
NIF*:	12345678A
PRIMER APELLIDO*:	Apellido1
SEGUNDO APELLIDO:	Apellido2

NOMBRE*:	Juan
DATOS DOMICILIARIOS	
DIRECCIÓN*:	San Juan Roque 19
LOCALIDAD*:	Sevilla
CODIGO POSTAL*:	41001
PROVINCIA*:	SEVILLA
PAIS*:	ESPAÑA

DATOS DE CONTACTO	
TELEFONO:	954123456
FAX:	954654321
E-MAIL:	cambiar@cambiar.es
DATOS DE LA SOLICITUD PKCS10	

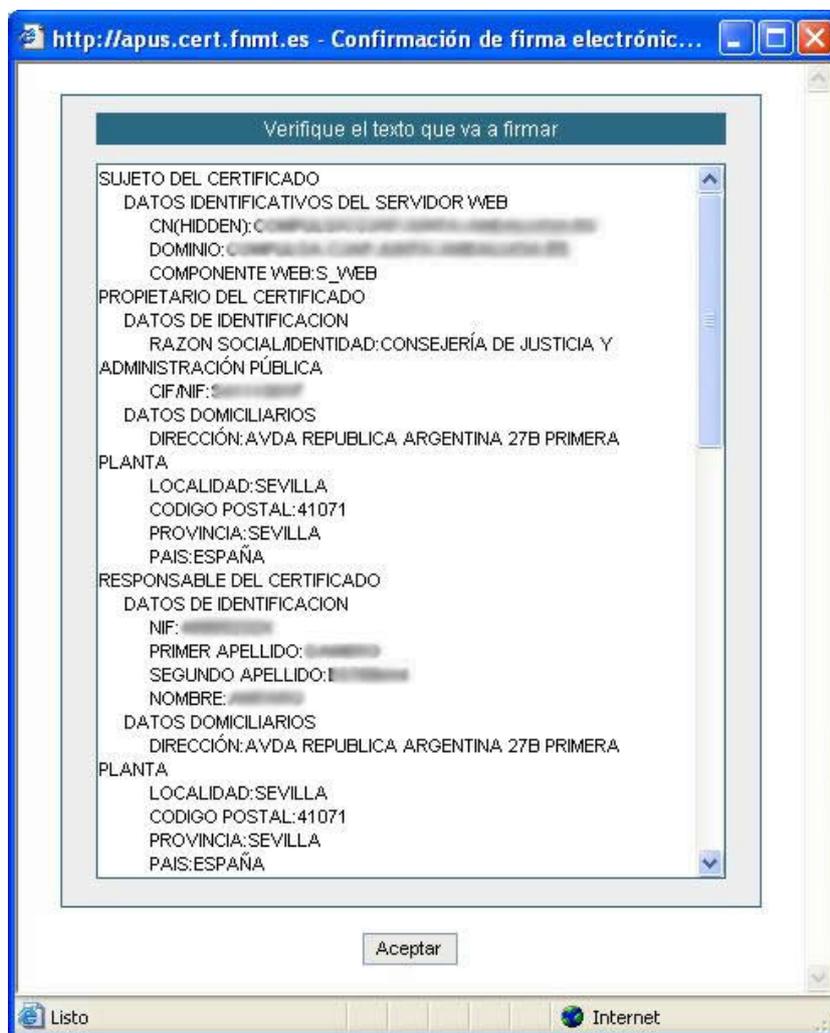
MIIDHTCCAoYCAQA w QDEhMB8GA1UEAxMYUHJI
cnJIZ2lzdHJvIGNvbXBvbmVudGVzMQ4w DA Y DV Q
QKEw VDRVJFUzELMAkGA1UEBhMCRVMw gZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALuw
9kpnRZ5fiXF3w 3w Xn4oR7Gw cQiznqUsOfQbme6g
kilw z85BPGSt0kWguvf5vtf32OLTyb1auteR9B2dyG
NSA lexCSBvL3Q4Fc587UNrS9aWGZLC+sD0dKSI
A tsCx46F7tfGEeUpkmDdbHbfvllhNy +jz0yzFyq+i2r6
DGtdrAgMBAAGgggGbbMBoGCisGAQQBgjcNAgMx
DBYKNS4xLjI2MDAuMjB7BgorBgEEAYI3AgEOMW0
w azAObgNVHQ8BAf8EBAMCBPAw RAYJKoZIhvc
NAQkPBDcw NTAObggqhkiG9w 0DAgICAIAw DgYI
KoZIhvcNAw QCAgCAMAcGBSsOA w IHMAoGCCq
GSIs3DQMhMBMGA1UdJQQMMAoGCCsGAQUFB
w MCMh/BgorBgEEAYI3DQICMYHw MIHtAgEBHlw A
TQBpAGMAcgBvAHMAbw BmAHQAIA BFA G4AaA
BhAG4AYw BIA GQAIA BDA HIAeQBw AHQA bw Bn
AHIA YQBw AGgAaQBjA CAA UAB yAG8AdgBpAG
QAZQByACAA dgAxAC4AMA OBIQcf +EY Tk0ykebs
QglNw ErmPSAWLdGf lJNHbeHHjRMOjk8VDA W0VG
8LTqik/9TxDivrhLWpx2ib/l6dY WXPY241T5yU6vyE
W1RscvPceg94
+kgrw cNC1mhF5RH/Wqk1w Tc0lg586PFkw A9AFJB
sZdF4kdn52j8s5FEhmGY RF2Aiw DQAAAAAAAAA
AMA0GCSqGSIs3DQEBBQUAA4GBAE29Y/TA xIFzi
jIB6MPGakNuHZ2KD0I3epNEidc0bNjK3ID3vGGA0K
X7GiNzuw KV +d7d64Ver10FILn/GNdstig9fph28WL
HfWJkxLPhMLQ8jxS4Q8XWvuXgM/iek3fvOiQ+tIAC
OLzRoWfZkGsS2SmA/MrrgxjP/KoQd55jrRS

