



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES
ÁREA DE REGISTRO

CERTIFICADOS DE COMPONENTES SOFTWARE Y SERVIDORES WEB EMITIDOS POR LA
FNMT - RCM BAJO LA DENOMINACIÓN DE
CERTIFICADOS AC DE COMPONENTES INFORMÁTICOS
CERTIFICADOS DE COMPONENTES

[PROCEDIMIENTOS DE REGISTRO]

Versión 2.1

	NOMBRE	FECHA
Elaborado por:	Área de Registro	28 de enero de 2013
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	Fecha	Descripción	Autor
1.0	11 de marzo de 2014	Creación del documento.	Área de Registro
V 1.1	12 de julio de 2014	<p>Incorporación como suscriptor a Organismos Públicos sin Encomienda de Gestión o Convenio firmado.</p> <p>Modificación del primer apartado del punto 3. <i>Entidades involucradas.</i></p> <p>Modificación del punto 5.1. <i>Consideraciones previas</i> en el apartado donde se habla de las personas que podrán ejercer como representantes.</p> <p>En los Anexos I y II, los puntos 6.1 y 7.1, se modifica su título para adaptarlo a la incorporación de Organismos Públicos sin Encomienda de Gestión o Convenio.</p> <p>Modificación de algunos textos para corregir su edición.</p> <p>Documentación necesaria para la cesión de dominios (dominios cuya titularidad no</p>	Área de Registro



		pertenece al solicitante del certificado).	
V1.2	24 de noviembre de 2014	Aceptación para la firma de los contratos de peticiones de todos aquellos certificados admitidos por el Ministerio de Industria, Turismo y Comercio.	Área de Registro
V 1.3	8 de mayo de 2015	Cambiar la dirección de correo electrónico donde enviar la documentación.	Área de Registro
v 1.4	20 de noviembre de 2015	En la emisión de certificados de servidor, no podrán ser admitidos aquellos dominios que no estén registrados en la <i>Internet Assigned Numbers Authority (IANA)</i> .	Área de Registro
V 2.0	28 de enero de 2016	Se incorpora más en detalle el proceso de revocación telefónica	Área de Registro
V 2.1	6 de junio de 2016	Corrección de la dirección web para acceder a la aplicación de solicitudes del certificado. Eliminar la opción de obtener este tipo de certificados para persona físicas. Eliminar los certificados SSL Plus.	Área de Registro

Referencia:

Documento clasificado como: *Público / Distribución limitada*



Procedimientos de registro

Certificados AC de Componentes Informáticos

(*Certificados de componente*)

Versión 2.1

Página 3 de 22

Índice

1. Introducción	6
2. Acrónimos y definiciones	6
2.1. Acrónimos.....	6
2.2. Definiciones	7
3. Entidades involucradas	8
4. Clases de Certificados de <i>Componente</i>	9
4.1. Certificados de Servidor	9
4.1.1. <i>Certificados SSL estándar [Certificado de Servidor Web identificado por el nombre del dominio (DNS)]</i>	9
4.1.2. <i>Certificados SSL Wildcard</i>	9
4.1.3. <i>Certificados SSL multidominio (SAN/UCC)</i>	9
4.2. Otros certificados de <i>componente</i>	9
4.2.1. <i>Certificado de sello de entidad</i>	9
4.2.2. <i>Certificado de componente de firma de código</i>	10
5. Gestión de solicitudes de registro	10
5.1. Consideraciones previas	10
5.2. Procedimiento de Registro	12
5.2.1. Expedición de certificados.....	12
5.2.2. Revocación de certificados	16
6. Anexo I. Documentación necesaria para la aceptación de una solicitud para la expedición de un certificado.....	20
6.1. Organismo Público	20
6.1.1. Documentación que hay que enviar	20
6.1.2. La FNMT - RCM, comprobará	20
6.2. Persona Jurídica	20
6.2.1. Documentación que hay que enviar	20



Procedimientos de registro

Certificados AC de Componentes Informáticos

(*Certificados de componente*)

Versión 2.1

Página 4 de 22

6.2.2.	La FNMT – RCM, comprobará	21
1.	Anexo II. Documentación necesaria para la aceptación de una petición para la revocación de un certificado a través de la oficina de registro de CERES.....	22
1.1.	Organismo Público CON Encomienda de Gestión o Convenio firmado	22
1.1.1.	Documentación que hay que enviar	22
1.1.2.	La FNMT – RCM, comprobará	22
1.2.	Persona Jurídica	22
1.2.1.	Documentación que hay que enviar	22
1.2.2.	La FNMT – RCM, comprobará	22



1. INTRODUCCIÓN

La gestión de certificados supone la realización de una serie de tareas en función de los requerimientos de los usuarios. Tareas que se han de llevar a efecto por parte de los *solicitantes* o titulares del propio certificado, en algunos casos por el Área de Registro u otras Áreas de la FNMT - RCM y la propia FNMT - RCM a través de su Departamento CERES.

