DIRECCIÓN DE SISTEMAS DE INFORMACIÓN
DEPARTAMENTO CERES
ÁREA DE REGISTRO

CERTIFICADOS ELECTRÓNICOS CUALIFICADOS DE FIRMA ELECTRÓNICA CENTRALIZADA PARA EL PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN PÚBLICA EMITIDOS POR LA FNMT – RCM

(CERTIFICADOS ELECTRÓNICOS CUALIFICADOS DE FIRMA ELECTRÓNICA CENTRALIZADA PARA EMPLEADOS PÚBLICOS)

[PROCEDIMIENTO DE REGISTRO]

Versión 2.1

	NOMBRE	FECHA
Elaborado por:	Área de Registro	
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO			
Versión	**Fecha**	**Descripción**	**Autor**
V 1.0	21 de septiembre de 2017	Creación del documento	Área de Registro
V 1.1	4 de octubre de 2018	Actualización de la acreditación para los extranjeros. El punto *5.2.1 Solicitud*, pasa a denominarse *Solicitud del certificado y obtención de las credenciales de acreditación.* El *PIN*, pasa a llamarse *PIN de firma*, y se genera en el HSM, una vez creadas las claves pública y privada. Se cambia el proceso de obtención del *PIN de firma*. Certificado cualificado – Firma avanzada.	Área de Registro

V 1.2	28 de noviembre de 2019	Un certificado por firmante (No se contempla la posibilidad de un certificado por organismo al que esté adscrito). Se expedirán dos certificados, uno a través de la AC AP y el otro de la AC Servicio Público. Se contempla un aviso en caso de discrepancia entre el primer apellido de un nuevo certificado solicitado y el de otro certificado activo en ese momento. Creación del Anexo III. Posibles escenarios existentes en el proceso de revocación de certificados.	Área de Registro
V 2.0	5 de octubre de 2020	El Código de solicitud se le envía al solicitante a través de la dirección de correo que aporta en el momento de la solicitud. Se añade un campo nuevo en la solicitud para recoger esta dirección de correo electrónico. Se modifica la solicitud autenticada en cuanto a los certificados válidos para esta autenticación. Se elimina el Anexo I Dirección de internet. Se elimina el Aneo II. Documentos acreditación de la identidad de una persona física, y se hará referencia al documento específico Acreditación identidad-NIF_NIE.	Área de Registro
V 2.1	20 de enero de 2021	Actualización de la referencia respecto a la normativa sobre la firma electrónica, sustituyendo la *Ley 95/2003, de 19 de diciembre, de firma electrónica* por la actual *Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.*	Área de Registro

Referencia:

Documento clasificado como: *Público*

Índice

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 suscriptores del propio certificado; los registradores, a través de las oficinas de registro; y la FNMT – RCM.

Este documento contempla los procedimientos a seguir por las partes involucradas en la gestión de los certificados en el ámbito de la Administración Pública, y para los referidos como *Certificados electrónicos cualificados de firma electrónica centralizada para el personal al servicio de la Administración Pública*.

Para que un usuario pueda acceder a los servicios de certificación ofrecidos por la FNMT-RCM es necesario que se realice una operación previa de registro en la infraestructura, la cual se realizará a través de la red de oficinas de registro designadas por el Órgano, Organismo o Entidad Pública (en adelante Organismo) correspondiente, donde presta sus servicios el firmante y custodio del certificado

En esta operación de registro, la FNMT-RCM verifica la identidad del usuario y recoge los datos necesarios para expedir, revocar y en su caso suspender y cancelar la suspensión, del certificado correspondiente.

Las operaciones de registro (tanto para la emisión como para la revocación) requieren siempre la comprobación de la identidad del solicitante, la cual se realizará a partir del documento de acreditación correspondiente. Estas operaciones, se llevarán a cabo en las oficinas de registro implantadas por las AAPP o a través de nuestra web mediante la autenticación del solicitante con el certificado correspondiente.

Todos los procedimientos aquí descritos están basados y soportados por la *DPC*, así como por las *Políticas y Prácticas de Certificación Particulares* correspondientes a estos certificados.