**SOLICITUD DE CERTIFICADO
(PKCS#10)*:**

(*) Campo obligatorio

Tras indicar la información necesaria en el formulario de solicitud y pulsar en el botón “Aceptar”, aparece de nuevo el formulario con todos los datos que se han introducido, para que el solicitante pueda comprobar que toda la información se ha introducido correctamente. Si están correctos, se procede a la firma digital del mismo mediante el certificado de persona física de la persona responsable del trámite de la entidad en cuestión. Recordar que no es necesario realizar este trámite desde la propia máquina que realiza las labores de servidor.

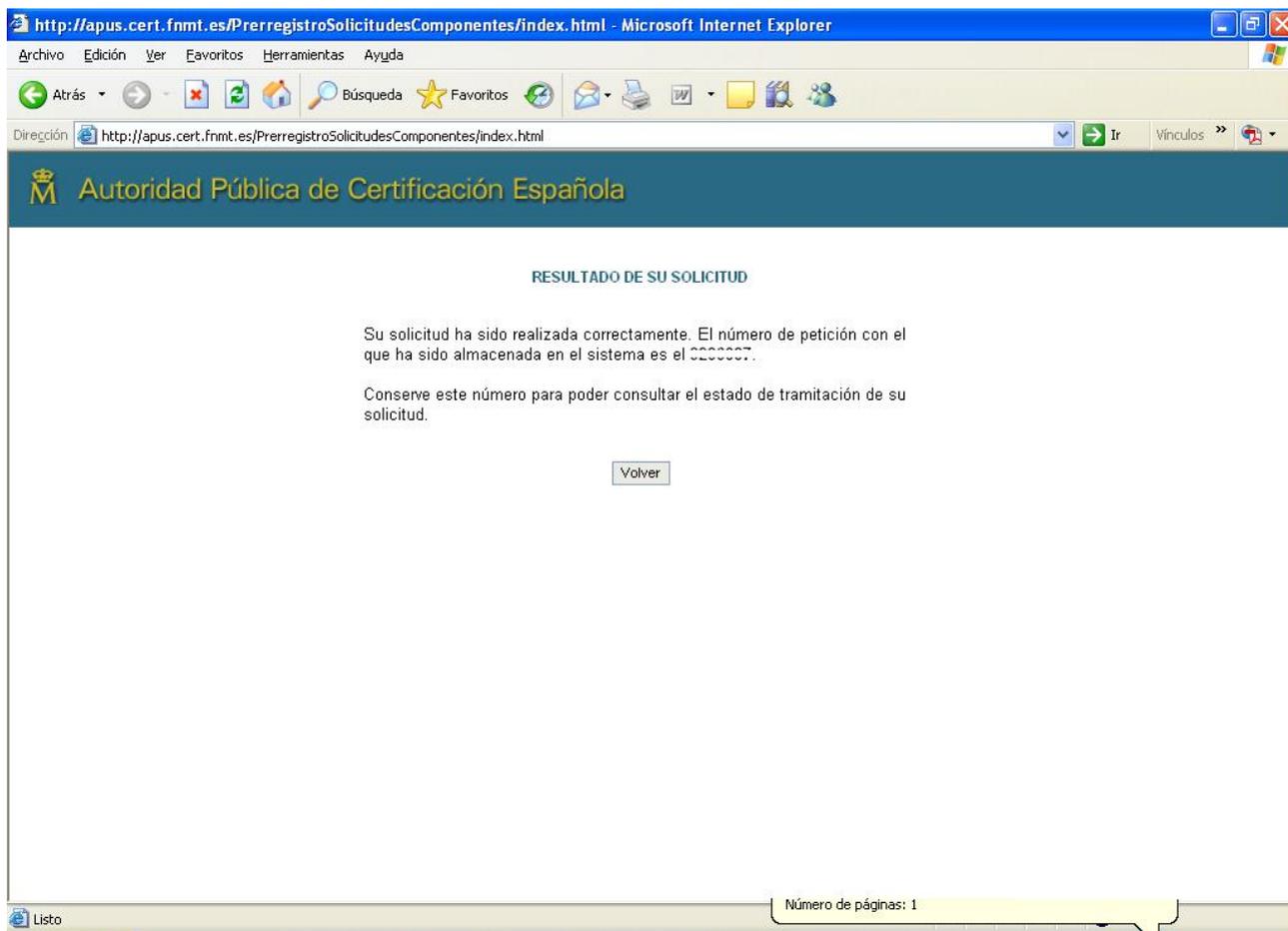
Antes de la firma, se muestra una ventana emergente con los datos que vamos a firmar (los datos de la captura no se corresponden con los aparecidos en el formulario anterior)



