



**Real Casa de la Moneda**  
Fábrica Nacional  
de Moneda y Timbre

**DIRECCIÓN DE SISTEMAS DE INFORMACIÓN**  
**DEPARTAMENTO CERES**

**MANUAL SOLICITUD CERTIFICADO DE AUTENTICACIÓN DE SITIO WEB**

	<b>NOMBRE</b>	<b>FECHA</b>
Elaborado por:	Soporte Técnico	05/06/2021
Revisado por:		
Aprobado por:		

<b>HISTÓRICO DEL DOCUMENTO</b>			
<b>Versión</b>	<b>Fecha</b>	<b>Descripción</b>	<b>Autor</b>
1.0	05/06/2021	Creación del documento	Soporte Técnico
1.1	17/10/2022	Modificación del documento	Soporte Técnico
1.2	01/09/2023	Modificación del documento	Soporte Técnico
1.3	29/02/2024	Modificación del documento	Soporte Técnico

**Referencia:**

**Documento clasificado como:** *Público*

## Contenido

1.	INTRODUCCIÓN.....	3
2.	APLICACIONES .....	3
2.1.	Generación de claves GCCC .....	3
2.2.	Aplicación Solicitud de Certificados.....	3
3.	ETAPA 1. GENERACIÓN DE LAS CLAVES PARA CERTIFICADO DE COMPONENTE ....	4
4.	ETAPA 1. GENERACIÓN DE LAS CLAVES PARA CERTIFICADOS OV Y EV .....	5
5.	SOLICITUD DEL CERTIFICADO.....	6
6.	VALIDACIÓN DEL CORREO ELECTRÓNICO .....	10
7.	ENVIAR CONTRATO FIRMADO.....	12
8.	DESCARGA PARTE PÚBLICA DEL CERTIFICADO.....	13
9.	ETAPA 2. GENERACIÓN DEL CERTIFICADO .....	14
10.	CONTACTO .....	16
11.	DECLARACION DE LAS PRACTICAS DE CERTIFICACIÓN .....	16

## 1. INTRODUCCIÓN

El presente documento describe el funcionamiento de la aplicación desarrollada por el departamento CERES, para la generación de claves y la solicitud de certificados de autenticación de sitios web de la FNMT-RCM.

Es un proceso guiado paso a paso de cómo obtener un certificado de componentes.

## 2. APLICACIONES

### 2.1. GENERACIÓN DE CLAVES GCCC

Esta aplicación tiene dos funcionalidades una es la propia generación de las claves que se deberán luego facilitar en la aplicación de pre-registro de componentes.

Y la generación del correspondiente fichero p12/pfx con el certificado completo. La necesidad de la generación de este fichero dependerá del tipo de servidor de aplicaciones que se utilice y los requerimientos del mismo para instalar el certificado, además del tipo de certificado que se haya solicitado.

La aplicación es un fichero jar autoejecutable, por lo que se requiere tener instalada la máquina virtual de Java (JRE) en su versión 8.

La aplicación puede descargarse desde la página de la FNMT-RCM.

<https://www.cert.fnmt.es/componente/generacion-claves>

**Opción alternativa a la aplicación Generación de claves GCCC:** Uno de los datos a aportar en el formulario web (4º Paso) es el PKCS#10 o CSR, con la clave privada a incluir en el certificado. Este dato se obtiene tras la generación de las claves de curva elíptica. Normalmente la generación de las claves se realiza, por seguridad, en el propio servidor utilizando las herramientas proporcionadas por el software/hardware que va a utilizar el certificado.

- **Certificados de Componente:** Las **claves RSA que generen** en el servidor deben tener un tamaño de **2048 bits**.
- **Certificados OV y EV:** Las **claves de curva elíptica que se generen** en el servidor deben tener un formato **ECC P-384**.