2. ACRÓNIMOS Y DEFINICIONES

2.1. ACRÓNIMOS

AAPP	Administraciones Públicas
AP	Administración Pública
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

2.2. DEFINICIONES

Aplicación de Registro	Aplicación Web mediante la cual se gestionan las solicitudes de emisión, revocación, y en su caso la suspensión y cancelación de la suspensión de un certificado
Cancelación de la Suspensión de Certificados	Procedimiento por el cual la FNMT-RCM activa nuevamente un certificado previamente suspendido, previa solicitud de la Oficina de Registro de la AP.
Certificado electrónico cualificado de firma electrónica centralizada para el personal al servicio de la Administración Pública	Certificado electrónico expedido por la FNMT-RCM al Personal al servicio de la Administración, orientado a la realización de firmas en remoto o en servidor. Esto significa que la generación de las Claves pública y privada se generan y almacenan en un entorno seguro perteneciente a la FNMT-RCM, garantizándose en todo momento el control exclusivo del uso de dichas claves por parte del firmante.
Clave de firma	Clave que protege la clave privada del certificado, cuando éste se expide a través de la AC Sector Público.
Clave de usuario	Forma parte de las *Credenciales de identificación*. Siempre será el NIF del usuario.
Contraseña	Forma parte de las *Credenciales de identificación*. Las genera el sistema. LA mitad se le entregará en el momento de la acreditación. La otra mitad se envía por correo electrónico.

Credenciales de identificación	La componen la *clave de usuario* y una *contraseña*. Junto con un clave *OTP*, sirven para identificar al usuario y le permiten acceder de forma segura al *Portal de gestión de identidades*, y a su clave privada.
Cuenta de usuario	Una por usuario y asociada a la identidad de este usuario. Se identifica con el primer apellido y el NIF del usuario. Recoge toda la información relativa a esta persona, tanto la personal como la del organismo, actualizándose dicha información, con la última aportada por el último certificado electrónico solicitado. Estará habilitada mientras exista un certificado electrónico activo.
Expedición de Certificados	Procedimiento por el cual la FNMT-RCM crea un certificado, previa solicitud recibida de la Oficina de Registro, y a nombre de la persona al servicio de dicha Administración Pública.
Firmante	Persona al servicio de la Administración Pública que hace uso de sus datos de creación de firma.
Identidad de firma	Lo componen la clave privada y la clave pública.
OTP (One Time Password)	Clave de único uso generada por el sistema en el momento de acceder al *Portal de Gestión de Identidades* o a su clave privada para la realización de una firma. Se envía al usuario a través de la dirección de correo electrónico que aportó en el momento de la solicitud del certificado electrónico.
Pin de firma	Clave que protege la clave privada del certificado, cuando éste se expide a través de la AC AP.
Registrador	Persona responsable del registro, que ha de comprobar, garantizar y autenticar la identidad de las personas que solicitan un certificado así como el resto de la información que se ha de incorporar al certificado. Todos los Registradores deberán ser funcionarios o personas adscritos a la Administración y estar en poder de un certificado emitido por la FNMT-RCM.
Registro de Usuarios	Procedimiento por el que mediante una aplicación Web, se toman los datos personales de un solicitante, se confirma su identidad y se formaliza su contrato con la FNMT-RCM para la emisión o revocación de un certificado.

Revocación de Certificados	Procedimiento por el cual la FNMT-RCM deja sin efecto la validez del certificado del solicitante, previa solicitud de la Oficina de Registro.
Solicitante	Persona que realiza una solicitud de registro para la emisión o revocación de certificados así como para la suspensión o cancelación de la suspensión de estos.
Soporte del Certificado	Lugar o dispositivo donde se guarda el certificado, y desde donde se ejecuta la firma electrónica.
Suscriptor	Órgano, Organismo o Entidad de la Administración Pública, bien sea ésta General, Autonómica o Local, cuya identidad queda vinculada a la clave pública consignada en el certificado.
Suspensión de Certificados	Procedimiento por el cual la FNMT-RCM deja sin efecto la validez del certificado del solicitante durante un período de tiempo y en unas condiciones determinadas, previa solicitud de la Oficina de Registro.

3. ENTIDADES INVOLUCRADAS

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

- Los suscriptores de los certificados, solicitantes de la expedición y revocación de los certificados.
- Las AAPP, en su actividad como oficina de registro.
- La FNMT-RCM que actúa como PSC.

4. GESTIÓN DE SOLICITUDES DE CERTIFICADOS. CONSIDERACIONES PREVIAS

- Las oficinas de registro solo podrán gestionar solicitudes al personal que preste sus servicios en la entidad a la que está adscrita[1].
- La FNMT – RCM avisará al suscriptor del certificado y al firmante del mismo, cualquier cambio del estado de éste.
- Un firmante podrá tener únicamente dos certificados de estas características, independientemente del número de organismos a los que esté adscrito. Uno de ellos expedito por la AC AP y otro por la AC Sector Público.
- No se contemplan los casos de suspensión y cancelación de la suspensión del certificado.
- De igual manera no se contempla la posibilidad de renovación de estos certificados.