Una vez firmado, nos muestra una ventana con dos marcos: en la parte inferior aparece un PDF con los datos que hemos introducido. Este archivo habrá que imprimirlo pulsando en el botón “Imprimir Contrato” que aparece en el marco superior, para posteriormente pulsar en “Aceptar”. Es obligatorio imprimirlo, ya que este contrato se tendrá que enviar a la FNMT para la solicitud del certificado.



Tras pulsar el botón “Aceptar”, el sistema devuelve un número de solicitud que tendrá que guardar, ya que con él consultará el estado de su petición de certificado.



El Modelo 003 completamente relleno, junto con el PDF impreso obtenido tendrá que enviarlo convenientemente firmado a la siguiente dirección postal:

FABRICA NACIONAL DE MONEDA Y TIMBRE
DEPARTAMENTO CERES
ÁREA DE REGISTRO
C/ JORGE JUAN, 106
28009 MADRID

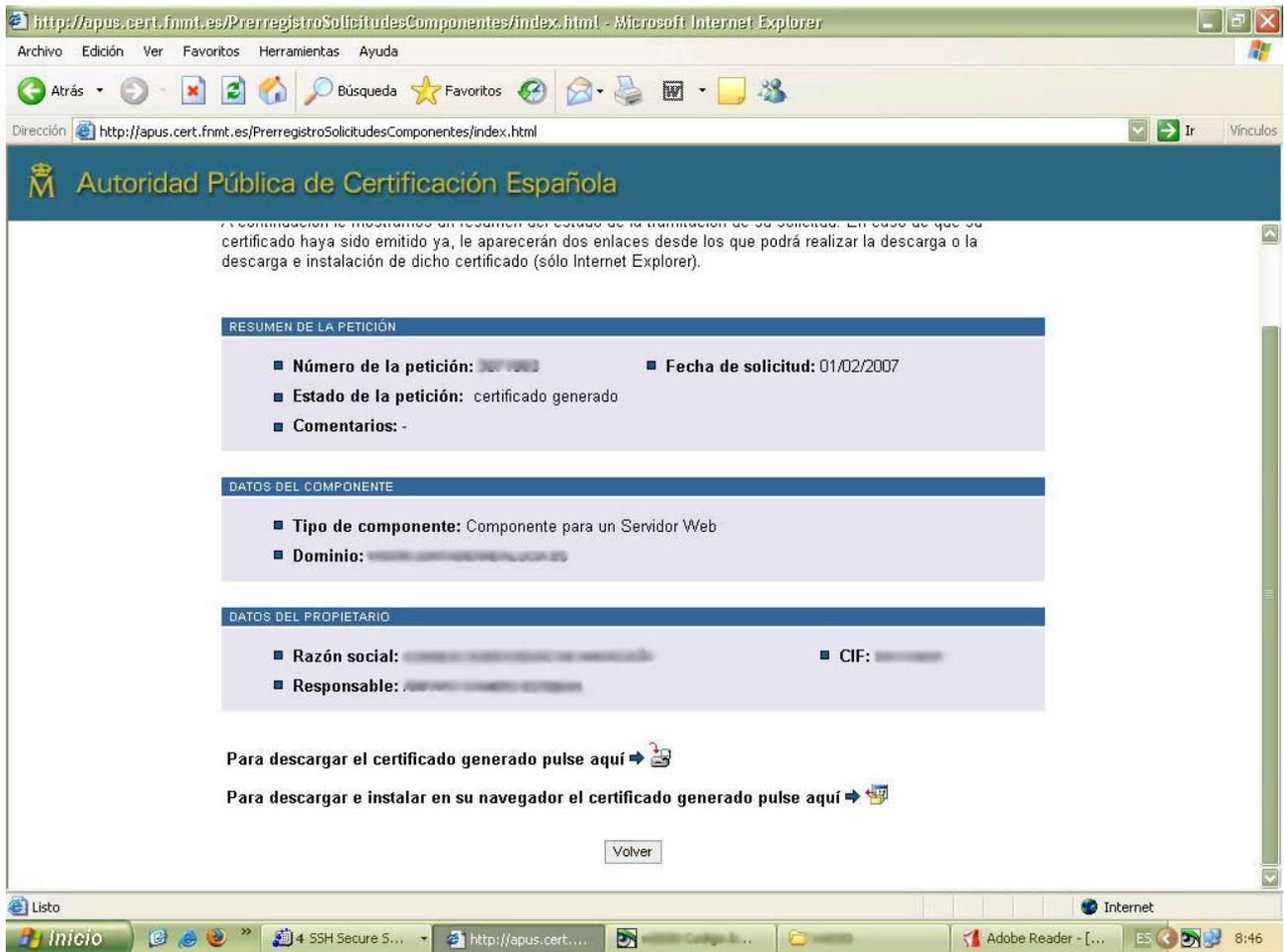
En caso de necesidad de agilizar el proceso, puede enviarlo por fax al 91 566 6905.