### 2.2. APLICACIÓN SOLICITUD DE CERTIFICADOS

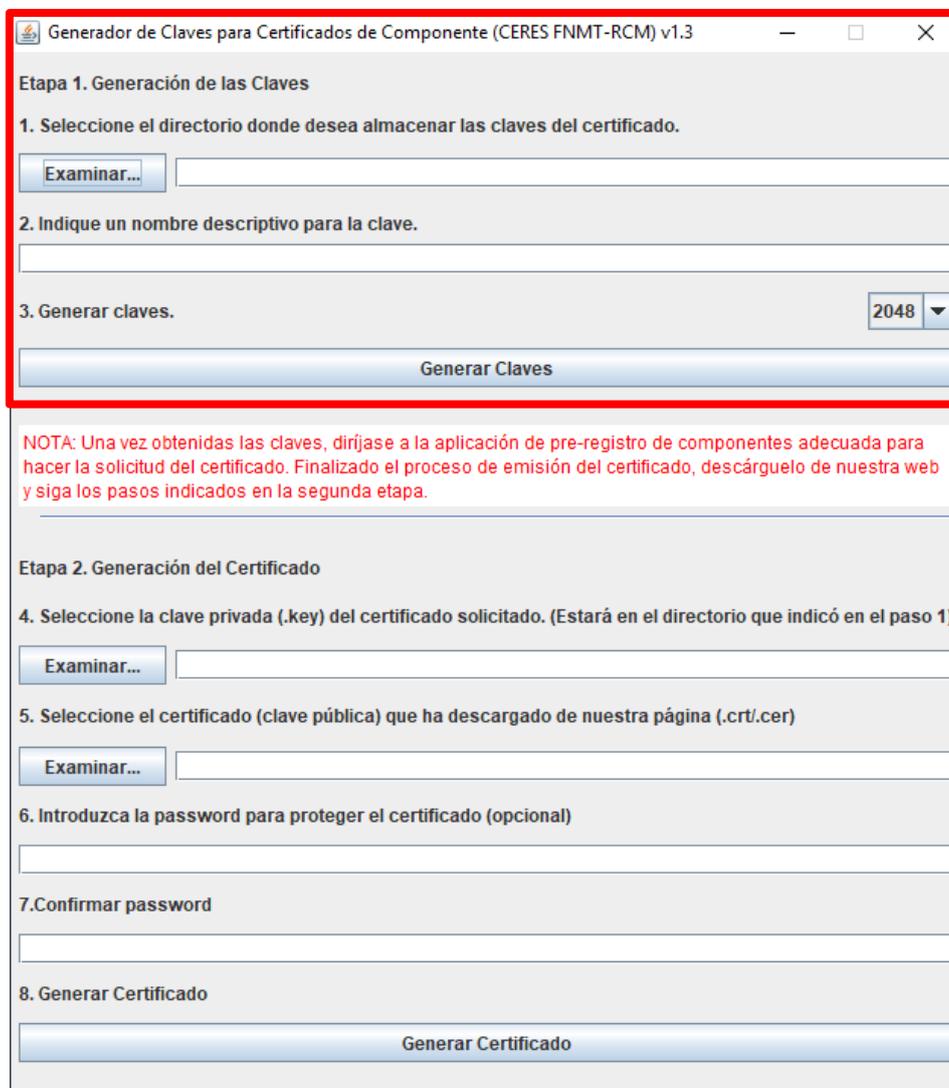
Esta aplicación su función es la solicitud de emisión, revocación, envío de contratos y descarga del certificado de componentes.

Para acceder deberá pulsar en el siguiente link:

<https://apus20.cert.fnmt.es/SolicitudCertComp/>

**NOTA:** Puede acceder desde cualquier navegador (menos **Internet Explorer** ya que no soporta **HTML5**).

### 3. ETAPA 1. GENERACIÓN DE LAS CLAVES PARA CERTIFICADO DE COMPONENTE



Etapa 1. Generación de las Claves

1. Seleccione el directorio donde desea almacenar las claves del certificado.

Examinar...

2. Indique un nombre descriptivo para la clave.

3. Generar claves. 2048

Generar Claves

NOTA: Una vez obtenidas las claves, diríjase a la aplicación de pre-registro de componentes adecuada para hacer la solicitud del certificado. Finalizado el proceso de emisión del certificado, descárguelo de nuestra web y siga los pasos indicados en la segunda etapa.

Etapa 2. Generación del Certificado

4. Seleccione la clave privada (.key) del certificado solicitado. (Estará en el directorio que indicó en el paso 1)

Examinar...

5. Seleccione el certificado (clave pública) que ha descargado de nuestra página (.crt/.cer)

Examinar...