[1] Sin perjuicio de la creación de oficinas de registro delegadas, centralizadas o implantadas mediante Convenios entre Administraciones.

- La duración del certificado será de dos (2) años para los expedidos en el año 2019 y de un (1) años, para los que se expidan en el año 2020[2].
- La clave privada en ningún momento estará en poder de los firmante, sino en la infraestructura del PSC. El firmante generará sus claves pública y privada (*Identidad de firma*) en el entorno seguro de la FNMT-RCM. La clave privada queda almacenada de forma protegida, garantizando el control exclusivo del uso de la misma por parte del firmante.

5. SOLICITUD DE EXPEDICIÓN DE CERTIFICADOS

5.1. INTRODUCCIÓN

- La solicitud de estos certificados deberá ser realizada por el firmante, debiendo ser éstos, personas físicas mayores de edad o menores que ostenten la facultad de emancipados[3].
- La acreditación de la identidad del suscriptor se llevará a cabo en las oficinas de registro correspondientes, y pertenecientes al organismo, y en su caso a la unidad organizativa, a la cual esté adscrito el empleado público para el cual será expedido el certificado[4]. También podrá hacerse de forma telemática, acreditándose con un certificado electrónico de empleado público, de los emitidos por la FNMT-RCM.
- Será responsabilidad de los correspondientes organismos que actuarán a través de las oficinas de registro, comprobar que estos firmantes del certificado se encuentran con su cargo, número de identificación profesional, empleo o autorización en vigor y, por tanto, habilitados para obtener el certificado.
- Las actividades de comprobación de esta información serán realizadas por las oficinas de registro implantadas por el organismo en cuestión, y que se corresponde, en cada caso, con el organismo, y en su caso unidad organizativa, a la que está adscrito el suscriptor y el firmante del certificado.

5.2. PROCEDIMIENTO

El procedimiento contemplado para la realización de esta opción abarca todos los procesos, funciones y operaciones que se han de realizar desde el inicio de la solicitud del certificado, hasta que el personal al servicio de las *AAPP* disponga de su certificado para acceder a los servicios de seguridad.

Este procedimiento consta de varias fases, la cuales se detallan a continuación.

[2] Por caducidad del certificado de la AC en el año 2021.

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

[4] Sin perjuicio de la creación de oficinas de registro delegadas, centralizadas o implantadas mediante Convenios entre Administraciones.

5.2.1. Solicitud del certificado electrónico y obtención de las C*redenciales de identificación.*

El empleado público, desde el equipo de su puesto de trabajo, realiza la solicitud para el certificado correspondiente a través de la Web que a tal efecto ha dispuesto la FNMT – RCM[5].

En este primer paso el solicitante:

- Aportará la siguiente información:
  - El número del documento de identidad[6].
  - El primer apellido del solicitante.
  - El NIF del organismo al que pertenece.
  - Una dirección de correo electrónico.
- Aceptará las condiciones de uso del certificado.
- La FNMT – RCM, a la recepción de la solicitud le devolverá al solicitante un *Código de solicitud*[7] asociado a dicha solicitud[8].

❖ En este caso, para este tipo de certificados, en este primer paso no se solicita el certificado ni se generan las claves.

5.2.2. Acreditación de la identidad y otra información del solicitante

5.2.2.1. A través de una oficina de registro

Personación ante las Oficinas de Registro

La acreditación se realizará mediante la personación[9] del empleado público ante la oficina de registro designada a tal efecto por el organismo, suscriptor del certificado y al que pertenece dicho empleado público.

---

[5] En este caso, y para este tipo de certificados, en este primer paso no se genera una petición de solicitud ni se generan las claves pública y privada.

[6] Según lo establecido en el documento *Acreditación identidad-NIF_NIE_v1.0.*

[7] Se recomienda al firmante (empleado público) que guarde 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 *5.3.1.2 A través del Centro de Atención Telefónica (CAT) de la FNMT – RCM (revocación telefónica)* de este documento.

[8] Se enviará a través de la dirección de correo electrónico aportada en el momento de realizar la solicitud.

