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

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

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
1.0	05/06/2021	Creación del documento	Soporte Técnico

Referencia:

Documento clasificado como: *Público*

Contenido

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 (CURVA ELÍPTICA)

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

http://www.cert.fnmt.es/certificados/certificados-componente/generacion-claves

Opción alternativa a la aplicación Generación de claves GCCC (Curva Elíptica): 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. Recuerde que las **claves de curva elíptica que se generen** en el servidor deben tener un formato **ECC P-384 (SHA384withECDSA)**.

2.2. APLICACIÓN SOLICITUD DE CERTIFICADOS

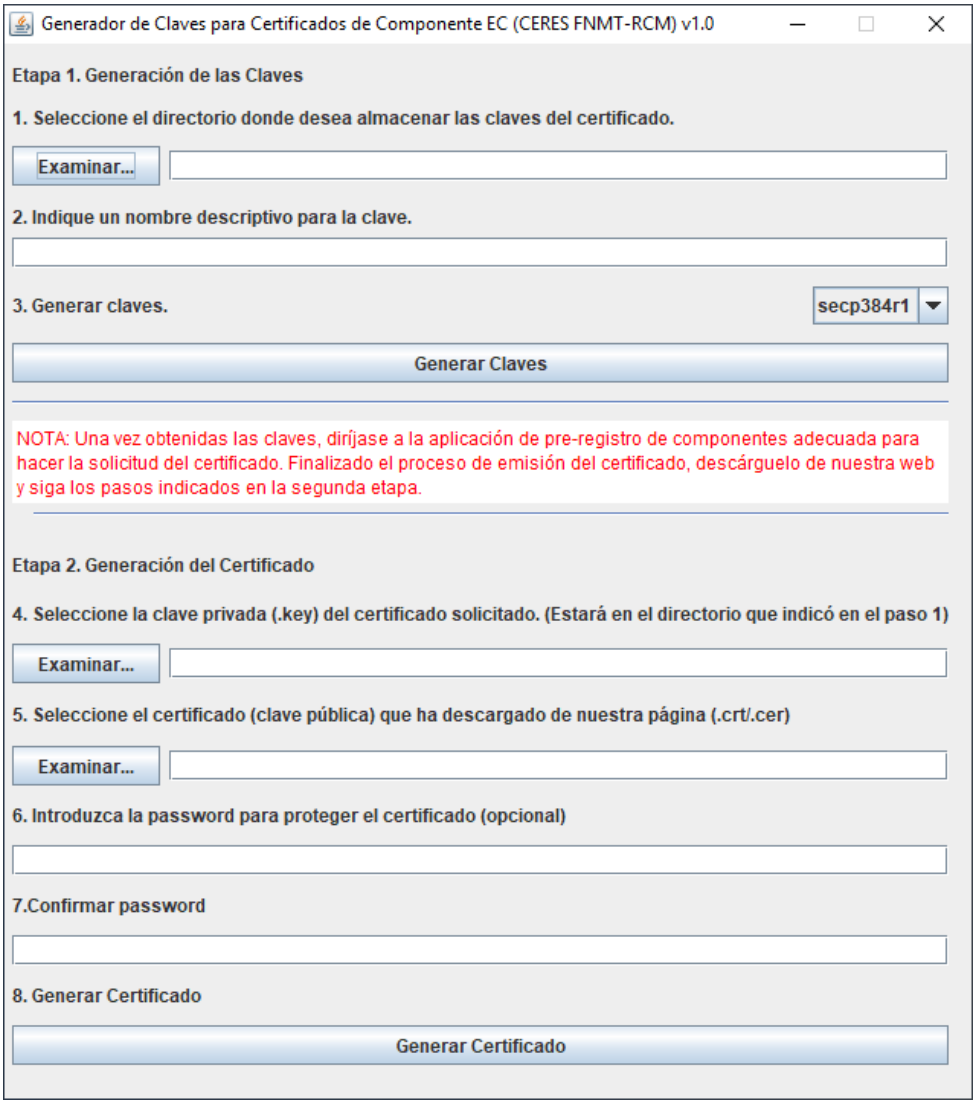
Esta aplicación su función es la solicitud de emisión, revocación, envió de contratos y descarga del certificado de componentes.

Para acceder deberá de 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 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. SOLICITUD DEL 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 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, DNIe 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 (*): Dominio del certificado

Descripción (*): Nombre o descripción de la SEDE

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

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 (*): Estandar de solicitud de certificacion

SUSCRIPTOR DEL CERTIFICADO

Organismo (*): Organismo (64).

Unidad Organizativa: Unidad Organizativa del suscriptor (64).

Tipo de Empresa (*): Administración Pública

CIF (*): CIF

Pais (*): España

Dirección (*): Dirección

Código Postal (*): Código Postal

Localidad (*): Localidad

Provincia (*):

Email (*): Email ejemplo@gmail.com

Repita el Email (*): Repita el email.

Teléfono (*): +34 000000000

REPRESENTANTE DEL SUSCRIPTOR

NIF Representante (*): NIE/DNI

Nombre (*): Nombre

Primer Apellido (*): Primer Apellido

Segundo Apellido: Segundo Apellido

Email (*): Email ejemplo@gmail.com

Repita el Email (*): Repita el email del Representante.

Teléfono (*): +34 000000000

Acepte el Captcha

No soy un robot

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 GCCCec, 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. Deberá introducirse el pkcs10 sin cabecera ni pie.

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 con 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?

