



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES
ÁREA DE REGISTRO

**GESTIÓN DE SOLICITUDES DE REGISTRO DE CERTIFICADOS PARA LA IDENTIFICACIÓN
DE LAS SEDES ELECTRÓNICAS Y SELLOS ELECTRÓNICOS DE CERTIFICADOS PARA LA
ACTUACIÓN AUTOMATIZADA EMITIDOS POR LA FNMT - RCM BAJO LA
DENOMINACIÓN DE *CERTIFICADOS PARA LA ADMINISTRACIÓN PÚBLICA*
(*CERTIFICADOS AP*)**

(*CERTIFICADOS DE SEDE ELECTRÓNICA - CERTIFICADOS DE SELLO ELECTRÓNICO*)

[MANUAL DE REGISTRO]

V 1.2

	NOMBRE	FECHA
Elaborado por:	Área de Registro	20/12/10
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	Fecha	Descripción	Autor
V 1.0	20 de diciembre de 2010	Procedimiento a seguir para la solicitud y descarga de certificados de Sede Electrónica y Sello Electrónico, emitidos por la FNMT - RCM bajo la denominación de <i>Certificados AP</i> .	Área de Registro
V 1.1	05 de enero de 2011	Se retira la necesidad de que las claves se generen en un Hardware criptográfico seguro.	Área de Registro
V 1.2	03 de junio de 2014	Acceso a la aplicación de registro mediante certificados de Clase 2 CA y certificados AP. Modificación de los requisitos de software y hardware	Área de Registro

Referencia:

Documento clasificado como: *Público / Distribución limitada*



Índice

1. Introducción.....	4
2. Pasos previos.....	4
3. Solicitud del certificado.....	4
3.1. Generación de las claves.....	4
3.2. Acceso a la aplicación para la solicitud del certificado correspondiente.....	4
3.2.1. Dirección Web donde se encuentra la aplicación.....	4
3.3. Autenticación del Registrador.....	5
3.4. Selección del tipo de certificado.....	7
3.5. Cumplimentación del formulario correspondiente.....	8
3.6. Firma de la solicitud.....	9
3.7. Impresión de contratos.....	12
3.8. Firma manual de los contratos.....	13
3.9. Envío de la solicitud a la FNMT - RCM.....	13
3.10. Envío de la documentación.....	14
4. Descarga del certificado.....	14
4.1. Comprobación del estado de su solicitud.....	14
Anexos.....	16
Anexo I. Requisitos de software y hardware.....	17
Anexo II. Errores detectados en la realización de registros.....	20
Anexo III. Datos de interés.....	21

1. INTRODUCCIÓN

El presente documento es un manual de ayuda para los usuarios que vayan a solicitar o descargarse un certificado de Sede Electrónica o Sello Electrónico emitidos por la FNMT-RCM bajo la denominación de Certificados Administración Pública (AP).

2. PASOS PREVIOS

Como paso previo, para poder realizar estas gestiones, el Registrador:

- Deberá estar dado de Alta en la infraestructura de CERES, con los perfiles y roles correspondientes.
- Estar en posesión de un certificado de persona física emitido por la FNMT - RCM, de los denominados como Certificados Clase 2 CA o de empleado público de los denominados como Certificados AP. Estos certificados, se recomiendan que estén soportados por una tarjeta criptográfica¹.
- El puesto de registro deberá cumplir con los requisitos mínimos de Sw y Hw establecidos².

Importante: Si el Registrador que vaya a hacer uso de la aplicación no cumple con los requisitos descritos anteriormente, deberá ponerse en contacto con la FNMT-RCM a través del Responsable de las Operaciones de Registro, con el fin de solucionar el problema existente.

3. SOLICITUD DEL CERTIFICADO

3.1. GENERACIÓN DE LAS CLAVES

En primer lugar se procederá a la obtención de las claves, mediante la generación de las mismas.

En este primer paso se generará el PKCS#10.