Este documento contempla los procedimientos a seguir por las partes involucradas en la gestión de este tipo de certificados y a las que se hace referencia en el párrafo anterior.

Todos los procedimientos aquí expuestos, están soportados por la Declaración de Prácticas de Certificación para estos certificados actualmente en vigor.

En esta versión sólo se contemplan procedimientos para el caso de que el *suscriptor* sea un organismo público con encomienda de gestión o convenio firmado o una persona jurídica.

2. ACRÓNIMOS Y DEFINICIONES

2.1. ACRÓNIMOS

AAPP	Administraciones Públicas
DGPC	Declaración General de Prácticas de Certificación
DI	Datos de Identidad
DPC	Declaración de prácticas de certificación
FNMT - RCM	Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda
LCR	Lista de certificados revocados
PSC	Prestador de Servicios de Certificación
ROR	Responsable de operaciones de registro
CSR	Petición del certificado.

[Certificate Signing
Request]



Procedimientos de registro

Certificados AC de Componentes Informáticos

(Certificados de componente)

Versión 2.1

Página 6 de 22

2.2. DEFINICIONES

Aplicación de registro	Aplicación Web mediante la cual se gestionan las solicitudes de expedición y revocación de un certificado.
Aplicación de solicitud y descarga	Aplicación Web mediante la cual se solicita la expedición de un certificado y posterior descarga del certificado.
Certificado de componente	Certificado empleado por un componente informático en una infraestructura de clave pública.
Componente (informático)	Conjunto de elementos interrelacionados entre sí para transmitir o tratar información y con capacidad de firmarla o cifrarla de manera autónoma ¹ .
CSR	Estructura de datos que garantizan la posesión de las claves por parte del <i>solicitante</i> del certificado. En esta información va incluida la clave pública cifrada con la clave privada. Según el tipo de navegador esta estructura se conformará como un PKCS #10 (Internet Explorer) o Spkac (Mozilla).
Expedición de certificados	Procedimiento por el cual la <i>FNMT-RCM</i> crea un certificado, previa petición del <i>solicitante</i> y solicitud recibida, y a nombre del <i>suscriptor</i> de dicho certificado.
Petición o solicitud de PKCS#10	Conjunto de datos en formato electrónico y de acuerdo con el estándar PKCS#10 que es creado como paso previo a la solicitud de un certificado.
PKCS#10	Estándar de los laboratorios RSA para la remisión de claves públicas al objeto de la composición o creación de un certificado.
Registro de usuarios	Procedimiento por el que mediante una aplicación Web, se toman los datos personales de un <i>solicitante</i> , se confirma su identidad y se formaliza su contrato con la <i>FNMT-RCM</i> para la expedición o revocación de un certificado.

¹ DPC para este tipo de certificados.



Representante	Administrador, cargo público o apoderado general del <i>Suscriptor</i> cuando este es una persona jurídica, órgano u organismo público y que actúa en nombre del <i>Suscriptor</i> . Es también la persona física a la que se reconoce la capacidad de autorizar al <i>Solicitante</i> .
Revocación de certificados	Procedimiento por el cual la FNMT-RCM deja sin efecto la validez del certificado, previa solicitud del titular del certificado, bien de forma directa o mediante persona autorizada.
Solicitante	Persona física, mayor de edad, que realiza la solicitud del <i>certificado</i> y, en el caso de expediciones, entrega la clave pública a la FNMT - RCM y recibe de ésta el <i>certificado</i> .
Soporte del certificado	Lugar o dispositivo donde se guarda el certificado, y desde donde se ejecuta la firma electrónica.
Sujeto del certificado	Campo <i>Subjet</i> del certificado que identifica al <i>suscriptor</i> y al <i>componente</i> ² .
Suscriptor	Persona jurídica, órgano u organismo público destinatario de las actividades de la FNMT-RCM como <i>Prestador de Servicios de Certificación</i> , que suscribe los términos y condiciones del servicio y se referencia en el <i>sujeto</i> en el <i>certificado</i> . Es el titular y responsable del uso del <i>certificado</i> que posee el control exclusivo y la capacidad de decisión sobre el <i>componente</i> .