[9] A estos efectos FNMT-RCM tendrá en cuenta las funcionalidades previstas en la legislación aplicable en relación con el DNIe, así como los sistemas de identificación y comprobación del cargo, función o empleo aplicables en las AAPP, por lo que el requisito de personación podrá ser sustituido por otros procedimientos que permitan la identificación, siempre que estén amparados por la intervención de la oficina de registro. En estos supuestos de procedimientos especiales de identificación propios del ámbito público, no será necesaria la personación

Datos y documentación

En este acto, el empleado público, aportará los datos y documentación exigida, así como acreditará su identidad personal y otras si fuera preciso. Igualmente deberá aportar el *Código de solicitud*.

I. Cumplimentación, por parte del registrador, del formulario correspondiente.

- ✓ Datos identificativos del firmante y del organismo
- ✓ *Código de solicitud*

II. Presentará la documentación[10] establecida que avale los datos registrados anteriormente en el formulario, especialmente:

- ❖ El de su identidad: Documentación original o fotocopia compulsada por el organismo al cual pertenezca el empleado público relativa a su identificación personal[11].
- ❖ Su condición de personal al servicio de la *AP*.
- ❖ El de cualquier otra información que vaya a incorporarse en el certificado y la oficina de registro estime oportuno.

Generación de las Credenciales de identificación [12]

En este paso del proceso, se generará:

- ✓ La *clave de usuario*
- ✓ La mitad de la *contraseña*.

Si cuando se expida un nuevo certificado existiera uno activo de la misma AC que el nuevo que se va a expedir, en este proceso, además de la revocación del existente, se borrarán las *Claves de identidad* asociadas a este certificado, y se generaría una nueva *contraseña*.

Firma del contrato

Una vez acreditada la identidad del empleado público el registrador imprimirá dos copias del contrato[13], el cual recoge

---

cuando por el órgano competente de la Administración se proceda a certificar los requisitos de identidad, vigencia del cargo y demás condiciones a comunicar a la oficina de registro, de acuerdo con lo previsto en la normativa vigente.

[10] Toda la documentación aportada deberá ser válida y estar vigente. Igualmente se deberá tener en cuanto cualquier otro medio admitido en derecho a efectos de identificación.

[11] Según lo establecido en el documento *Acreditación identidad-NIF_NIE_v1.0*.

[12] En el caso de que ya exista algún certificado activo, y al ser las mismas *Credenciales de identificación* similares para todos los certificados, no se generarán unas nuevas.

[13] Una para la oficina de registro y la otra para empleado público que pasa a ostentar la figura de firmante.

- ✓ Información relativa a dicho empleado público y del organismo
- ✓ Las *condiciones de uso* del certificado.
- ✓ Las *Credenciales de identificación*[14] [15] del solicitante.

Ambas copias serán firmadas por el firmante y el registrador.

En el caso de que el contrato se gestionara en formato electrónico, este deberá ser firmado electrónicamente[16].

Guarda y custodia de la documentación relacionada con el certificado

Toda la documentación generada y asociada a la expedición del certificado, incluido el contrato[17], deberá ser guardada y custodiada por la oficina de registro durante el tiempo previsto por la normativa al efecto[18].

Igualmente, esta documentación deberá estar a disposición de la FNMT – RCM, durante, al menos, el periodo de tiempo señalado por la legislación que la regula.

Envío de la solicitud a la FNMT-RCM

Una vez firmado el contrato por ambas partes, el registrador procederá a enviar la información recogida, la solicitud, a la FNMT - RCM[19] [20].

[14] En este primer paso, únicamente la mitad de la contraseña.

[15] En el caso de que ya exista algún certificado activo, y al ser las mismas *Credenciales de identificación* similares para todos los certificados y no tenerlas, por seguridad, la FNMT-RCM, no incluirá en el contrato las ya existentes en poder del firmante.

[16] Esta firma se realizará con un certificado de persona física (de los emitidos por la FNMT – RCM como Certificados AC FNMT Usuarios), de representante (de los emitidos por la FNMT – RCM como Certificados AC Representación) 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 o Certificado SP). En cualquier caso, y en su defecto, la FNMT – RCM acepará la firma electrónica realizada con todos aquellos certificados que cumplan lo establecido por la normativa vigente.

[17] Tanto si el contrato se haya gestionado en papel o de forma electrónica.