3.2. ACCESO A LA APLICACIÓN PARA LA SOLICITUD DEL CERTIFICADO CORRESPONDIENTE

3.2.1. Dirección Web donde se encuentra la aplicación

El acceso a dicha aplicación se realiza a través de la siguiente dirección:

¹ Esta tarjeta la proporciona la FNMT - RCM en el momento de dar de alta al Registrador en su infraestructura.

² Ver Anexo I de este documento.

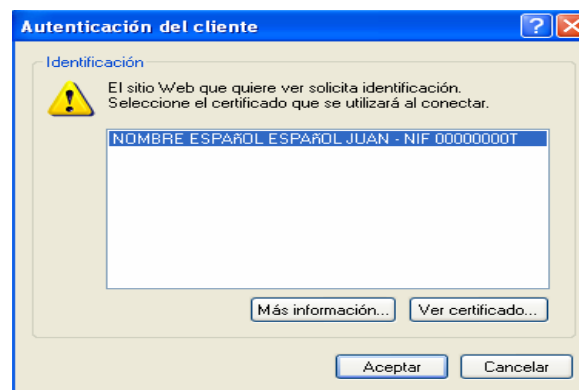
<https://apuc20.cert.fnmt.es/PreregistroComponentes/indexCRDinamicos.jsp>

Recuerde: Para poder acceder a ella es necesario estar en posesión de un certificado de persona física emitido por la FNMT – RCM, de los denominados como Certificados Clase 2 CA o de empleado público de los denominados como Certificados AP. Estos certificados, se recomiendan que estén soportados por una tarjeta criptográfica³

3.3. AUTENTICACIÓN DEL REGISTRADOR

Para entrar en la aplicación, el Registrador deberá identificarse, lo que hará mediante el certificado obtenido anteriormente, y a través de la pantalla *Autenticación del Cliente*.

En esta pantalla deberá seleccionar su certificado y pulsar **Aceptar**



Como último paso para acceder a la Aplicación de Registro, el sistema le solicitará que introduzca su número de identificación personal (PIN) y con el que protege el uso de su certificado frente a terceros.

Recuerde que para utilizar la aplicación deberá **tener en todo momento su tarjeta FNMT-CA introducida en el lector** y que a la hora de teclear su PIN debe **respetar las mayúsculas y minúsculas**.

³ Esta tarjeta la proporciona la FNMT – RCM en el momento de dar de alta al Registrador en su infraestructura.



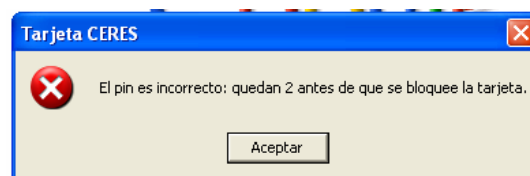
Una vez que haya introducido su PIN pulse el botón **Aceptar**.

Al introducir el PIN observará que no se refleja en pantalla, sino que en su lugar aparecen asteriscos. Esto no es un mal funcionamiento del programa, sino una medida de seguridad para que nadie pueda ver el código tecleado.

❖ Posibles errores en la introducción del PIN

Si el PIN tecleado por usted es **incorrecto** aparecerá un diálogo que le informará de dicho error.

- En caso de que el número de caracteres introducidos no coincida con el número de caracteres del PIN el mensaje de error le avisará de dicho evento
- Si el error es debido a que la cadena de caracteres introducida no es la correcta, se contabilizará además el número de intentos que se lleva para introducir el PIN. Recuerde que **si introduce erróneamente el PIN tres veces consecutivas la tarjeta se bloqueará**. No servirá para romper la serie de intentos el cerrar y arrancar de nuevo la aplicación así como el introducir o retirar la tarjeta del lector.



El chip de la tarjeta lleva un contador que solamente es accesible a través de la FNMT-RCM.

Para proceder al desbloqueo de su tarjeta seleccione en:

Inicio/Programas/FNMT-RCM/Utilidades/Desbloqueo de Tarjeta y Cambio de PIN. Desde esta aplicación podrá desbloquear su tarjeta introduciendo la Clave de Desbloqueo, que junto con el PIN, le fueron entregados con su tarjeta para obtener su certificado.