6. Introduzca la password para proteger el certificado (opcional)

7. Confirmar password

8. Generar Certificado

Generar Certificado

Para obtener las claves siga los pasos aquí descritos, que se identifican con los pasos indicados en la aplicación:

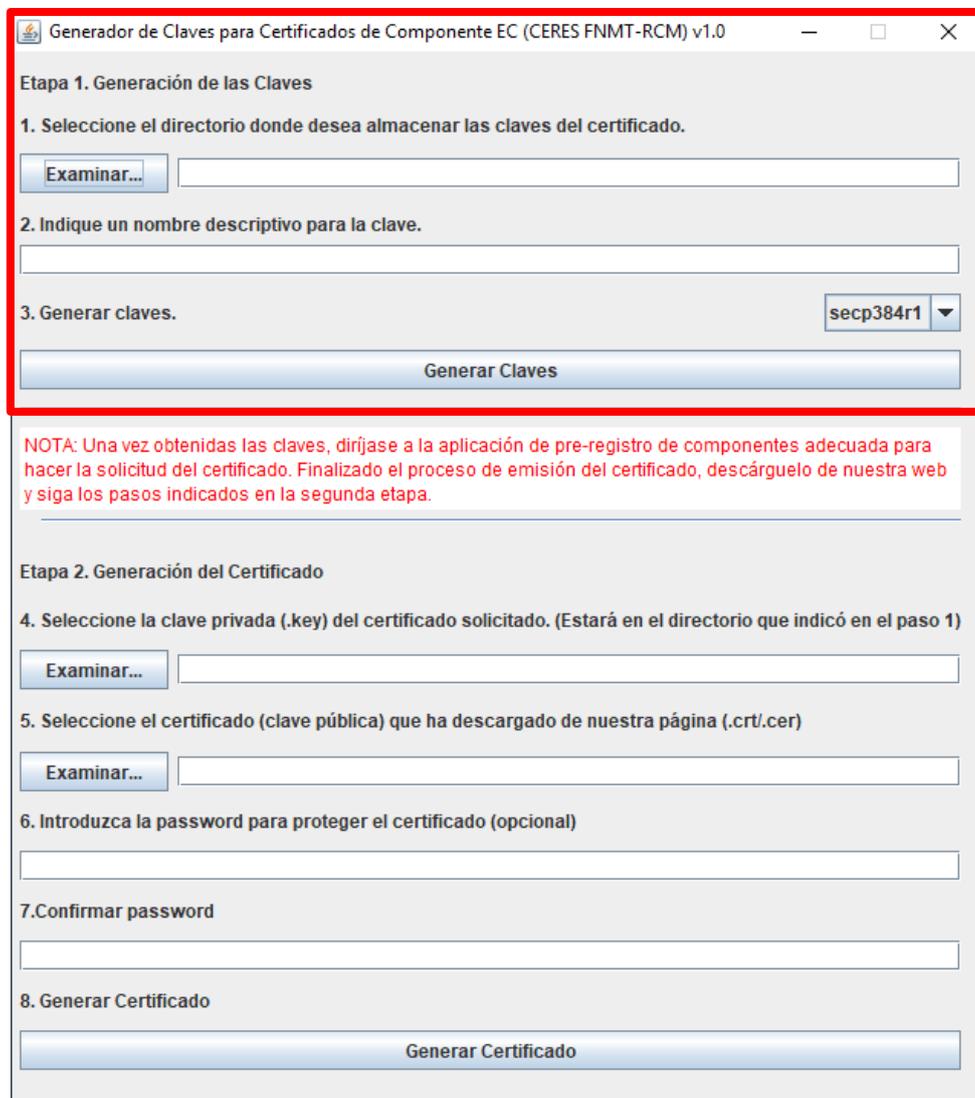
**Paso 1:** En primer lugar debemos seleccionar el directorio donde queremos almacenar los ficheros que van a contener la clave privada y el PKCS#10 que deberemos proporcionar en el formulario de pre-registro de componentes.

**Paso 2:** Le damos un nombre descriptivo a los ficheros que vamos a generar.

**Paso 3:** Generar claves, en el directorio seleccionado en el **paso 1** se crean dos archivos con el nombre indicado en el **paso 2**. Uno de los ficheros tendrá extensión .key, es la clave privada del certificado, y otro tendrá extensión .pkcs10.

El archivo con extensión pkcs10 contiene la información que deberemos pegar en el formulario de pre-registro de componentes, este fichero lo abriremos con un editor de texto y pegaremos su contenido en el citado formulario.

#### 4. ETAPA 1. GENERACIÓN DE LAS CLAVES PARA CERTIFICADOS OV Y EV



Etapa 1. Generación de las Claves

1. Seleccione el directorio donde desea almacenar las claves del certificado.

Examinar...