[18] En la actualidad el tiempo previsto es de 15 años (*Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Artículo 9, 3 a.*)

[19] Esta transmisión de información a la FNMT-RCM se realizará mediante comunicaciones seguras establecidas para tal fin entre la oficina de registro y la FNMT-RCM.

[20] Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

5.2.2.2. *De manera telemática*

Acreditación y aportación de otra información del solicitante

Este certificado podrá obtenerse de manera telemática a través de nuestra página web y siempre que se cumplan los siguientes requisitos, en relación con el certificado electrónico que vaya a utilizarse para su autenticación:

- Que no haya caducado.
- Que tenga la misma información que el que se vaya a solicitar (organismo, cargo, etc.).
- Que se haya obtenido, con acreditación previa de la identidad, de manera presencial en una oficina de registro, y en un plazo no superior a cinco (5) años.
- Que sea un certificado de empleado público o empleado público de firma centralizada, emitidos a través de la Autoridad de Certificación de Administración Pública (AC AP) o Sector Público (AC SP) por la FNMT-RCM.

Datos y documentación

Toda la información referente a la solicitud se extraerá del certificado utilizado para la autenticación.

Además, deberá incorporar el *código de solicitud.*

Generación de las Credenciales de identificación [21]

En este paso del proceso, se generará:

- ✓ La *clave de usuario*
- ✓ La mitad de la *contraseña.*

Si cuando se expida un nuevo certificado existiera uno activo de la misma AC que el nuevo que se va a expedir, en este proceso, además de la revocación del existente, se borrarán las *Claves de identidad* asociadas a este certificado, y se generaría una nueva *contraseña*.

Firma del contrato

Una vez acreditada la identidad del empleado público y obtenida el resto de la información del solicitante, éste firmará electrónicamente el contrato, el cual recoge

- ✓ Información relativa a dicho empleado público y del organismo
- ✓ Las *Condiciones de uso* del certificado.

[21] En el caso de que ya exista algún certificado activo, y al ser las mismas *Credenciales de identificación* similares para todos los certificados, no se generarán unas nuevas.

Entrega de las credenciales de identificación

Una vez firmado el contrato, se le mostrarán en pantalla las *Credenciales de identificación*[22] del solicitante[23].

Guarda y custodia de la documentación relacionada con el certificado

Toda la documentación generada y asociada a la expedición del certificado, incluido el contrato, será guardada y custodiada por la FNMT-RCM durante el tiempo previsto por la normativa al efecto[24].

Envío de la solicitud a la FNMT-RCM

Una vez firmado el contrato, la aplicación procederá a enviar la información recogida, la solicitud, a la FNMT - RCM[25] [26].

5.2.3. Creación de la *Cuenta de usuario*

Una vez finalizado el proceso de registro:

- Se generará una *Cuenta de usuario*[27], con la información obtenida en el momento de la acreditación[28]. En el caso de que ya existiera una cuenta habilitada, y se solicitara un nuevo certificado, la información proporcionada por este último actualizaría la existente, independientemente de la *AC* a través de la cual se expida el certificado.

5.2.4. Finalización de la generación de las *Credenciales de identificación*

Una vez creada la mitad de la *contraseña* que faltaba, ésta le será enviada al solicitante a través de la dirección de correo electrónico que aportó en el momento de la solicitud.

[22] En este primer paso, únicamente la mitad de la contraseña.

[23] En el caso de que ya exista algún certificado activo, y al ser las mismas *credenciales de identificación* similares para todos los certificados y no tenerlas, por seguridad, la FNMT-RCM, no se generarán unas nuevas y tampoco se mostrarán las existentes en poder del firmante.

[24] En la actualidad el tiempo previsto es de 15 años (*Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Artículo 9, 3 a.*)

[25] Esta transmisión de información a la FNMT-RCM se realizará mediante comunicaciones seguras establecidas para tal fin por la FNMT-RCM.

[26] Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

[27] En el caso de que el usuario no tuviera otra con anterioridad.

[28] En el caso de que ya existiera una cuenta de usuario habilitada, no se crearía otra (sólo se tiene una cuenta de usuario por firmante).

5.2.5. Acceso al Portal de Gestión de Identidades (*Generación del certificado*)

El solicitante accederá al *Portal de gestión de identidades*[29], identificándose previamente. Esta identificación podrá hacerse:

- ✓ Con las *Credenciales de identificación* obtenidas con anterioridad, más un segundo factor de autenticación, *OTP*, o
- ✓ Con un certificado electrónico[30].