3. ENTIDADES INVOLUCRADAS

Las partes que están involucradas en este proceso son las siguientes:

- Las personas jurídicas, así como Organismos Públicos, *suscriptores* y *solicitantes* de los certificados.
- La FNMT-RCM que actúa como Prestador de Servicios de Certificación, y Oficina de Registro.

² DPC para este tipo de certificados.



Procedimientos de registro

Certificados AC de Componentes Informáticos

(*Certificados de componente*)

Versión 2.1

Página 8 de 22

4. CLASES DE CERTIFICADOS DE COMPONENTE

4.1. Certificados DE SERVIDOR

Certificados asociados a uno o más dominios web.

4.1.1. *Certificados SSL estándar [Certificado de Servidor Web identificado por el nombre del dominio (DNS)]*

Permite establecer comunicaciones seguras utilizando el protocolo SSL/TLS. Este tipo de certificado garantiza la identidad del dominio donde se encuentra la web.

4.1.2. *Certificados SSL Wildcard*

Permite a las organizaciones dar seguridad a un conjunto ilimitado de subdominios, a partir del tercer nivel, asociados a un dominio determinado, con un único Certificado SSL.

4.1.3. *Certificados SSL multidominio (SAN/UCC)*

Permite a las organizaciones proteger varios nombres de dominio independiente entre sí, con un único certificado, sin necesidad de adquirir y gestionar múltiples certificados electrónicos.

Se permite elegir el uso extendido de la clave:

- *Certificados para la autenticación de un servidor (Por defecto).*
- *Certificados para la autenticación mutua de un cliente – servidor (Autenticación de cliente).*
- *Certificados para la autenticación de un servidor de correo (Protección de correo electrónico).*

4.2. OTROS CERTIFICADOS DE COMPONENTE

Sistema con capacidad de realizar operaciones criptográficas para la autenticación y/o firma digital.

4.2.1. *Certificado de sello de entidad*

Sirve para para la automatización de proceso de firma y autenticación entre *componentes* informáticos.

Se permite elegir el uso extendido de la clave:

- *Certificados la para autenticación mutua de un cliente – servidor (Autenticación de cliente).*



Procedimientos de registro

Certificados AC de Componentes Informáticos

(*Certificados de componente*)

Versión 2.1

Página 9 de 22

- *Certificados para la autenticación de un servidor de correo (Protección de correo electrónico).*
- *Certificados para autenticación diversa (Cualquier uso extendido de la clave).*

4.2.2. *Certificado de componente de firma de código*

Permite firmar software y garantizar la identidad del propietario y la integridad del código.

5. GESTIÓN DE SOLICITUDES DE REGISTRO

5.1. CONSIDERACIONES PREVIAS

- La solicitud de estos certificados solamente podrá ser realizada por personas físicas mayores de edad o los menores que ostenten la facultad de emancipados³.
- Las solicitudes, tanto de expedición como de *revocación* de un *certificado*, serán solicitadas por el *suscriptor* del certificado o su *representante* en el caso de que éste sea una persona jurídica, independientemente de que la petición sea gestionada por otra persona (*solicitante*).
- Las revocaciones de certificados se realizarán en la oficina de registro de la FNMT – RCM o de forma telefónica, no contemplándose la revocación online.
- La suspensión de un certificado o la cancelación de la suspensión del mismo se realizarán a través de la oficina de registro de la FNMT – RCM.
- No existe la renovación de certificados. Cuando el certificado haya caducado, se deberá solicitar uno nuevo.
- No se contempla la autorevocación de certificados, por lo que se podrán tener activos dos o más certificados del mismo tipo, y para un mismo *suscriptor*.
- Las solicitudes de expedición recibidas en la FNMT – RCM tendrán un plazo de validez de tres (3) meses, transcurridos los cuales, si no han sido gestionadas, serán borradas, teniendo que realizar una nueva solicitud en el caso de que se quiera continuar con dicha petición.
- En todos los tipos de certificados se podrá establecer el tiempo de validez del certificado, pudiendo ser este periodo de uno (1), dos (2) o tres (3) años.
- En los certificados de servidor, no serán admitidos aquellos dominios que no estén registrados en la *Internet Assigned Numbers Authority (IANA)*⁴.