Si necesita alguna aclaración adicional o si tiene alguna incidencia en el procedimiento de petición del certificado, no dude en consultarnos a info.admonelectronica@juntadeandalucia.es

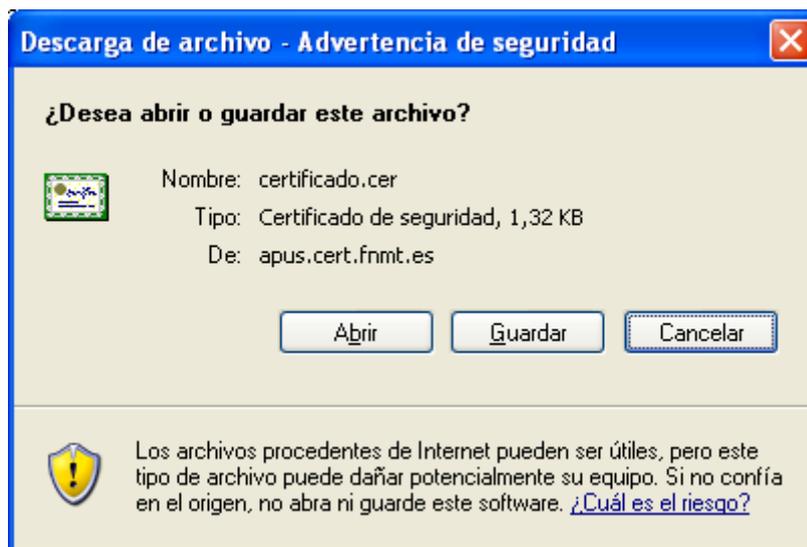
Tras realizar el envío y trascurridas aproximadamente 72 horas, puede consultar el estado de su solicitud en la página <http://apus.cert.fnmt.es/PrerregistroSolicitudesComponentes/index.html> en la sección remarcada en la siguiente captura, introduciendo el CIF del Solicitante y el Código:

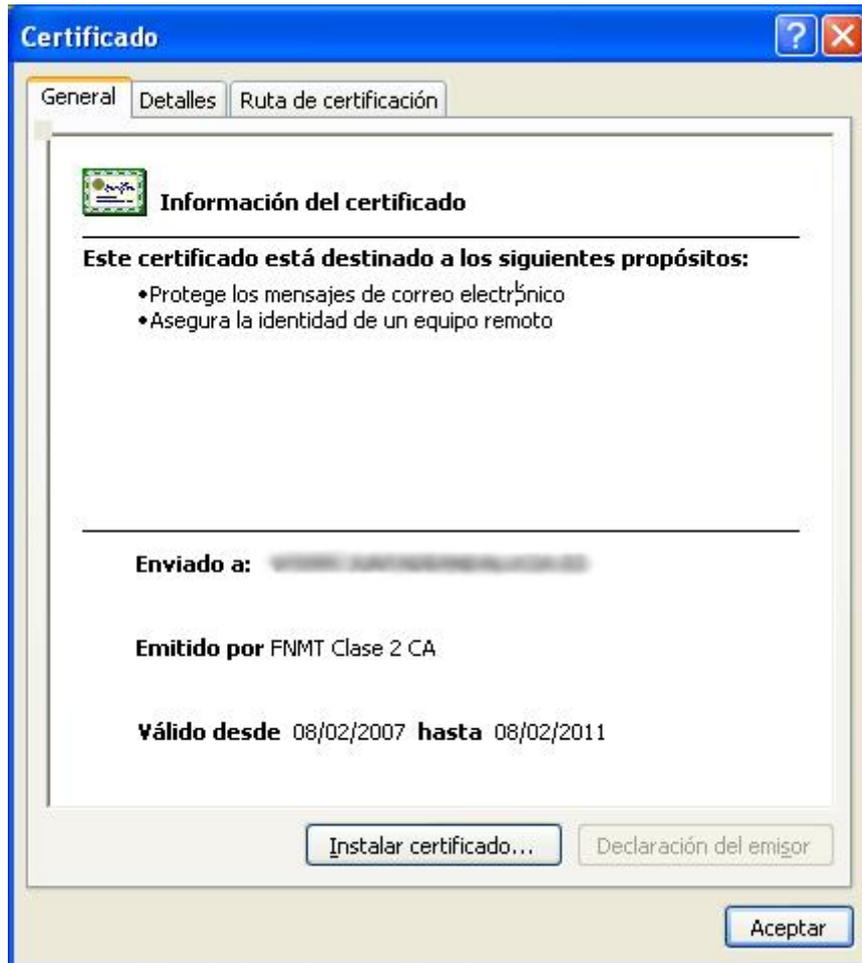
The screenshot shows the website interface for the 'Autoridad Pública de Certificación Española'. The main heading is 'OBTENGA SU CERTIFICADO DE COMPONENTE'. Below this, there is a section titled 'SOLICITUDES EN CURSO' which is circled in red. This section contains a form with the following fields: 'Nº PETICIÓN:' and 'CIF:'. A 'Consultar' button is located below these fields. To the right of the form, there is a list of links for requesting certificates, including 'Solicitar un certificado de F.N.M.T. Clase 2 CA para un servidor web identificado por el nombre del dominio', 'Solicitar un certificado de F.N.M.T. Clase 2 CA para un servidor web identificado por la dirección IP', 'Solicitar un certificado de F.N.M.T. Clase 2 CA para firma de software', 'Solicitar un certificado de F.N.M.T. Clase 2 CA para clientes de servicios avanzados', and 'Solicitar un certificado de F.N.M.T. Clase 2 CA para componentes informáticos genéricos'. Below the form, there is a 'GENERACIÓN DE CLAVES' section with a 'Generar claves' button. At the bottom of the page, there is a note that says 'IMPRESCINDIBLE'.