Una vez haya accedido a la aplicación aparecerá un ventana que mostrará el tipo de certificados que esté autorizado a solicitar.



SOLICITUDES EN CURSO

[Consulte el estado de su solicitud](#)

OBTENGA SU CERTIFICADO DE COMPONENTE

Seleccione un tipo de certificado de los siguientes:

Certificado de la AP de tipo Sello Electrónico
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.

Certificado de la AP de tipo Sede 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.

[Solicitar Certificado](#)

3.4. SELECCIÓN DEL TIPO DE CERTIFICADO

A continuación deberá determinar el tipo de certificado que va a solicitar.

- **Certificado de la AP de tipo Sede Electrónica identificado por el nombre del dominio.** Para la identificación de Sedes Electrónicas. 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.

Certificado de la AP del tipo Sello Electrónico. Utilizados para la automatización de procesos administrativos. 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.

Seleccione el tipo de certificado que desea solicitar y pulse **Solicitar Certificado**

SELLO ELECTRÓNICO



Real Casa de la Moneda
FÁBRICA NACIONAL DE MONEDA Y TIMBRE


SOLUCIONES EN CURSO
Consulte el estado de su solicitud

DETERMINA SU CERTIFICADO DE COMPONENTE
Seleccione un tipo de certificado de los siguientes:

- Certificado de la AP de tipo Sello Electrónico
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.
- Certificado de la AP de tipo Sede 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.

Solicitar Certificado

SEDE ELECTRÓNICA



Autoridad Pública de Certificación Española

SOLUCIONES EN CURSO
Consulte el estado de su solicitud

DETERMINA SU CERTIFICADO DE COMPONENTE
Seleccione un tipo de certificación en los siguientes:

- Certificado de la AP de tipo Sello Electrónico
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.
- Certificado de la AP de tipo Sede 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.

Solicitar Certificado

3.5. CUMPLIMENTACIÓN DEL FORMULARIO CORRESPONDIENTE

Recuerde: Antes de iniciar la cumplimentación del formulario, es conveniente que tenga a mano todos los datos a cumplimentar en el formulario como son los datos de la entidad, el nombre del certificado, los datos del responsable del mismo, el PKCS#10, etc.

Importante: No introduzca caracteres extraños, solo caracteres alfanuméricos.

Los campos con asterisco (*) son obligatorios.

SELLO ELECTRÓNICO



Autoridad Pública de Certificación Española

GENERACIÓN CERTIFICADO SELLO ELECTRÓNICO PARA LA APE

SUJETO
DATOS DEL COMPONENTE CRIPTOGRÁFICO (NOMBRE)
NOMBRE COMPONENTE*:

PROPIETARIO DEL CERTIFICADO
DATOS IDENTIFICACIÓN PERSONA JURÍDICA
CIF ENTIDAD SUSCRIPTORA*:
RAZÓN SOCIAL*:

DATOS DOMICILIARIOS
PAIS*:
DIRECCIÓN*:
CÓDIGO POSTAL*:
LOCALIDAD*:

SEDE ELECTRÓNICA



Autoridad Pública de Certificación Española

GENERACIÓN DE UN CERTIFICADO SEDE WEB PARA LA APE, IDENTIFICADO POR DNS

SUJETO
DATOS IDENTIFICATIVOS DE LA SEDE ELECTRÓNICA
DOMINIO*:
DESCRIPCIÓN*:
EMAIL:

PROPIETARIO DEL CERTIFICADO
DATOS IDENTIFICACIÓN PERSONA JURÍDICA
CIF ENTIDAD SUSCRIPTORA*:
RAZÓN SOCIAL*:
DATOS DOMICILIARIOS

Cuando rellene el formulario, compruebe que los datos introducidos son correctos y pulse el botón “**Aceptar**”. La selección de esta opción nos enviará a la ventana de **confirmación de datos**.

En esta pantalla:

- ✓ **Si se observase algún error:** Pulse el botón **Corregir datos**. De esta forma volveremos al formulario nuevamente y podremos corregir los datos incorrectos.
- ✓ **Si los datos fueran correctos:** Pulse el botón **Aceptar**. Esta opción validará los datos e iniciará el proceso de firma.