³ Según lo dictado por la normativa al efecto, vigente en el momento de la solicitud del certificado.

⁴ Según recomendación de CA/Browser Forum.



- En los certificados de sello de entidad y SSL multidominio (SAN/UCC), se podrá elegir el uso extendido de la clave, entre las posibilidades establecidas.
- Cuando el solicitante del certificado no sea el titular del dominio, deberá adjuntar un documento de cesión del mismo, formalizado y firmado por un representante del organismo o empresa que ostenta esta titularidad.
- En el caso de certificados SSL Wildcard
 - La FNMT - RCM exigirá al *suscriptor* la acreditación de que todos los subdominios amparados por el dominio que aparece en el certificado son de su propiedad.
 - En el caso de que el certificado fuese utilizado para un subdominio que no cumpliera la condición anterior, la FNMT - RCM se exime de toda responsabilidad respecto del uso que del certificado se haga. Además, y en el caso de que la FNMT - RCM tenga conocimiento de este uso indebido, se procederá a la *revocación* del mismo.
 - Se limitará la posición del comodín (*) dentro del dominio. La posición se deberá situar al menos en el tercer nivel de dominio.
- En el caso de certificados SSL multidominio (SAN/UCC),
 - La FNMT - RCM exigirá al *suscriptor* la acreditación de que todos los dominios integrados en el certificado son de su propiedad.
 - La solicitud para este tipo de certificados contendrá un mínimo de 2 dominios y un máximo de 12.
- Podrán ejercer como *representantes*:
 - De un Organismo Público
 - Si el contrato se firma con un certificado de empleado público, la persona que aparezca como representante del organismo en dicho certificado.
 - Si el contrato se firma con un certificado de persona jurídica, la persona que aparezca como representante del organismo en dicho certificado.
 - En el caso de que el organismo tuviera una Encomienda de Gestión o Convenio firmado con la FNMT - RCM, el responsable de operaciones de registro (ROR) del *suscriptor*⁵

⁵ Puede ser de cualquiera de las CAs existentes en el momento de la firma (Clase 2 CA, AP, Usuarios,...)



- En solicitudes de certificado de servidor, la persona que aparezca como persona de contacto administrativo o técnico del dominio o dominios solicitados.
- Que sea una persona que conste en la FNMT - RCM con capacidad de representación del *suscriptor*.
- En el caso de que sea una sociedad mercantil de titularidad pública, la persona que aparezca como tal en el Registro Mercantil.
- De una persona jurídica
 - Si el contrato se firma con un certificado de persona jurídica, la persona que aparezca como representante en dicho certificado.
 - En solicitudes de certificado de servidor, la persona que aparezca como persona de contacto administrativo o técnico del dominio o dominios solicitados
 - Que sea una persona que conste en la FNMT - RCM con capacidad de representación del *suscriptor*.
 - La que aparezca como tal en el Registro Mercantil.

5.2. PROCEDIMIENTO DE REGISTRO

5.2.1. Expedición de certificados

5.2.1.1. Consideraciones previas

El procedimiento contemplado abarca todos los procesos, funciones y operaciones que se han de realizar desde el inicio de la solicitud de expedición del certificado hasta que éste es recibido por el *suscriptor* del mismo.

En este procedimiento de solicitud, se toman los datos identificativos del *suscriptor*, de su *representante*, en el caso de que el *suscriptor* fuera una persona jurídica y del *solicitante* del certificado. Además se confirma la propiedad del dominio en su caso y la capacidad del *solicitante* para realizar la solicitud en nombre del *suscriptor* para el cual se emite el *certificado de componente* y se formaliza su contrato con la FNMT-RCM. Posteriormente se procederá a la expedición del *certificado de componente* solicitado, una vez realizadas las validaciones pertinentes.

La validación de las solicitudes será realizada por el Área de Registro del Departamento de CERES de la FNMT-RCM.