Una vez en el portal:

- ➢ Si es la primera vez que se accede y no existe ningún certificado activo

  El usuario ha de:

  - Cambiar la contraseña
  - Establecer el *PIN de firma* o la *Clave de firma* del certificado que se va a expedir.

  El sistema:

  - Crea la *Identidad de firma*.
  - Genera y expide el certificado
- ➢ Si no es la primera vez que se accede y se ha solicitado un nuevo certificado

  El usuario ha de:

  - Cambiar la contraseña [sólo si ha habido un cambio de contraseña previamente]
  - Establecer el *PIN de firma* o la *Clave de firma* del nuevo certificado que se va a expedir.

  El sistema:

  - Crea la *Identidad de firma* del nuevo certificado
  - Genera y expide el nuevo certificado

5.2.6. Creación de la *Identidad de firma*

Una vez realizados los pasos establecidos en el punto anterior, el sistema procederá a la creación de la *Identidad de firma*, mediante la generación de las claves pública y privada[31].

[29] La primera que se accede al Portal de gestión de identidades, el sistema le obligará a cambiar la contraseña.

[30] Los certificados electrónicos admitidos son los expedidos por la FNMT-RCM, como certificados de persona física y empleado público. También se puede utilizar el DNIe.

[31] Se generarán en un dispositivo HSM.

En ese momento, el sistema, requerirá al solicitante que establezca el *PIN de firma* o la *Clave de firma* que protegerá la clave privada frente a terceros, y que le será requerido en el momento de la firma para el uso de esta clave.

5.2.7. Expedición del certificado

Una vez establecido el *PIN de firma* o la *Clave de firma*, y creada la *Identidad de firma*, se expedirá el certificado correspondiente.

5.2.8. Notificación de la expedición del certificado

En el momento de la expedición del certificado, se notificará al solicitante, mediante un mensaje en la propia pantalla de la máquina donde esté realizando este trámite, la creación de la Identidad de firma, lo que lleva asociado la expedición del certificado.

5.2.9. Publicación del certificado

Generado el certificado, éste se publicará en una nueva base de datos de la AC.

6. REVOCACIÓN DE CERTIFICADOS

6.1. CONSIDERACIONES PREVIAS

- La revocación de certificados implica, en general:
  - La extinción y finalización de la relación y régimen de uso del certificado con la FNMT-RCM.
  - La deshabilitación de la *Cuenta de usuario*[32].
  - La anulación de las *Credenciales de identificación*[33].
  - La eliminación de las claves, pública y privada.

  Para ver los distintos posibles escenarios en el proceso de revocación, vea al *Anexo I. Posibles escenarios existentes en el proceso de revocación de certificados.*

[32] Siempre y cuando no exista otro certificado activo, en cuyo caso la *Cuenta de usuario* permanecerá habilitada. En el caso de que se deshabilite la cuenta, y se vuelva a solicitar un nuevo certificado, la cuenta volverá a habilitarse recuperando toda la información existente previamente a la deshabilitación.

[33] Siempre y cuando no exista otro certificado activo, en cuyo caso las *Credenciales de identificación* seguirán activas. En el caso de la *Cuenta de usuario* esté deshabilitada y se solicite un nuevo certificado, ésta se habilitará y se generarían unas nuevas *Credenciales de identificación*.

- La revocación de este tipo de certificados podrá ser solicitada, tanto por el firmante como por el suscriptor.
- No obstante, la FNMT-RCM podrá revocar los certificados para el personal al servicio de la Administración en los supuestos recogidos en la DPC correspondiente.
- La Ley de Expedición podrá establecer adicionalmente otras causas de revocación.
- La revocación de estos certificados se realizará a través de la oficina de registro, que perteneciente al suscriptor, esté adscrito el firmante de dicho certificado[34]. En el caso de que sea el firmante el solicitante de la revocación, además del procedimiento establecido para el suscriptor, éste podrá revocar el certificado de forma telefónica a través de del Centro de Atención Telefónica (CAT) que la FNMT – RCM ha habilitado a tal efecto[35].
- La revocación de un certificado, existiendo dos certificados activos, supondrá
  - Si el nuevo certificado se expide a través de la AC AP, revocará únicamente, el activo perteneciente a esta AC.
  - Si el nuevo certificado se expide a través de la AC Servicio Público, se revocarán los dos certificados que pudiera haber, el perteneciente a la AC Servicio Público y el perteneciente a la AC AP.