2. Indique un nombre descriptivo para la clave.

3. Generar claves. secp384r1 ▼

Generar Claves

**NOTA:** Una vez obtenidas las claves, diríjase a la aplicación de pre-registro de componentes adecuada para hacer la solicitud del certificado. Finalizado el proceso de emisión del certificado, descárguelo de nuestra web y siga los pasos indicados en la segunda etapa.

Etapa 2. Generación del Certificado

4. Seleccione la clave privada (.key) del certificado solicitado. (Estará en el directorio que indicó en el paso 1)

Examinar...

5. Seleccione el certificado (clave pública) que ha descargado de nuestra página (.crt/.cer)

Examinar...

6. Introduzca la password para proteger el certificado (opcional)

7. Confirmar password

8. Generar Certificado

Generar Certificado

Para obtener las claves siga los pasos aquí descritos, que se identifican con los pasos indicados en la aplicación:

**Paso 1:** En primer lugar debemos seleccionar el directorio donde queremos almacenar los ficheros que van a contener la clave privada y el PKCS#10 que deberemos proporcionar en el formulario de pre-registro de componentes.

**Paso 2:** Le damos un nombre descriptivo a los ficheros que vamos a generar.

**Paso 3:** Generar claves, en el directorio seleccionado en el **paso 1** se crean dos archivos con el nombre indicado en el **paso 2**. Uno de los ficheros tendrá extensión .key, es la clave privada del certificado, y otro tendrá extensión .pkcs10.

El archivo con extensión pkcs10 contiene la información que deberemos pegar en el formulario de pre-registro de componentes, este fichero lo abriremos con un editor de texto y pegaremos su contenido en el citado formulario.

## 5. SOLICITUD DEL CERTIFICADO



Sede Electrónica FNMT | Declaración Prácticas de Certificación | Soporte Técnico | +Info

## Certificados de componente de la FNMT-RCM



### Certificados de autenticación de sitio web

Los certificados autenticación de sitio web se utilizan para acreditar la identidad de un servidor web y establecer una comunicación segura con los usuarios mediante protocolos de comunicación cifrada como SSL. Disponer de un certificado de autenticación de sitio web ofrece garantías y seguridad a los usuarios que acceden a un sitio web.

Solicitar emisión

Solicitar revocación

Enviar contrato

Descargar certificado

Tras la generación de las claves vamos a proceder a realizar la solicitud, para ello deberemos pulsar en el botón *Solicitar emisión*.

## Solicitud de emisión de certificados de autenticación de sitio web

Los servicios de autenticación de sitios web proporcionan un medio por el que puede garantizarse a la persona que visita un sitio web que existe una entidad auténtica y legítima que respalda la titularidad del sitio web. Recuerde que una vez descargado el contrato y antes de su envío, ha de ser firmado electrónicamente por el representante del suscriptor del certificado. Esta comprobación se realizará una vez remitida la documentación a la FNMT-RCM y antes de su expedición.

### Certificados de componente

El certificado electrónico de componente es utilizado por servidores web y otros componentes informáticos para, según el tipo de certificado, garantizar la autenticación de los mismos y/o realizar firmas electrónicas.

- Certificado SSL estándar
- Certificado SSL Wildcard
- Certificado SSL multidominio (SAN/UCC)

### Certificados OV

Los certificados OV (validación organización) confirman la existencia de la entidad y la titularidad del dominio.

- Certificado SSL OV
- Certificado SSL Wildcard OV
- Certificado Multidominio (SAN/UCC) OV

### Certificados EV

Los certificados EV (validación extendida) confirman la existencia de la entidad, de la representación legal de la misma y la titularidad del dominio.

- Certificado SSL EV
- Certificado Multidominio (SAN/UCC) EV
- Certificado Cualificado de SEDE Electrónica EV

Pulse aquí para consultar y aceptar los términos y condiciones de uso del certificado seleccionado

[Solicitar Certificado](#) [Volver](#)

Marcamos el certificado que queremos solicitar y pulsamos para aceptar los términos y condiciones.

A continuación, deberemos pulsar el botón *Solicitar Certificado*, en esta página tenemos el formulario de pre-registro de componentes donde tendremos que rellenar los campos obligatorios.