Procedimientos de registro

Certificados AC de Componentes Informáticos

(*Certificados de componente*)

Versión 2.1

Página 12 de 22

5.2.1.2. Presolicitud

Esta operación deberá realizarla el *suscriptor*. Deberá realizar:

1. Generación de las claves⁶. Esta operación deberá realizarse en una máquina del *suscriptor* y utilizando las herramientas de que disponga⁷.
2. Creación de la *petición del certificado (CSR)*⁸

5.2.1.3. Solicitud

Cumplimentación del formulario correspondiente, envío de la solicitud a la FNMT-RCM y recepción del Código de Solicitud

Se realizará por parte del *solicitante* y a través de la página web que la FNMT - RCM ha puesto a disposición de los *solicitantes*⁹: <https://apus20.cert.fnmt.es/PreregistroComponentes/>

En ella realizará los siguientes pasos:

1. Seleccionar el *suscriptor* (persona jurídica u organismo público).
2. Elección del certificado que va a solicitar.
3. Aceptación de las condiciones de uso del certificado.
4. Cumplimentación del formulario correspondiente¹⁰.
5. Firma electrónica¹¹ de la solicitud (formulario) por parte del *solicitante*.
6. Impresión de un resumen o justificante de la solicitud¹².

⁶ La longitud de las claves será de 2048 bits.

⁷ HSM o servidor normal.

⁸ CSR (Certificate Signing Request). Se incluye la clave pública previamente generada, y puede ser un *PKCS#10* (utilizado por el navegador Internet Explorer) o un *Spkac* (utilizado por el navegador Mozilla).

⁹ El acceso a esta aplicación se realizará sin autenticación del *solicitante*.

¹⁰ En el caso de que la petición sea para un certificado de firma de código o de sello de entidad, el nombre del *componente* no podrá entrar en conflicto con ninguna marca o patente existente. Será responsabilidad del *suscriptor* que esta premisa se cumpla.

¹¹ Esta firma se realizará con un certificado de persona física o persona jurídica (de los emitidos por la FNMT - RCM como Certificados Clase 2 CA) o con el DNIe. En el caso de que la solicitud se haga en el ámbito de la Administración Pública podrá utilizarse también el certificado de empleado público (de los emitidos por la FNMT - RCM como Certificados AP).

¹² Recogerá toda la información sobre el 9, *representante*, si lo hubiera y el *solicitante*, así como el *Código de Solicitud*.



7. Envío de la solicitud, en formato electrónico, a la FNMT – RCM.
8. Recepción del *Código de Solicitud*¹³.

Firma del Contrato

1. Complimentación del contrato¹⁴.
2. Firma electrónica del contrato. Deberá ser firmada¹⁵ por el *suscriptor* o su *representante*, en el caso de que éste sea una persona jurídica o un organismo público, y enviado a la FNMT – RCM.
3. Envío del contrato a la FNMT – RCM a la dirección de correo electrónico registroceres@fnmt.es.

5.2.1.4. Validación de la solicitud por parte de la FNMT - RCM

Recepción del contrato relativo a la solicitud del certificado

La FNMT – RCM, a través del Área de Registro del Departamento CERES, recepcionará este documento y procederá a realizar las comprobaciones pertinentes, como paso previo a la aprobación de la solicitud.

Validación de la información referente al suscriptor, representante si lo hubiera y certificado solicitado

Se realizan las comprobaciones establecidas según el tipo de *suscriptor* y la clase de certificado solicitado (*Ver Anexo I*)

Aprobación de la solicitud

Una vez realizadas las comprobaciones necesarias:

¹³ Se recomienda guardar este *Código de Solicitud* durante todo el ciclo de vida del certificado. En caso de querer hacer una revocación telefónica de este certificado este código le será solicitado (Vea el apartado *A través del Centro de Atención Telefónica (CAT) del Departamento de CERES de la FNMT – RCM* de este documento).

¹⁴ En documento aparte y específico para cada tipo de certificado.

¹⁵ Esta firma se realizará con un certificado de persona física o persona jurídica (de los emitidos por la FNMT – RCM como Certificados Clase 2 CA) o con el DNIe. En el caso de que la solicitud se haga en el ámbito de la Administración Pública podrá utilizarse también el certificado de empleado público (de los emitidos por la FNMT – RCM como Certificados AP). En cualquier caso, y en su defecto, la FNMT – RCM aceptará la firma electrónica realizada con todos aquellos certificados que cumplan lo establecido en el *Artículo 13, apartados 1 y 2, de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos* y admitidos por el Ministerio de Industria, Turismo y Comercio que cumplan lo dispuesto en los *Artículos 10 y 23 del Real Decreto 1672/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*.