6.2. PROCEDIMIENTO

6.2.1. Solicitud

6.2.1.1. A través de la oficina de registro a la cual está adscrito el suscriptor

Acreditación de la identidad

El solicitante deberá presentarse[36] ante la oficina de registro a la cual está adscrito el suscriptor del certificado a revocar, donde acreditará su identidad.

En este acto, el solicitante aportará los datos y documentación establecida, así como acreditará la identidad personal del empleado público (firmante).

---

[34] Sin perjuicio de la creación de oficinas de registro delegadas, centralizadas o implantadas mediante Convenios entre Administraciones.

[35] Este servicio se prestará durante las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año.

[36] A estos efectos *FNMT-RCM* tendrá en cuenta las funcionalidades previstas en la legislación aplicable en relación con el DNIe, así como los sistemas de identificación y comprobación del cargo, función o empleo aplicables en las *AAPP*, por lo que el requisito de personación podrá ser sustituido por otros procedimientos que permitan la identificación, siempre que estén amparados por la intervención de la oficina de registro. En estos supuestos de procedimientos especiales de identificación propios del ámbito público, no será necesaria la personación cuando por el órgano competente de la Administración se proceda a certificar los requisitos de identidad, vigencia del cargo y demás condiciones a comunicar a la oficina de registro, de acuerdo con lo previsto *en la normativa en vigor.*

Cumplimentación del formulario de revocación

El registrador, cumplimentará el formulario que a tal efecto propiciará la aplicación de registro, con los datos del suscriptor y el firmante del certificado objeto de la revocación, así como del solicitante de la petición de revocación.

Firma de Contrato

Una vez verificada la identidad del solicitante de la revocación y cumplimentado el formulario, el registrador imprimirá dos copias del contrato[37], que serán firmadas por el solicitante y el propio registrador.

En el caso de que el contrato se gestionara en formato electrónico, este deberá ser firmado electrónicamente[38].

Envío de la solicitud a la FNMT-RCM

Una vez firmado el documento que recoge las condiciones de uso del certificado por ambas partes, el registrador validará los datos recogidos y procederá a enviar esta información, la solicitud, a la FNMT - RCM[39] [40].

6.2.1.2. A través del Centro de Atención Telefónica (CAT) de la FNMT – RCM (revocación telefónica)

Llamada al Centro de Atención Telefónica

El solicitante[41] deberá realizar una llamada[42] al CAT de la FNMT - RCM solicitando la revocación de su certificado.

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

---

[37] Una para la oficina de registro y la otra para el solicitante de la revocación.

[38] Esta firma se realizará con un certificado de persona física (de los emitidos por la FNMT – RCM como Certificados AC FNMT Usuarios), 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 o Certificados SP). En cualquier caso, y en su defecto, la FNMT – RCM acepará la firma electrónica realizada con todos aquellos certificados que cumplan con la normativa existente al efecto.

[39] Esta transmisión de información a la FNMT-RCM se realizará mediante comunicaciones seguras establecidas para tal fin entre la oficina de registro y la FNMT-RCM.

[40] Los datos personales y su tratamiento quedarán sometidos a la legislación específica.

[41] El firmante (empleado público).

[42] Este servicio se prestará a través del número de teléfono 902 200 616, 917 406 848 o 913 878 337.

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 del solicitante

El solicitante, que en este caso es siempre el firmante del certificado, tendrá que aportar los datos de su identidad: Nombre, Apellidos y el número del documento de identidad correspondiente.

Acreditación de que el solicitante es el firmante del certificado a revocar

Esta acreditación la hará mediante la aportación del *Código de solicitud* que 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 a través de la oficina de registro a la cual está adscrito el suscriptor.

Aceptación de la solicitud de revocación

La comunicación entre el solicitante y el CAT quedará grabada y registrada[43], 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 resultas de la revocación se imprimirán dos 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.

[43] 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.

El registrador preguntará al peticionario de la revocación si quiere recibir la copia del contrato correspondiente al solicitante.

El envío de esta copia podrá hacerse también en formato electrónico, firmándose en este caso, dicha copia, de forma electrónica.

Envío de una copia del contrato al solicitante

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

6.2.2. Guarda y custodia de la documentación relacionada con el certificado

Toda la documentación generada y asociada a la expedición del certificado, incluido el contrato[44], deberá ser guardada y custodiada por la oficina de registro[45] durante el tiempo previsto por la normativa al efecto[46].

Igualmente esta documentación deberá estar a disposición de la FNMT – RCM, durante al menos, el periodo de tiempo señalado por la legislación que la regula[47].