3.6. FIRMA DE LA SOLICITUD

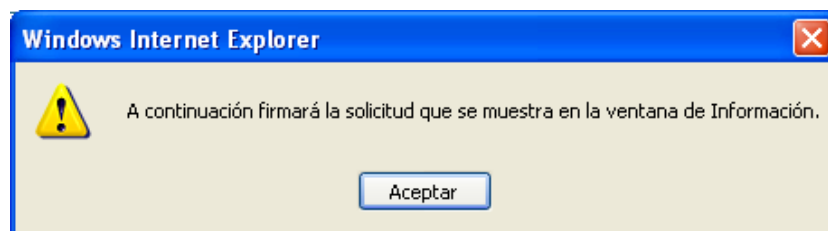
A continuación el Registrador deberá firmar electrónicamente la solicitud.

Recuerde: Para realizar la firma de los datos es necesario disponer de un certificado de Persona Física emitido por la FNMT – RCM bajo la denominación de Certificado Clase 2 CA.

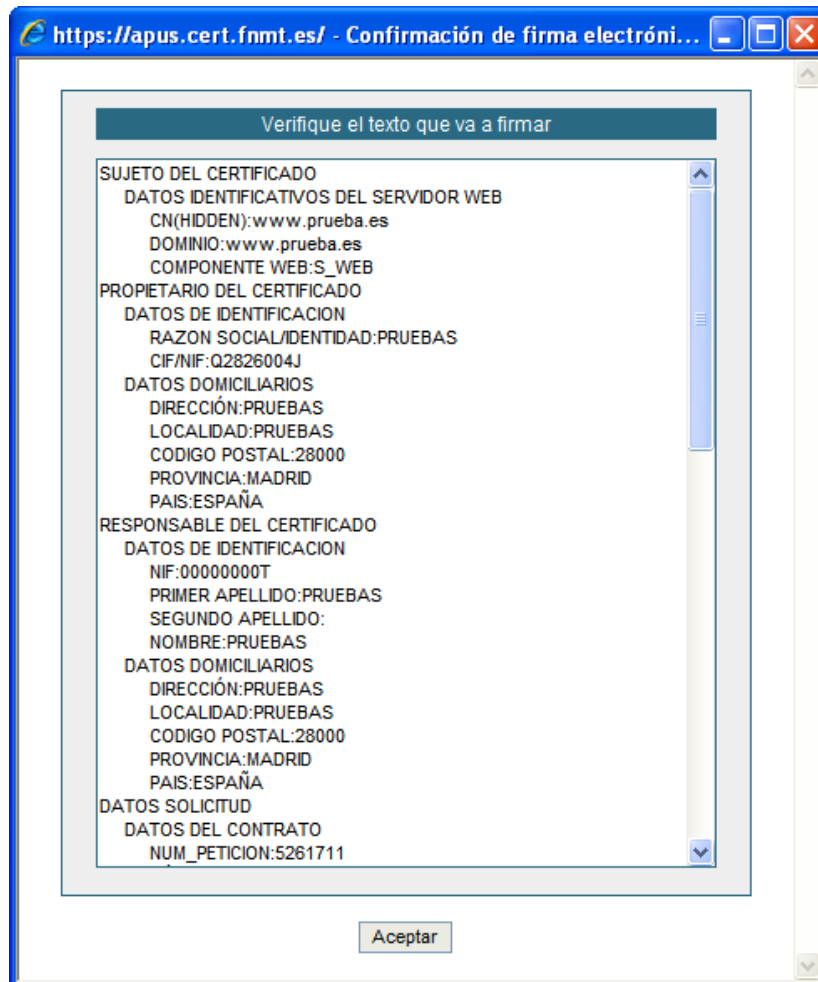
Recuerde: Previo al proceso de solicitud del certificado debe de haber instalado la librería CAPICOM. Si necesita más información sobre la instalación de CAPICOM puede consultarla en el **Anexo I** de este documento.