Procedimientos de registro

Certificados AC de Componentes Informáticos

(*Certificados de componente*)

- a. Si todo se considera correcto, se procederá a aprobar la solicitud.
- b. En el caso de que exista falta de información, ésta no se corresponda con la solicitud, o la existente no sea válida o correcta, se desestimará la aprobación. En este caso se le notificará al *solicitante* esta desestimación comunicándole el porqué de la misma.

Archivo de la documentación recibida

Tramitada la solicitud correspondiente, toda la documentación recibida y correspondiente al certificado solicitado será archivada con todas las garantías de seguridad establecidas al efecto.

5.2.1.5. Expedición del certificado

Verificación de la solicitud

Como paso previo a la expedición del certificado, la FNMT – RCM, comprobará:

- a. Que la petición no es de alto riesgo (dominios o subdominios de nombres similares pero no iguales a otros conocidos).
- b. Que el certificado no está incluido en una lista negra creada al efecto con aquellos dominios o subdominios relacionados con usos fraudulentos y revocados por esta causa.

Expedición del certificado.

Una vez realizadas las comprobaciones pertinentes, si todo es correcto se procederá a la generación y expedición del certificado.

Notificación de la expedición del certificado

Una vez expedido el certificado, se notificará éste al *representante* del *suscriptor* y al *solicitante*.

5.2.1.6. Descarga del certificado

La descarga de los certificados se llevará a efecto través de la página web que la FNMT – RCM tiene al efecto¹⁶: <https://apuc20.cert.fnmt.es/PreregistroComponentes/>

Consulta de la petición

- a. Certificado expedido. Se procede a su descarga.
- b. Certificado no expedido. Consultar por la causa de la no expedición.

¹⁶ El acceso a esta aplicación se realizará sin autenticación del *solicitante*.



Descarga del certificado

Para esto se deberá introducir:

- El NIF del *suscriptor* del certificado.
- El *Código de Solicitud* que se generó en el momento de realizar la solicitud.

5.2.2. Revocación de certificados

5.2.2.1. Consideraciones previas

El procedimiento contemplado abarca todos los procesos, funciones y operaciones que se han de realizar desde el inicio de la solicitud de *revocación del certificado* hasta que el certificado es publicado en la lista de certificados revocados.

Esta solicitud deberá realizarla:

- Persona Física.- El *suscriptor* del certificado a revocar
- Persona Jurídica u organismo público.- El *representante* del *suscriptor* del certificado a revocar, independientemente que éste sea la misma persona que actuó como tal en la solicitud de expedición de dicho certificado.

La solicitud de revocación podrá realizarse:

- A través del Área de Registro del Departamento de CERES de la FNMT – RCM.
- De forma telefónica a través del centro de atención a usuarios del Departamento de CERES de la FNMT – RCM.

5.2.2.2. Solicitud

A través del Área de Registro del Departamento de CERES de la FNMT – RCM.

La solicitud de revocación se solicitará mediante la cumplimentación, firma electrónica¹⁷ y envío a la FNMT – RCM del contrato correspondiente.

¹⁷ Esta firma se realizará con un certificado de persona física o persona jurídica (de los emitidos por la FNMT – RCM como Certificados Clase 2 CA) o con el DNIe. En el caso de que la solicitud se haga en el ámbito de la Administración Pública podrá utilizarse también el certificado de empleado público (de los emitidos por la FNMT – RCM como Certificados AP). En cualquier caso, y en su defecto, la FNMT – RCM aceptará la firma electrónica realizada con todos aquellos certificados que cumplan lo establecido en el *Artículo 13, apartados 1 y 2, de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos* y admitidos por el Ministerio de Industria, Turismo y Comercio que cumplan lo dispuesto en los *Artículos 10 y 23 del Real Decreto 1672/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*.



Procedimientos de registro

Certificados AC de Componentes Informáticos

(*Certificados de componente*)

Versión 2.1

Página 16 de 22

Recibido la solicitud (el contrato), el Área de Registro del Departamento de CERES de la FNMT - RCM, la tramitará según el procedimiento interno establecido.

Previa a la gestión de la solicitud recibida se realizarán las comprobaciones establecidas según el tipo de *suscriptor* y la clase de certificado a revocar (*Ver Anexo II*)

El contrato, así como cualquier otra documentación relativa al certificado a revocar y recibida en la FNMT - RCM, será archivado con todas las garantías de seguridad establecidas al efecto.