6.2.3. Anulación de la identidad del usuario

Una vez recibida la petición de solicitud de revocación, se procederá a eliminar la identidad del usuario, lo que significa:

- ✓ Eliminación de las claves, pública y privada.
- ✓ Deshabilitar la *Cuenta del usuario*[48].
- ✓ Anulación de las *Credenciales de identificación*[49].

---

[44] Tanto si el contrato se haya gestionado en papel o de forma electrónica.

[45] Según consta en el Convenio o Encomienda de Gestión firmado entre el Organismo al cual pertenece la oficina de registro, y la FNMT – RCM.

[46] En la actualidad el tiempo previsto es de 15 años (*Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Artículo 9, 3 a.*)

[47] Según consta en el Convenio o Encomienda de Gestión firmado entre el Organismo al cual pertenece la oficina de registro, y la FNMT – RCM.

[48] Siempre y cuando no exista otro certificado activo, en cuyo caso la *Cuenta de usuario* permanecerá habilitada. En el caso de que se deshabilite la cuenta, y se vuelva a solicitar un nuevo certificado, la cuenta volverá a habilitarse recuperando toda la información existente previamente a la deshabilitación.

[49] Siempre y cuando no exista otro certificado activo, en cuyo caso las *Credenciales de identificación* seguirán activas. En el caso de la *Cuenta de usuario* esté deshabilitada y se solicite un nuevo certificado, ésta se habilitará y se generarían unas nuevas *Credenciales de identificación*.

6.2.4. Revocación de los certificados

Recibida la solicitud por parte de la FNMT - RCM, y tras ésta procederá a la revocación del certificado solicitado.

6.2.5. Notificación de la revocación del certificado

Una vez revocado el certificado, se notificará ésta al solicitante de la petición de revocación y al firmante, que aparecía como tal, en el certificado revocado[50].

6.2.6. Publicación de los certificados

Una vez que la *FNMT - RCM* ha procedido a la revocación del certificado, se publicará en el Directorio la correspondiente *LCR* indicando:

- ✓ El número de serie del certificado revocado.
- ✓ La fecha y hora en que se ha realizado la revocación.
- ✓ La causa de revocación.

7. SUSPENSIÓN DE CERTIFICADOS

No se contempla

8. CANCELACIÓN DE LA SUSPENSIÓN

No se contempla

9. RENOVACIÓN DE CERTIFICADOS

No se contempla.

Se deberá realizar una nueva solicitud siguiendo el procedimiento establecido en este documento para la expedición de un muevo certificado electrónico.

[50] Esta comunicación se hará, para el firmante, a través de la dirección de correo electrónico aportada en el momento de la solicitud de expedición del certificado; y al solicitante de la revocación, a la dirección de correo electrónico aportada en el momento de la solicitud de la revocación.

ANEXO I. POSIBLES ESCENARIOS EXISTENTES EN EL PROCESO DE REVOCACIÓN DE CERTIFICADOS

Escenario I

- Un solo certificado activo perteneciente a la AC AP o a la AC Sector Público
- Se revoca el certificado expedido por la AC AP o AC Sector Público

- Se revoca el certificado activo correspondiente.
- Borra las identidades de firma vinculadas al certificado revocado.
- Anula las *Credenciales de identificación*.
- Deshabilita la *Cuenta de usuario*.

Escenario II

- Dos certificados activos pertenecientes a la AC AP y AC Sector Público.
- Se revoca un certificado expedido por la AC AP.

- **Mantiene** activo el certificado AC Sector Público.
- Se revoca el certificado activo perteneciente a la AC AP.
- Borra las identidades de firma vinculadas al certificado activo perteneciente a la AC AP.
- **NO** anula las *Credenciales de identificación*.
- **NO** deshabilita la *Cuenta de usuario*.
- **NO** genera nueva contraseña.

Escenario II

- Dos certificados activos pertenecientes a la AC AP y AC Sector Público.
- Se revoca un certificado expedido por la AC Sector Público.

- Se revoca el certificado activo perteneciente a la AC AP.
- Borra las identidades de firma vinculadas al certificado activo perteneciente a la AC AP.
- Se revoca el certificado activo perteneciente a la AC Sector Público.
- Borra las identidades de firma vinculadas al certificado activo perteneciente a la AC Sector Público.
- Anula las *Credenciales de identificación*.
- Deshabilita la *Cuenta de usuario*.