La secuencia de pantallas que nos guiarán por el proceso de firma es la que se describe a continuación:

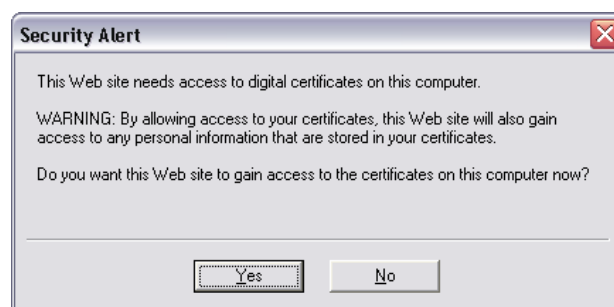
La primera de las pantallas del proceso de firma nos indica que va a comenzar el mismo,



Pulse **Aceptar**. Nos aparecerá una ventana con la información que vamos a firmar.

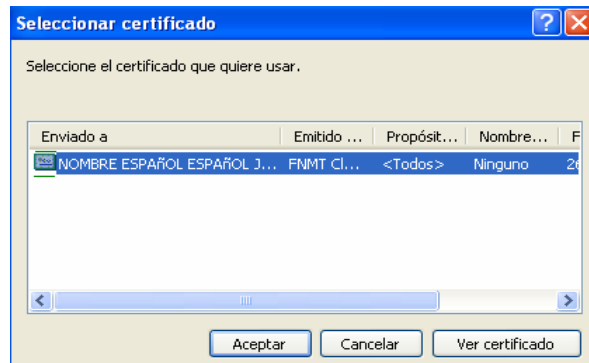


Pulse **Aceptar**. Aparecerá la siguiente pantalla:



Nota: Este es un aviso independiente a la aplicación y proporcionado por Microsoft, que nos pregunta si confiamos en el certificado que está instalado en nuestro navegador y con el que hemos entrado en la aplicación. Pulsaremos el Botón **Yes**.

Aparecerá una nueva pantalla que le mostrará los certificados que existan en la tarjeta criptográfica.



Seleccione el correspondiente al Registrador:

Nota: Se muestra otra alerta parecida a la anteriormente mencionada para de nuevo aceptar la confianza del certificado que estamos utilizando para registrar.



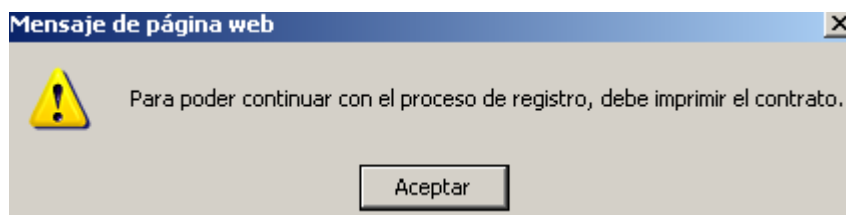
Pulsaremos el botón **Yes**. Si el proceso de firma ha finalizado correctamente, la siguiente pantalla que nos aparecerá será la de impresión de contratos.

3.7. IMPRESIÓN DE CONTRATOS

Recordar: El contrato ha de imprimirse el anverso y el reverso en una sola hoja. Para ello existe la opción de impresión a doble cara. Si la impresora que se vaya a utilizar para esta impresión lo permite solicite esta opción al Área de Registro del Departamento CERES de la FNMT – RCM. En el caso de que su impresora no permitiera esta opción, deberá imprimir previamente los reversos de los contratos y colocarlos en su impresora de manera que en el anverso de los mismos puedan imprimirse los datos del solicitante del registro.

Seleccione la opción **Imprimir**. Se imprimirán las dos copias del contrato que deberán ser firmadas por el Solicitante y Registrador.

Nota: Si intentan aceptar antes de imprimir la aplicación les devolverá un cuadro de diálogo como este,



Importante. Revise la información que aparece en los contratos antes de pasar a la siguiente opción.