## Solicitud de expedición de certificado de autenticación de sitios web SEDE

### INSTRUCCIONES:

- Asegúrese de que los correos electrónicos asociados a su certificado son correctos, pues serán los utilizados para el envío de todas las notificaciones relacionadas con el ciclo de vida del certificado.
- Recuerde que para continuar con el proceso de solicitud ha de descargar el contrato (en su equipo u otro soporte electrónico) y firmarlo con un certificado (de persona física, empleado público, DNle o de representante) perteneciente al representante del suscriptor del certificado.
- En breve recibirá en la cuenta de correo electrónico indicada su CÓDIGO DE SOLICITUD. Este código le será requerido para la descarga de su certificado una vez que haya sido generado y en caso de revocación telefónica del mismo.
- Una vez descargado el contrato, y para finalizar el proceso de solicitud, envíe el contrato desde la página de inicio.



**DATOS DEL CERTIFICADO**

Nombre del dominio del certificado (\*):   


Descripción (\*):   


Fecha de publicación en el BO correspondiente (\*):   


En el caso de que no exista esta publicación, documento oficial donde se haga constar la creación de dicha sede electrónica.

**SOLICITUD PKCS#10 (Generado con claves ECC P-384)**

Estandar de solicitud de certificación (\*):   


**SUSCRIPTOR DEL CERTIFICADO**

Organismo (\*):   
Unidad Organizativa:   


Tipo de Empresa (\*):   


CIF (\*):   


Pais (\*):   
Dirección (\*):   
Código Postal (\*):   


Localidad (\*):   
Provincia (\*):   
Email (\*):   
Repita el Email (\*):   
Teléfono (\*):   


**REPRESENTANTE DEL SUSCRIPTOR**

NIF Representante (\*):   


Nombre (\*):

Primer Apellido (\*):

Segundo Apellido:

Email (\*):

Repita el Email (\*):   
Teléfono (\*):   


Acepte el Captcha

No soy un robot   
reCAPTCHA  
Privacidad · Términos

[Descargar contrato de expedición](#)

[VOLVER](#)



**Nombre del dominio del certificado:** es el nombre identificativo del dominio que queremos autenticar.  
Ejemplo; fnmt.es.

**Solicitud PKCS#10:** Aquí pondremos el archivo con extensión pkcs10 generado con la Aplicación GCCC, este fichero lo abriremos con un editor de texto y pegaremos su contenido en el citado formulario. O bien unas claves de Curva Elíptica que hayan generado.

**Suscriptor del Certificado:** los datos referentes a la entidad.

**Representante del Suscriptor:** los datos del representante de la entidad.

Una vez rellenados todos los campos, aceptamos el Captcha y pulsamos en el botón *Descargar contrato de expedición*.

Buscamos el contrato generado en la carpeta que tengamos asignada a las descargas por defecto del navegador utilizado, con el nombre *ContratoSSLFNMT.pdf*

Deberemos revisar el contrato y comprobar que todos los datos introducidos sean correctos.

Una vez verificado procedemos a firmarlo electrónicamente con nuestro certificado (de persona física, empleado público, DNIE o de representante) perteneciente al representante del suscriptor del certificado.

**IMPORTANTE: La firma debe realizarse a través de Adobe Reader y no por otras aplicaciones externas de firma, ya que si no dará error al enviar el contrato.**

En caso de no saber cómo se firma electrónicamente un documento PDF con Adobe Reader y su certificado digital, puede visitar nuestra web de Preguntas Frecuentes:

[¿Cómo puedo firmar un documento PDF con Adobe Acrobat Reader DC?](#)

## 6. VALIDACIÓN DEL CORREO ELECTRÓNICO

Para realizar la validación de su correo electrónico se remitirá un código aleatorio a la dirección de correo que ha rellenado en el formulario. Se debe introducir el código en la siguiente pantalla, para continuar.



### Valide su correo electrónico

Le hemos enviado un correo electrónico a la dirección **EJEMPLO@EJEMPLO.ES**. Por favor, introduzca el código recibido para validar su dirección de correo:

Código de validación:

Si no recibe el correo, o la validación ha fallado y necesita un nuevo código de validación pinche [aquí](#).

Una vez introducido el código de validación podremos descargar el contrato, deberemos firmarlo y enviarlo.



### Su correo ha sido validado correctamente

A continuación se descargará el contrato. Deberá firmarlo y enviárnoslo pinchando [aquí](#).