EJEMPLO DE CONTRATO DE EXPEDICIÓN

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

SOLICITUD DE EXPEDICION DE CERTIFICADOS DE SEDE ELECTRÓNICA EV

IDENTIFICACIÓN DE LA SOLICITUD

DOMINIO DEL CERTIFICADO
fnmt.es

DESCRIPCIÓN DEL CERTIFICADO
Sede FNMT

FECHA DE PUBLICACIÓN EN EL BO
01/01/2021

SUSCRIPTOR DEL CERTIFICADO

TIPO DE EMPRESA
Administración Pública

ORGANISMO
FNMT-RCM

NIF	DIRECCIÓN	PROVINCIA
Q2826004J	Calle Jorge Juan 106	MADRID

C.POSTAL	LOCALIDAD	PAÍS
28009	Madrid	España

DIRECCIÓN DE CORREO ELECTRÓNICO	TELÉFONO
FNMT@FNMT.ES	+34 915666666

REPRESENTANTE DEL SUSCRIPTOR

NIF	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
00000000T	Juan	Español	Español

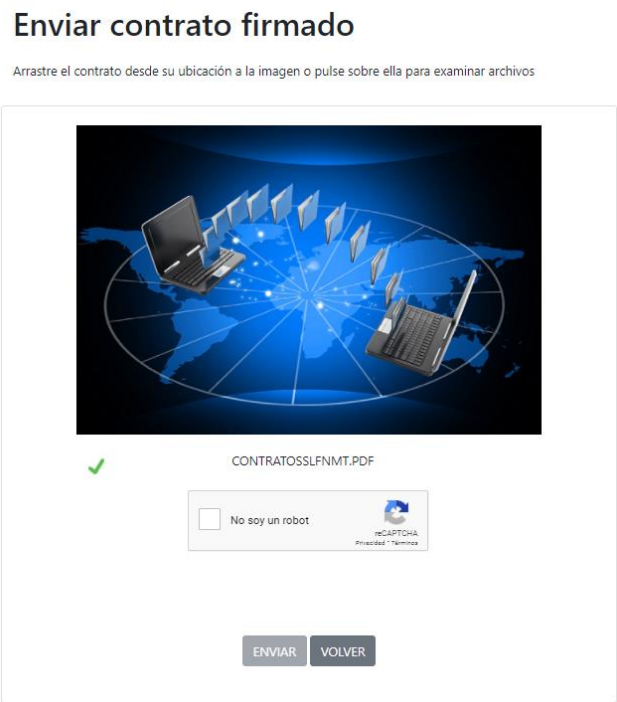
DIRECCIÓN DE CORREO ELECTRÓNICO
FNMT@FNMT.ES

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

Firma electrónica del representante del suscriptor

"Firmado por FIRMACONTRATOSFNMTPRO el día 26/06/202"

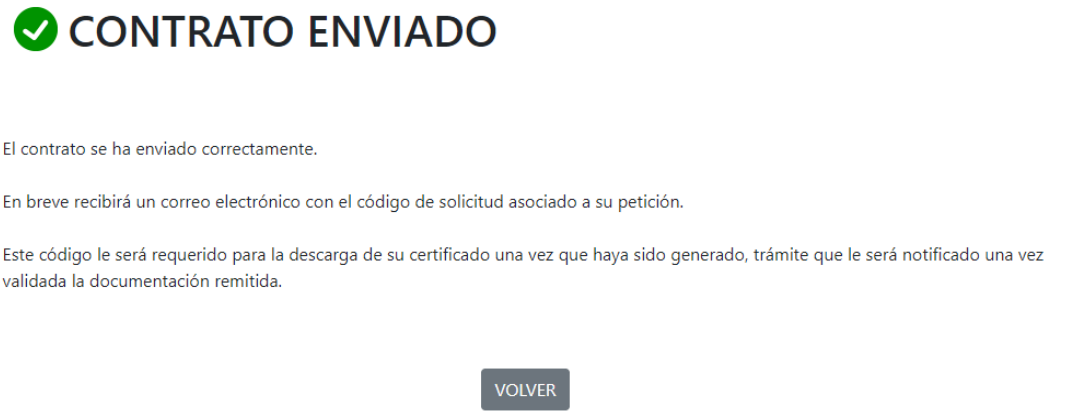
5. ENVIAR CONTRATO FIRMADO



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

Marque el Captcha y pulse el botón *Enviar*.

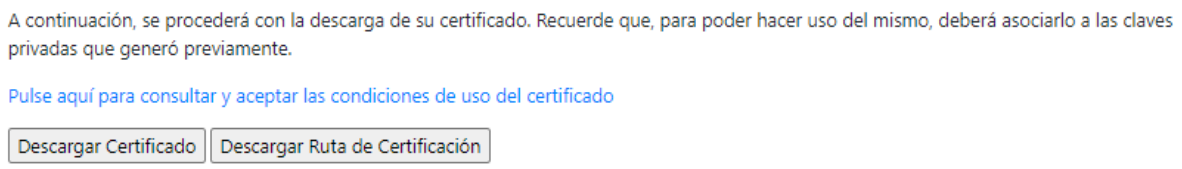
Se iniciará el proceso de envió y por ultimo aparecerá la confirmación de recepción, indicándole que en el correo facilitado recibirá en breve su código de solicitud asociado a su petición.



6. DESCARGA PARTE PÚBLICA DEL CERTIFICADO

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

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*.



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*

7. 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 GCCCec, procediendo a vincular la parte publica 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:

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.**

8. CONTACTO

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

Registro: Teléfonos: 915666916 Email: 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

Comercial: Tlf. 915666948 Email: comercial.ceres@fnmt.es

9. 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