Además, en la pantalla del contrato aparecen las siguientes opciones: **Imprimir**, **Aceptar**, **Corregir Datos** y **Cancelar**

- Opción **Imprimir**: Si ha de imprimir nuevamente las copias del contrato, seleccione esta opción.
- Opción **Aceptar**: Una vez impreso el contrato y firmado por el Solicitante y Registrador. **Importante:** No pulse el botón Aceptar hasta que el contrato se haya impreso, comprobado que los datos son los correctos y firmado por el solicitante y el registrador, pues una vez seleccionada esta opción no podrá volver a imprimir el contrato y deberá volver a realizar la solicitud del certificado desde el principio, incluyendo la realización de una nueva solicitud.

- Opción **Corregir datos**: Cuando los datos que aparecen en el contrato no son correctos. Su selección le lleva a la pantalla anterior de introducción de datos lo que le permitirá corregir los campos con datos erróneos.
- Opción **Cancelar**: Cancela el registro y le lleva al menú Principal.

3.8. FIRMA MANUAL DE LOS CONTRATOS

Si los datos que aparecen en el contrato son correctos, se procede a la firma manuscrita por parte del Solicitante y el Registrador, de las dos copias. Una de ellas será entregada al Solicitante, mientras que la otra deberá ser guardada por la Oficina de Registro según lo establecido en el procedimiento de registro correspondiente.

3.9. ENVÍO DE LA SOLICITUD A LA FNMT - RCM

Firmado el contrato por ambas partes, el Solicitante y el Registrador, se deberá proceder al envío de la solicitud a la FNMT - RCM. Para esto seleccionaremos la opción de **Aceptar** que aparece en la pantalla.

Si el proceso se completa con éxito, se nos mostrará una pantalla donde se indica que la solicitud de registro para el acceso a los servicios de certificación ha sido efectuada correctamente. Igualmente y en la misma pantalla la aplicación nos devolverá el **código de solicitud** del certificado.

Nota: Cuando se selecciona la opción de **Aceptar**, el Registrador estará firmando electrónicamente la solicitud de Registro y no habrá posibilidad de modificar ningún dato, ya que el registro será efectivo.

Recuerde guardar este número pues le será necesario para la descarga del certificado.



Autoridad Pública de Certificación Española

El código de solicitud generado es:

501819394

IMPORTANTE: Guarde este código, pues lo necesitará tanto para acabar de cumplimentar la solicitud en la oficina de registro, como para la descarga de su certificado una vez se haya generado. Además, podrá hacer un seguimiento de su solicitud con dicho código.

[Volver](#)

3.10. ENVÍO DE LA DOCUMENTACIÓN

Para que el proceso de generación del certificado siga adelante debe enviar la documentación requerida, y descrita en los Procedimientos de Registro correspondientes.

Esta documentación es necesaria para que la solicitud recibida sea aprobada por la FNMT - RCM y el certificado pueda ser creado.

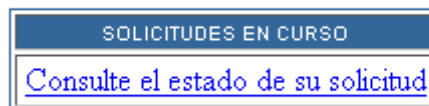
4. DESCARGA DEL CERTIFICADO

Una vez procesada en la infraestructura de la FNMT - RCM la solicitud recibida, el certificado estará disponible para su descarga, la cual se realizará desde la propia Oficina de Registro y a través de la página Web que la FNMT - RCM tiene al efecto, cuya dirección es:

<https://apuc20.cert.fnmt.es/PreregistroComponentes/indexCRDinamicos.jsp>

4.1. COMPROBACIÓN DEL ESTADO DE SU SOLICITUD

En esta pantalla, seleccione el tipo de certificado que quiere buscar y posteriormente la opción **Solicitudes en curso**.



Introduzca el **nombre del componente / dominio** para el que ha solicitado el certificado y el **código de solicitud** y pulse **Enviar**.

SELLO ELECTRÓNICO

SEDE ELECTRÓNICA

Introduzca los siguientes datos correspondientes a su solicitud		Introduzca los siguientes datos correspondientes a su solicitud	
NOMBRE COMPONENTE:	<input type="text"/>	DOMINIO:	<input type="text"/>
Código Solicitud:	<input type="text"/>	Código Solicitud:	<input type="text"/>
<input type="button" value="Enviar"/>		<input type="button" value="Enviar"/>	

Le aparecerá una lista de los certificados existentes. Si su certificado se ha generado podrá proceder a su descarga.