*EJEMPLO DE CONTRATO DE EXPEDICIÓN*



**SOLICITUD DE EXPEDICION DE CERTIFICADOS DE SEDE ELECTRÓNICA EV**

**IDENTIFICACIÓN DE LA SOLICITUD**

DOMINIO DEL CERTIFICADO	<input type="text" value="fnmt.es"/>
DESCRIPCIÓN DEL CERTIFICADO	<input type="text" value="Sede FNMT"/>
FECHA DE PUBLICACIÓN EN EL BO	<input type="text" value="01/01/2021"/>

**SUSCRIPTOR DEL CERTIFICADO**

TIPO DE EMPRESA	<input type="text" value="Administración Pública"/>		
ORGANISMO	<input type="text" value="FNMT-RCM"/>		
NIF	DIRECCIÓN	PROVINCIA	
<input type="text" value="Q2826004J"/>	<input type="text" value="Calle Jorge Juan 106"/>	<input type="text" value="MADRID"/>	
C.POSTAL	LOCALIDAD	PAÍS	
<input type="text" value="28009"/>	<input type="text" value="Madrid"/>	<input type="text" value="España"/>	
DIRECCIÓN DE CORREO ELECTRÓNICO	TELÉFONO		
<input type="text" value="FNMT@FNMTES"/>	<input type="text" value="+34 915666666"/>		

**REPRESENTANTE DEL SUSCRIPTOR**

NIF	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
<input type="text" value="00000000T"/>	<input type="text" value="Juan"/>	<input type="text" value="Español"/>	<input type="text" value="Español"/>
DIRECCIÓN DE CORREO ELECTRÓNICO			
<input type="text" value="FNMT@FNMTES"/>			

- Botón derecho sobre el recuadro de firma
- Firmar documento
- Seleccionar el certificado
- Guardar documento
- Enviar documento firmado

"Firmado por **FIRMA CONTRATOS FNMT PRO** el día 26/06/2021"



Firma electrónica del representante del suscriptor



## 7. ENVIAR CONTRATO FIRMADO

### Enviar contrato firmado

Arrastre el contrato desde su ubicación a la imagen o pulse sobre ella para examinar archivos



CONTRATOSLFINMT.PDF

No soy un robot 

reCAPTCHA  
Privacidad · Términos

Arrastre el contrato desde su ubicación a la imagen o pulse sobre ella para examinar archivos.

Marque el Captcha y pulse el botón *Enviar*.

Se iniciará el proceso de envío y por ultimo aparecerá la confirmación de recepción, indicándole que en el correo facilitado recibirá en breve su código de solicitud asociado a su petición.

## CONTRATO ENVIADO

El contrato se ha enviado correctamente.

En breve recibirá un correo electrónico con el código de solicitud asociado a su petición.

Este código le será requerido para la descarga de su certificado una vez que haya sido generado, trámite que le será notificado una vez validada la documentación remitida.

## 8. DESCARGA PARTE PÚBLICA DEL CERTIFICADO

### Descarga de certificados de autenticación de sitio web

Consulte el estado de su solicitud y en caso de haber sido aprobada, podrá descargar su certificado.



Seleccione el tipo de certificado que quiere descargar

**Certificados de componente**

- SSL estándar
- SSL Wildcard
- SSL multidominio (SAN/UCC)

**Certificados OV**

- SSL OV
- SSL Wildcard OV
- Multidominio (SAN/UCC) OV

**Certificados EV**

- SSL EV
- Multidominio (SAN/UCC) EV
- Cualificado de SEDE Electrónica EV

Introduzca los siguientes datos correspondientes a su solicitud

Dominio:

Código de solicitud:

[Consultar estado solicitud](#)

[Volver](#)

Seleccionamos el certificado que queremos descargar y rellenamos los datos que nos solicitan, a continuación, pulsamos el botón *Consultar estado solicitud*.

### Descarga de certificados de autenticación de sitio web

#### Datos de la solicitud

Autoridad de certificación emisora:

Tipo de solicitud:

Código de solicitud:

Número de petición:

#### Eventos asociados a la solicitud

NÚMERO	OPERACIÓN REALIZADA	FECHA DE OPERACIÓN
1	Certificado descargado por parte del usuario.	25-06-2021 14:21:49
2	Certificado revocado.	08-06-2021 17:32:51
3	Certificado descargado por parte del usuario.	25-05-2021 10:39:53
4	Certificado generado (listo para descargar por el usuario en certificados Web).	20-05-2021 15:42:52
5	Petición lista para ser procesada	20-05-2021 15:42:48
6	Pendiente de aprobación	17-05-2021 16:34:26
7	Solicitud de preregistro recibida e insertada, pendiente de procesar	17-05-2021 16:34:26

[Continuar >>](#)

[Volver](#)

Como podéis ver en esta captura pantalla de ejemplo, nos aparece el estado de la solicitud. Tras la autorización de la emisión del certificado aparecerá la opción “Certificado generado (listo para descargar por el usuario en certificados web)”. En ese momento podremos pulsar en el botón *Continuar*.