Si su solicitud se ha tramitado correctamente, obtendrá una ventana que le mostrará la siguiente información donde podrá descargar el certificado generado o descargar e instalar dicho certificado generado:

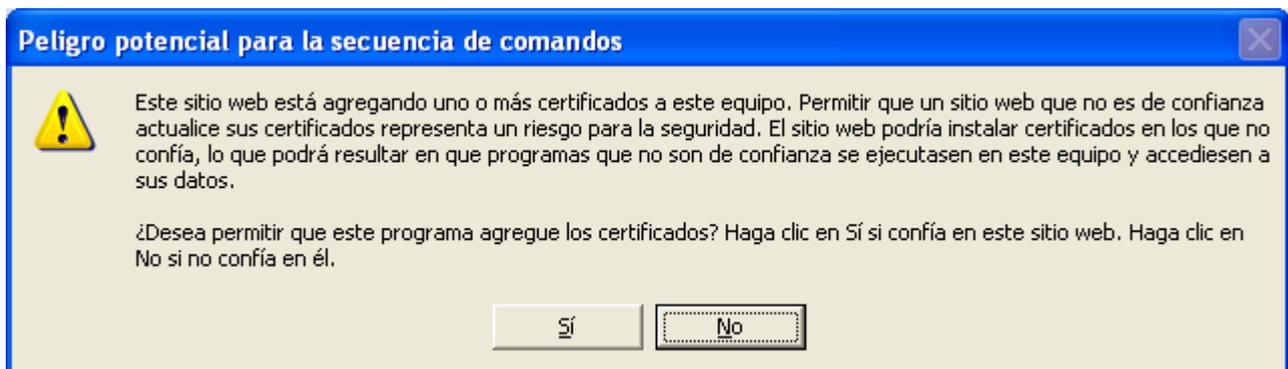


Con la descarga del certificado generado podrá obtener un fichero con extensión “cer” que podrá guardar, para posteriormente instalarlo si lo desea:



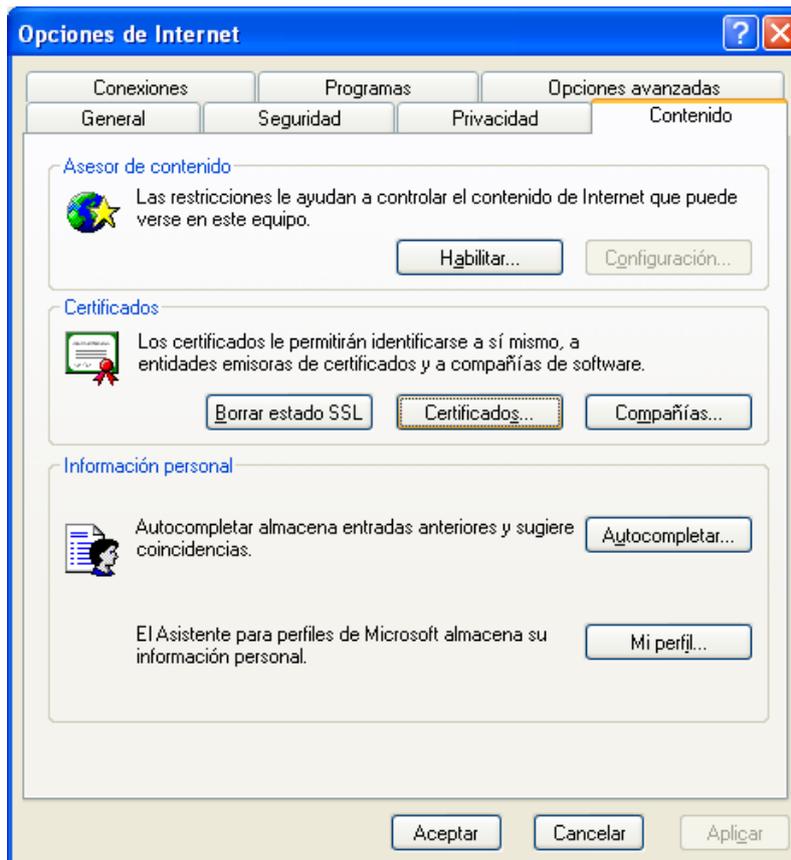


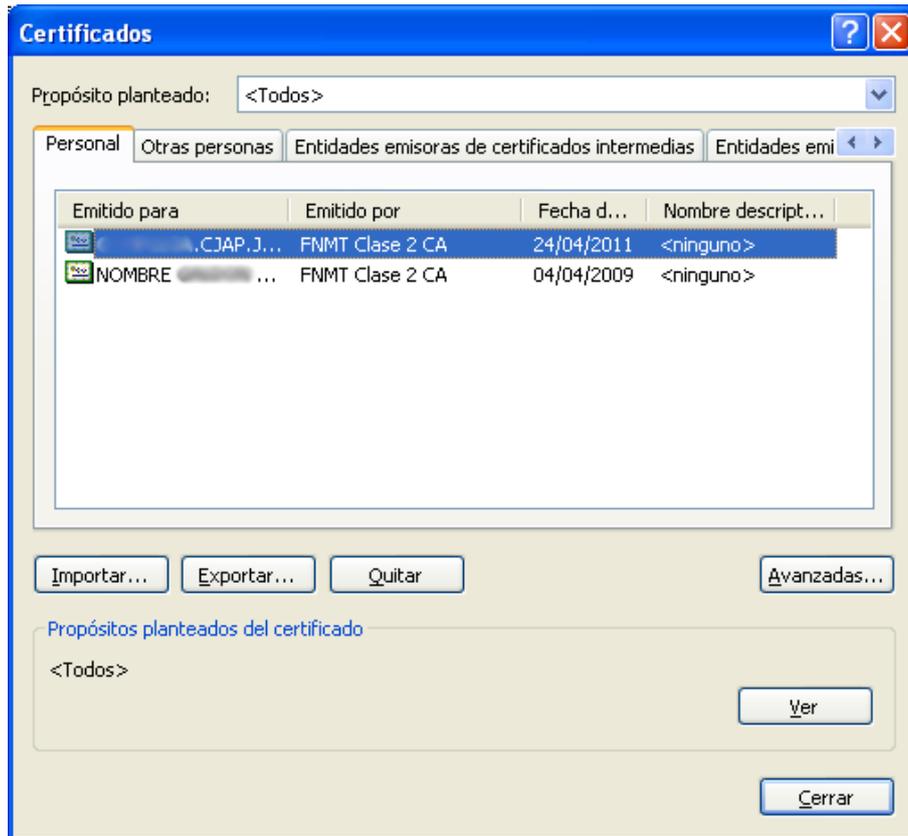
Si elige la opción de descargar e instalar el certificado en su navegador, le aparecerá la siguiente relación de capturas:





Una vez descargado e instalado, puede exportar con su clave privada para obtener los archivos “pfx” necesarios para su servidor. El proceso a seguir será el siguiente:

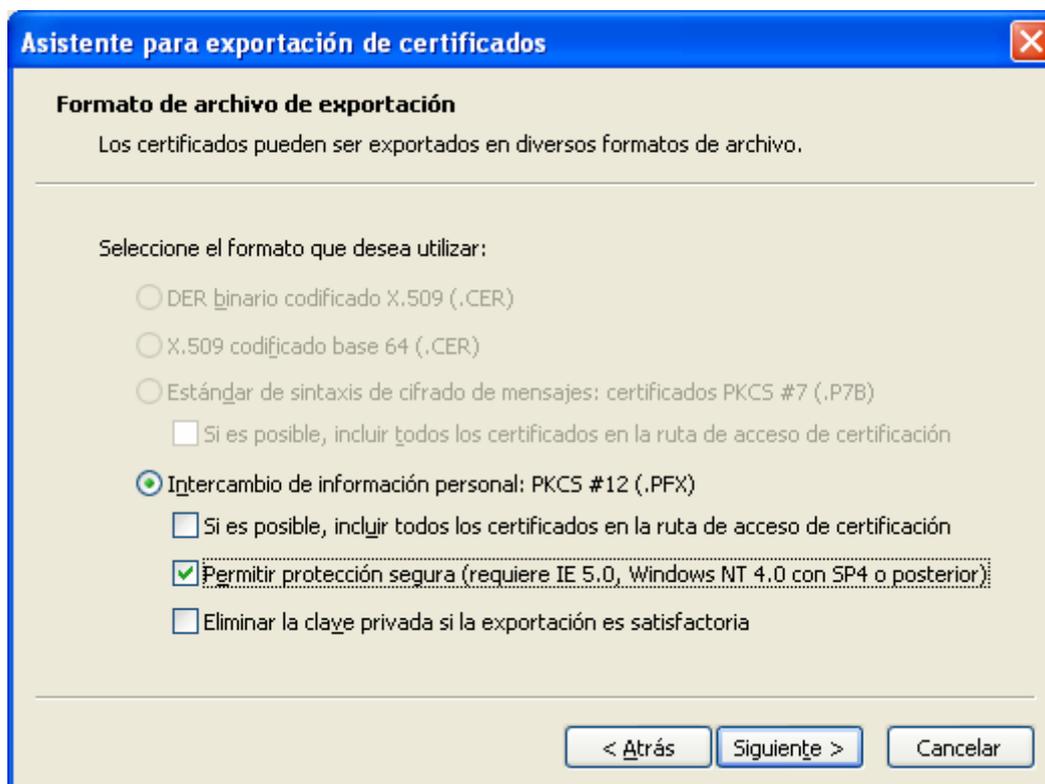




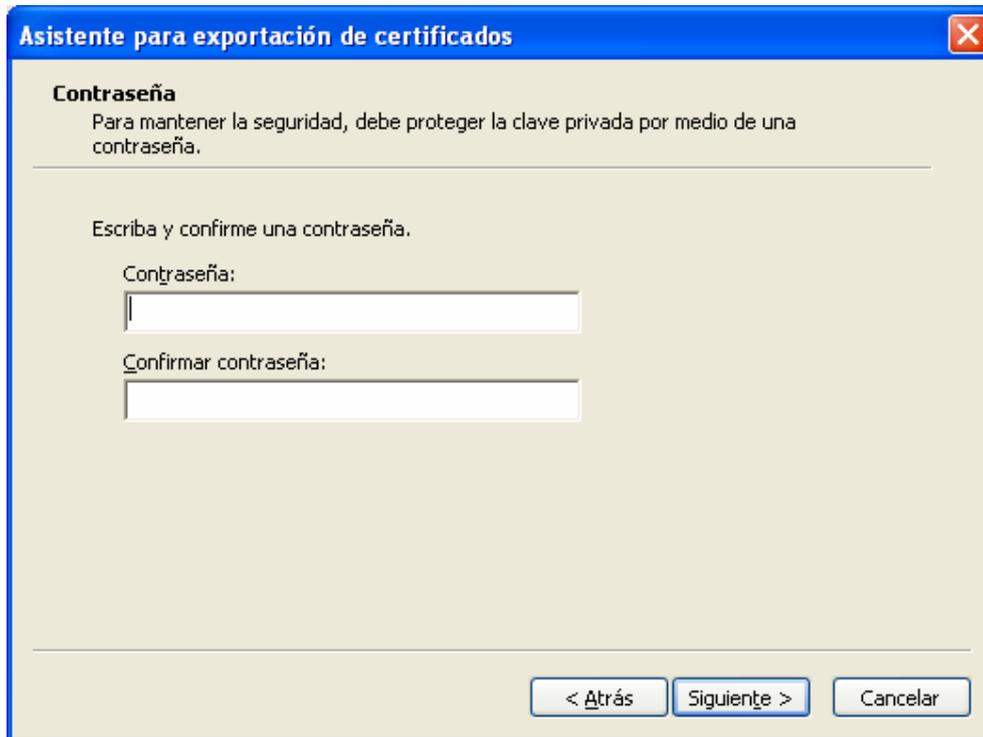
Seleccionando el certificado en cuestión, pulsamos en Exportar, realizando el proceso siguiendo estas ventanas:



Seleccionar “Exportar la Clave Privada”, definiendo a posteriori el formato de almacenamiento:



Debe definir la contraseña para proteger la información de su certificado. Posteriormente a la definición de la contraseña, deberá especificar una ruta donde almacenar el archivo pfx a generar:



Asistente para exportación de certificados

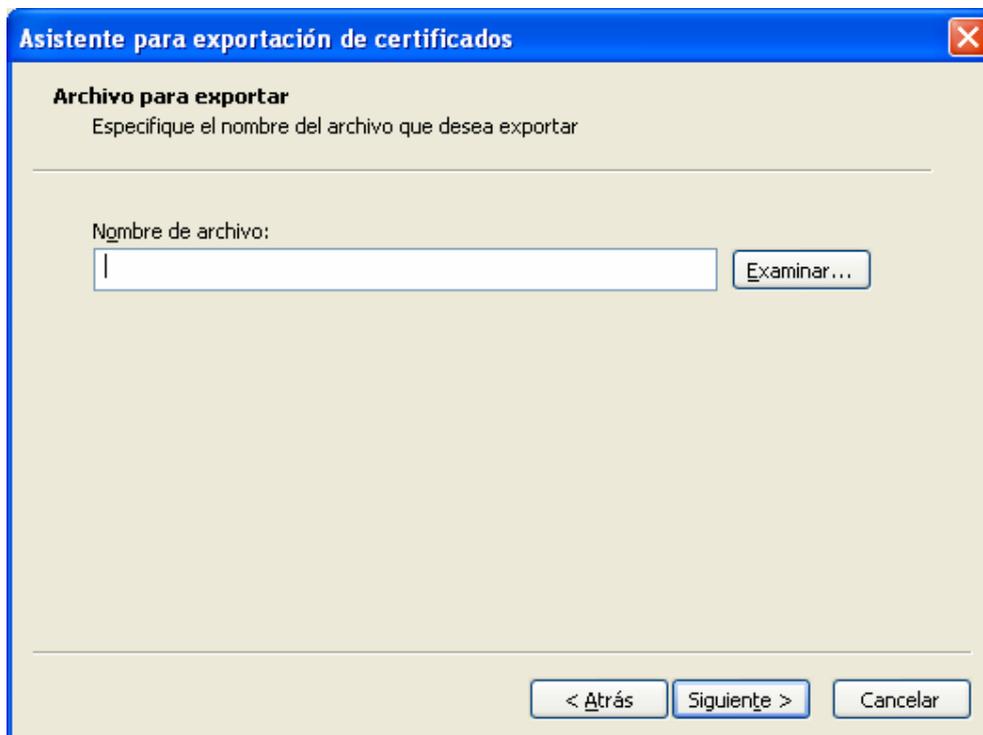
Contraseña
Para mantener la seguridad, debe proteger la clave privada por medio de una contraseña.