A través del Centro de Atención Telefónica (CAT) del Departamento de CERES de la FNMT - RCM

Esta posibilidad estará operativa las 24 horas del día durante los 365 días del año.

El acceso a esta forma de revocación se hará a través del número de teléfono 902 200 616, 917 406 848 ó 913 878 337.

La comunicación quedará grabada y registrada, sirviendo de soporte y garantías de la aceptación de la solicitud de revocación solicitada.

El proceso es el siguiente:

Llamada al Centro de Atención Telefónica

El solicitante deberá realizar una llamada al CAT de la FNMT - RCM solicitando la revocación del certificado.

En el momento de la llamada el solicitante oirá dos mensajes:

1. Se informa al usuario que por medidas de seguridad la conversación será grabada y en caso de disconformidad lo comunique inmediatamente a la operadora.
2. Información sobre la Ley Orgánica de Protección de Datos (LOPD) vigente.

Aportación de la identidad y otros datos del solicitante

El solicitante tendrá que aportar los siguientes datos:

- Datos de identidad: Nombre, Apellidos y el número del documento de identidad correspondiente.
- Datos domiciliarios
- Datos de contacto: Al menos una dirección de correo electrónico.



Procedimientos de registro

Certificados AC de Componentes Informáticos

(*Certificados de componente*)

Versión 2.1

Página 17 de 22

Aportación de información del certificado a revocar:

- Del representante del suscriptor¹⁸: Nombre, Apellidos y NIF.
- Del suscriptor: Denominación o razón social y NIF.
- Del certificado: Nombre del componente, tipo de certificado, número de serie y causa de la revocación.

Acreditación de que el solicitante está autorizado a revocar el certificado

Esta acreditación la hará mediante la aportación del *Código de Solicitud* que se obtuvo en el momento de la solicitud del certificado.

Verificación de la información aportada por el solicitante

El registrador de la oficina de registro de la FNMT – RCM que está tratando la solicitud de revocación comprobará que toda la información aportada por el solicitante es correcta y se corresponde con el certificado a revocar.

En el caso de que esta información fuera incorrecta, el proceso de solicitud de la revocación se paralizaría indicándole al solicitante que realice esta solicitud del Área de Registro del Departamento de CERES de la FNMT – RCM.

Aceptación de la solicitud de revocación

La comunicación entre el solicitante y el CAT quedará grabada y registrada¹⁹, sirviendo de soporte y garantías de la aceptación de la solicitud de revocación solicitada.

Tratamiento de la solicitud

El registrador, una vez comprobado que la información aportada se corresponde con el certificado a revocar, procederá a revocar el certificado.

Firma de Contrato

Como resultado de la revocación se imprimirán tres copias del contrato, las cuales serán firmadas por el registrador, y a las cuales se les incorporará un sello relativo a este tipo de revocaciones telefónicas.

¹⁸ Si el certificado está a nombre de una persona jurídica u organismo público. En este caso, la persona física que aparece como tal en el certificado.

¹⁹ Quedará grabada y registrada la siguiente información: Fecha, hora de inicio y hora final de la llamada; Objeto de la llamada: revocación del certificado; Nombre, Apellidos y número del documento de identidad del solicitante; si solicita el envío del contrato y si así fuera, la dirección postal al que se le ha de enviar.



Envío de una copia del contrato al solicitante

En el caso de que el solicitante haya solicitado una copia del contrato se le enviará ésta a la dirección postal que haya aportado previamente.

5.2.2.3. *Revocación del certificado*

Revocación del certificado

Una vez realizada y procesada la solicitud se procederá a la *revocación del certificado*.

Notificación de la revocación del certificado

Una vez revocado el certificado, se notificará ésta al *representante del suscriptor*.



Procedimientos de registro

Certificados AC de Componentes Informáticos

(*Certificados de componente*)

Versión 2.1

Página 19 de 22

6. ANEXO I. DOCUMENTACIÓN NECESARIA PARA LA ACEPTACIÓN DE UNA SOLICITUD PARA LA EXPEDICIÓN DE UN CERTIFICADO

6.1. ORGANISMO PÚBLICO

6.1.1. Documentación que hay que enviar

- El contrato

Deberá firmarse electrónicamente con los certificados electrónicos aprobados y enviarse en formato electrónico a la dirección de correo electrónico establecida, no admitiéndose en ninguna circunstancia la firma manuscrita y su posterior envío en papel.