A continuación, se procederá con la descarga de su certificado. Recuerde que, para poder hacer uso del mismo, deberá asociarlo a las claves privadas que generó previamente.

[Pulse aquí para consultar y aceptar las condiciones de uso del certificado](#)

Descargar Certificado

Descargar Ruta de Certificación

Pulsamos el link para aceptar las condiciones y pulsamos el botón *Descargar Certificado* para obtener la parte pública.

Buscamos el certificado generado en la carpeta que tengamos asignada a las descargas por defecto del navegador utilizado, con el nombre *AC\_SERVIDORES\_SEGUROS\_TIPOX\_XXXXXXXXX.cer*

## 9. ETAPA 2. GENERACIÓN DEL CERTIFICADO

En caso de haber utilizado la opción alternativa para la generación de claves deberá de seguir el procedimiento de ese software para unir las claves.

Deberá de seguir estos pasos si usted ha generado las claves a través de nuestra aplicación de Generación GCCC, procediendo a vincular la parte pública del certificado que ha descargado desde nuestra web a las claves privadas que generó en el punto 3 de la Etapa 1, siga las instrucciones de la Etapa 2:



Generador de Claves para Certificados de Componente EC (CERES FNMT-RCM) v1.0

**Etapa 1. Generación de las Claves**

1. Seleccione el directorio donde desea almacenar las claves del certificado.

2. Indique un nombre descriptivo para la clave.

3. Generar claves.

**NOTA:** Una vez obtenidas las claves, dirjase a la aplicación de pre-registro de componentes adecuada para hacer la solicitud del certificado. Finalizado el proceso de emisión del certificado, descárguelo de nuestra web y siga los pasos indicados en la segunda etapa.

**Etapa 2. Generación del Certificado**

4. Seleccione la clave privada (.key) del certificado solicitado. (Estará en el directorio que indicó en el paso 1)

5. Seleccione el certificado (clave pública) que ha descargado de nuestra página (.crt/.cer)

6. Introduzca la password para proteger el certificado (opcional)

7. Confirmar password

8. Generar Certificado

**Paso 4:** seleccionamos en fichero con extensión .key generado en el **paso 3** de la etapa 1. Recuerde que este fichero tendrá el nombre que ha indicado en el **paso 2** y estará en el directorio que selecciono en el **paso 1**.

**Paso 5:** Seleccione el fichero .cer/crt que ha descargado de nuestra web tras la autorización a la emisión del certificado.

**Pasos 6 y 7:** Si lo desea en este paso puede poner una contraseña al p12/pfx, (fichero que contiene las claves públicas y privadas del certificado en formato estándar). Deberá introducir la misma contraseña en ambas casillas.

**Paso 8:** Generar certificado, tras pulsar el botón generaremos un fichero con extensión .p12 en el directorio donde este el fichero .key, que le hemos proporcionado a la aplicación en el **paso 4**.



## 10. CONTACTO

Cualquier duda sobre este procedimiento de solicitud y/o su documentación administrativa, pueden dirigirla a:

**Registro:** Teléfonos: 915666916 Email: [registroceres@fnmt.es](mailto:registroceres@fnmt.es)

Si su consulta es de carácter técnico, pueden dirigirse a nuestro Área de Soporte Técnico:

**Soporte Técnico:** Tlf. 915666914 Email: [soporte\\_tecnico\\_ceres@fnmt.es](mailto:soporte_tecnico_ceres@fnmt.es)

**Comercial:** Tlf. 915666948 Email: [comercial.ceres@fnmt.es](mailto:comercial.ceres@fnmt.es)

## 11. DECLARACION DE LAS PRACTICAS DE CERTIFICACIÓN

Puede revisar la DPC que rige la emisión de este tipo de certificados en la siguiente URL:

<http://www.cert.fnmt.es/dpc>