DATOS DE LA SOLICITUD			
Codigo Solicitud: 501819394			
Número de Petición: 5052			
EVENTOS ASOCIADOS A SU SOLICITUD			
CA	TIPO DE CERTIFICADO	OPERACION REALIZADA	FECHA DE OPERACIÓN
AP CA	CD	Solicitud de preregistro recibida e insertada, pendiente de procesar	17-12-2010 07:11:57


Pulse en Descargar certificado.

En la página de descarga del certificado pulse en Instalar Certificado para descargar el fichero que deberá asociar a la clave privada.

CERTIFICADOS:

Para cada certificado obtenido puede instalarlo, acceder a la DPC (Declaración de política de certificación) y la ruta de certificación asociadas.

Certificado 1

 [Información DPCs](#)

Recuerde que debe instalar el certificado en la misma máquina desde la que generó las claves, lo que aquí descarga es sólo la parte pública del certificado, que debe asociarse a la clave privada para ser completamente funcional.

ANEXOS

ANEXO I. REQUISITOS DE SOFTWARE Y HARDWARE

INTRODUCCIÓN.

El objetivo de este Anexo es describir los requisitos mínimos, tanto software como hardware, para poder utilizar la aplicación de registro Web a través de SSL con certificados AC FNMT Usuarios.

NECESIDADES HARDWARE.

- a) Será necesario una maquina (PC) con las siguientes características mínimas:
- Lector de Tarjetas criptográficas.
 - Conexión a Internet con los requisitos indicados posteriormente.
 - Conexión directa o mediante red local a impresora correctamente configurada.

2. NECESIDADES HARDWARE.

- a) *Drivers* del lector de tarjetas correspondiente al dispositivo instalado.
- b) Sistema Operativo Windows Vista, Windows 7 o Windows 8 (Es recomendable que el sistema operativo esté totalmente actualizado)
- c) Navegadores
1. Disponer de Internet Explorer 8, 9, 10 o 11* con todas las actualizaciones instaladas y tener habilitadas las cookies.
 2. Mozilla Firefox 3.5 o superior.
- d) Adobe Reader 8.X o superior con plug-in instalado en el navegador.
- e) Instalación del Software correspondiente según el certificado lo tenga en el propio navegador o en una tarjeta criptográfica:
- Cuando el certificado esté en el navegador (Software). Deberá tener instalado el configurador de la FNMT-RCM. Puede descargarlo desde: https://www.sede.fnmt.gob.es/documents/11614/70993/Configurador_FNMT_RCM.exe
 - Cuando el certificado lo tenga en una tarjeta criptográfica. Deberá tener instalado el módulo criptográfico de la FNMT-RCM. Puede descargarlo desde: <https://www.sede.fnmt.gob.es/descargas/descarga-software>, en la sección Software de usuario en tarjeta criptográfica. Elija la versión de 32 o 64 bits en función de su sistema operativo.

NOTA: Para que la aplicación de registro funcione con IE 11, hay que meter la URL de la aplicación de registro en los sitios de la intranet y luego activar la vista de compatibilidad para los sitios de la intranet. Para esto siga los siguientes pasos:

- 1 - Debe abrir Internet Explorer, Herramientas > opciones de internet > Seguridad > Intranet local > Sitios > Opciones avanzadas, escribir <https://registro.cert.fnmt.es> o <https://registro20.cert.fnmt.es> (según corresponda) y pulsar en Agregar. Pasará a la barra de abajo. Acepte todas las ventanas.
- 2 - Luego pulse en Herramientas > Configuración de la vista de Compatibilidad, compruebe que la casilla Mostrar sitios de la intranet en Vista de compatibilidad. Acepte todas las ventanas y reinicie el navegador.

Configuración de Internet Explorer:

Antes de comenzar recomendamos tener el Sistema Operativo lo más actualizado posible con las actualizaciones y parches de seguridad de Windows.