- Documento de cesión del dominio (sólo cuando el solicitante del certificado no sea el titular del dominio)

El organismo o empresa titular del dominio deberá remitir un escrito oficial (documento administrativo con sello del organismo o empresa), firmado por un representante de este organismo o empresa con capacidad de representación suficiente, y legitimado notarialmente. Deberá estar acompañado de un poder notarial en el que se haga constar la representación de esta persona con la empresa titular del dominio.

6.1.2. La FNMT - RCM, comprobará

- 1º. Que la información del contrato y la solicitud coinciden.
- 2º. Que la firma electrónica del contrato es válida y correcta.
- 3º. La identidad del *suscriptor*
- 4º. La identidad del *representante*, cuando éste sea el firmante del contrato.
- 5º. Que el contrato ha sido firmado por el *suscriptor* o su *representante*.
- 6º. Que el *representante* puede actuar como tal en la solicitud de expedición del certificado.
- 7º. La titularidad del dominio o dominios solicitados

6.2. PERSONA JURÍDICA

6.2.1. Documentación que hay que enviar

- El contrato

Deberá firmarse electrónicamente con los certificados electrónicos aprobados y enviarse en formato electrónico a la dirección de correo electrónico establecida, no admitiéndose en ninguna circunstancia la firma manuscrita y su posterior envío en papel.



- Documento de cesión del dominio (sólo cuando el solicitante del certificado no sea el titular del dominio)

El organismo o empresa titular del dominio deberá remitir un escrito oficial (documento administrativo con sello del organismo o empresa), firmado por un representante de este organismo o empresa con capacidad de representación suficiente, y legitimado notarialmente. Deberá estar acompañado de un poder notarial en el que se haga constar la representación de esta persona con la empresa titular del dominio.

6.2.2. La FNMT - RCM, comprobará

- 1º. Que la información del contrato y la solicitud coinciden
- 2º. Que la firma electrónica del contrato es válida y correcta.
- 3º. La identidad del *suscriptor*
- 4º. La identidad del *representante*, cuando éste sea el firmante del contrato.
- 5º. Que el contrato ha sido firmado por el *suscriptor* o su *representante*.
- 6º. Que el *representante* puede actuar como tal en la solicitud de expedición del certificado.
- 7º. La titularidad del dominio o dominios solicitados



Procedimientos de registro

Certificados AC de Componentes Informáticos

(*Certificados de componente*)

Versión 2.1

Página 21 de 22

1. ANEXO II. DOCUMENTACIÓN NECESARIA PARA LA ACEPTACIÓN DE UNA PETICIÓN PARA LA REVOCACIÓN DE UN CERTIFICADO A TRAVÉS DE LA OFICINA DE REGISTRO DE CERES

1.1. ORGANISMO PÚBLICO CON ENCOMIENDA DE GESTIÓN O CONVENIO FIRMADO

1.1.1. Documentación que hay que enviar

- El contrato

Deberá firmarse electrónicamente con los certificados electrónicos aprobados y enviarse en formato electrónico a la dirección de correo electrónico establecida, no admitiéndose en ninguna circunstancia la firma manuscrita y su posterior envío en papel.

1.1.2. La FNMT - RCM, comprobará

- 1º. Que la firma electrónica del contrato es válida y correcta.
- 2º. La identidad del *suscriptor*
- 3º. La identidad del *representante*, cuando éste sea el firmante del contrato.
- 4º. Que el contrato ha sido firmado por el *suscriptor* o su *representante*.
- 5º. Que el *representante* puede actuar como tal en la solicitud de revocación del certificado.
- 6º. Número de serie del certificado.

1.2. PERSONA JURÍDICA

1.2.1. Documentación que hay que enviar

- El contrato

Deberá firmarse electrónicamente con los certificados electrónicos aprobados y enviarse en formato electrónico a la dirección de correo electrónico establecida, no admitiéndose en ninguna circunstancia la firma manuscrita y su posterior envío en papel.

1.2.2. La FNMT - RCM, comprobará

- 1º. Que la firma electrónica del contrato es válida y correcta.
- 2º. La identidad del *suscriptor*
- 3º. La identidad del *representante*, cuando éste sea el firmante del contrato.
- 4º. Que el contrato ha sido firmado por el *suscriptor* o su *representante*.
- 5º. Que el *representante* puede actuar como tal en la solicitud de revocación del certificado.
- 6º. Número de serie del certificado.