Escriba y confirme una contraseña.

Contraseña:

Confirmar contraseña:

< Atrás Siguiete > Cancelar



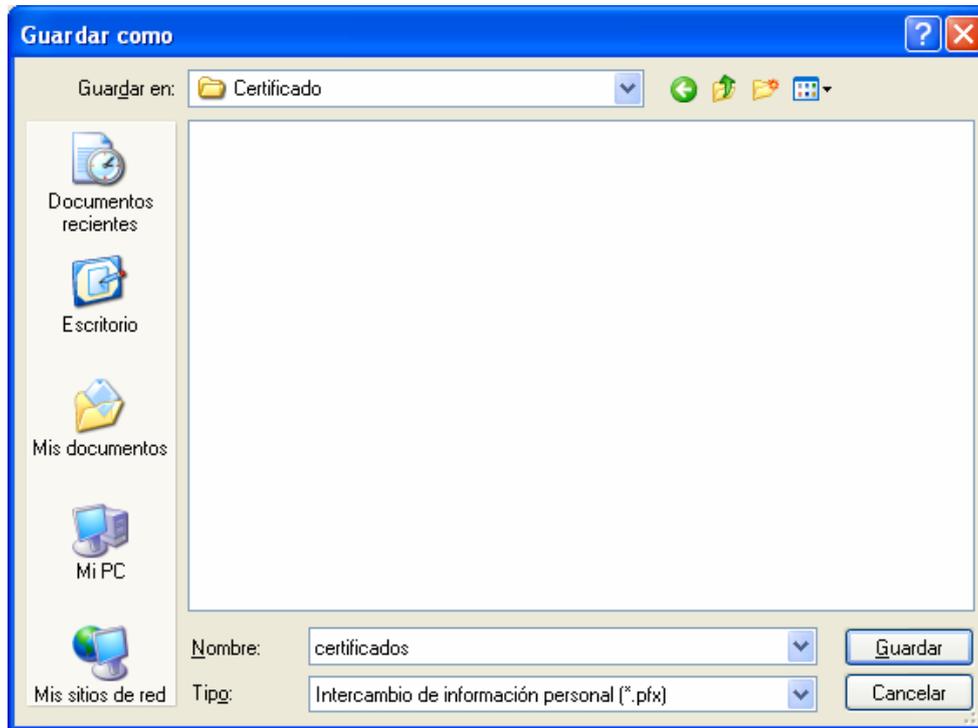
Asistente para exportación de certificados

Archivo para exportar
Especifique el nombre del archivo que desea exportar

Nombre de archivo:
 Examinar...

< Atrás Siguiete > Cancelar

Pulsando en el botón Examinar, definimos la ruta y el nombre:



Tras pulsar en finalizar, le aparecen las siguientes ventanas:



Instalación del certificado en servidor de aplicaciones tipo Apache

Los servidores web de las características del Apache, para configurar que sus aplicaciones que funcionen bajo ssl, necesitan separar la clave privada y la clave pública, del certificado web solicitado (fichero extensión *.p12 o *.pfx)

Una vez obtenido el fichero de extensión *.p12 o *.pfx del certificado ssl de servidor web a través de la herramienta de FNMT-RCM, siguiendo las instrucciones anteriormente descritas, es necesario separarlo en dos ficheros necesarios para la configuración del Apache, para ello se usará la herramienta criptográfica Openssl, disponible tanto para sistemas Windows como Linux.

Paso 1

Exporta la clave privada del fichero de extensión pfx o p12

```
openssl pkcs12 -in certificadoServidorWeb.pfx -nocerts -out key.pem
```

Paso 2

Elimina la palabra de paso de la clave privada para facilitar su implantación en el Apache.

Obtenemos la clave privada

```
openssl rsa -in key.pem -out server.key
```

Paso 3

Exporta la clave pública a partir del fichero de extensión pfx o p12

```
openssl pkcs12 -in certificadoServidorWeb.pfx -clcerts -nokeys -out cert.pem
```

Para más información específica sobre como configurar su Apache, accede a la página oficial de Apache Web Server en <http://httpd.apache.org/>

Instalación del certificado en servidor de aplicaciones tipo JBoss o Tomcat

Una vez obtenido el fichero de extensión *.p12 o *.pfx del certificado ssl de servidor web a través de la herramienta de FNMT-RCM anteriormente descritas, se deben seguir las instrucciones concretas para configurar el ssl en el servidor web de aplicaciones concreto del que dispongamos.