Configuración automática para Internet Explorer, Mozilla Firefox y Google Chrome:

Para evitar problemas a la hora de solicitar un certificado es conveniente que instale nuestro configurador automático ([Configurador FNMT-RCM](#)). Descargue el software, cierre todas las ventanas del navegador, ejecútelo como administrador del equipo y reinicie su PC. En el proceso de instalación se realizan las siguientes tareas:

- Instala todos los certificados de las CAs (Autoridades de Certificación) raíces e intermedias.
- Instala la librería Capicom.
- Realiza modificaciones en el registro de Windows para configurar las opciones de seguridad de su navegador.

Configuración manual para Internet Explorer:

En primer lugar debe descargar e instalar con permisos de administrador la [librería CAPICOM](#).

Debe seguir también los siguientes pasos:

- En el navegador Internet Explorer, vaya a Herramientas/Opciones de Internet/Seguridad.
- Pulsar en "Sitios de Confianza" y a continuación pulsar en "Sitios".
- Abajo, desmarcar la opción de "Requerir comprobación del servidor (https://)" para todos los sitios de la zona"
- En el cuadro de texto "Agregar este sitio Web a la zona": tendremos que agregar las siguientes URLs https://*.fnmt.es , https://*.fnmt.gob.es , http://*.fnmt.es y http://*.fnmt.gob.es
- Cerrar la ventana.

En "Nivel de seguridad para esta zona" pulse el botón Nivel personalizado. Busque el apartado "Controles y complementos de ActiveX" y Habilite todas las opciones.

Pulsar en Aceptar, le aparecerá un mensaje para confirmar que deberá aceptar.

Aplicar y aceptar la última ventana.

Cerrar el navegador para que se apliquen los cambios.

En windows Vista, desactive el Control de Cuentas de Usuario en Inicio, Panel de control, Cuentas de usuario, activar o desactivar el control de cuentas de usuario. Desactivar la casilla de verificación y reiniciar el equipo.

Configuración manual para Mozilla Firefox (No soportadas las versiones de la 33.0 a la 34.0). La versión 35 y posteriores requieren de la instalación de un [complemento para firmar](#)

[Instalación de los certificados raíces](#)

ANEXO II. ERRORES DETECTADOS EN LA REALIZACIÓN DE REGISTROS

- ❖ **Ha ocurrido un error al firmar el contenido:** El servidor de automatización no puede crear el objeto (también en inglés), o bien, la librería criptográfica no está instalada.



- Hay que instalar la librería CAPICOM. [Instalador CAPICOM](#)

Si no se soluciona el error escriba un correo a: soporte_tecnico_ceres@fnmt.es.

- ❖ **No tiene permisos de registrador**

Notificarlo al responsable asignado en la oficina a la que pertenece y este será el que debe ponerse en contacto con registroceres@fnmt.es para comprobar los permisos del registrador, en caso de que no estén dados de alta, el responsable procederá a su solicitud siguiendo el procedimiento de alta de registradores.

- ❖ **No dispone de certificados válidos**



Este error aparece cuando no tiene instalado su certificado personal para poder firmar la petición. Debe instalarlo en el navegador o tenerlo en tarjeta criptográfica para firmar la solicitud.

Si no dispone de un certificado de usuario puede solicitarlo gratuitamente desde la siguiente dirección: <https://www.sede.fnmt.gob.es/certificados/persona-fisica>

ANEXO III. DATOS DE INTERÉS

Si durante el proceso de solicitud encuentra dificultades técnicas, puede ponerse en contacto con el Área de Soporte Técnico de CERES, a través de:

- ♦ Correo electrónico: soporte_tecnico_ceres@fnmt.es
- ♦ Teléfonos: 915 666 914 / 915 666 908 / 915 667 824.

Para cualquier duda sobre el proceso de solicitud y documentación a aportar, puede ponerse en contacto con el Área de Registro, a través de:

- ♦ Correo electrónico: registroceres@fnmt.es
- ♦ Teléfonos: 915 666 916 / 915 666 697 / 915 667 917 / 915 666 919.