Despliegue del Certificado para el personal al servicio del Ministerio de Economía y Hacienda

Beatriz Vera Mateos

Jefa de área de Administración Electrónica

Carlos Arroyo García

Jefe de servicio - Administración Electrónica

Subdirección General de Tecnologías de Información y de las Comunicaciones

Subsecretaría

Ministerio de Economía y Hacienda

ÍNDICE

1 INTRODUCCIÓN

Desde el año 2000, las Administraciones Públicas españolas vienen realizando un esfuerzo importante en el desarrollo de su administración electrónica habiendo recibido un impulso adicional en los últimos tres años, merced a diferentes planes del Gobierno y a la aprobación de la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos (LAECSP).

La aprobación y publicación de esta Ley ha focalizado la atención en la forma en que se puede acceder a los servicios públicos, en el uso que se hace de las tecnologías de la información y comunicación en las Administraciones y en la incidencia que estas tecnologías pueden tener para facilitar las relaciones con los ciudadanos.

Aunque el impulso dado en los últimos años al desarrollo de la administración electrónica en España ha sido intenso – como ha quedado resaltado en el último estudio de la Comisión Europea sobre acceso electrónico a los servicio públicos, que sitúa a España en el 9º lugar de los 31 países analizados -, las exigencias de la Ley requieren de un esfuerzo adicional para garantizar su cumplimiento íntegro antes de finales del año 2009. Este plan, así como el marco estratégico en el que se inscribe, desarrollan las previsiones de la Ley y garantiza la actuación coordinada y eficaz de todos los organismos de la Administración General del Estado para dar cumplimiento a la Ley.

Para realizar el despliegue de una Infraestructura de clave pública en el Ministerio de Economía y Hacienda, se ha definido el siguiente procedimiento, teniendo en cuenta la siguiente documentación como base.

- Instrucción de 6 de Julio de 2009, de la subsecretaría del departamento, sobre el establecimiento de una PKI corporativa en el ámbito del Ministerio de Economía y Hacienda.
- Políticas y prácticas de certificación particulares aplicables a los servicios de certificación y firma electrónica en el ámbito de la organización y funcionamiento de las AAPP, sus organismos y entidades vinculadas y dependientes. FNMT-RCM. Versión 1-0. (DPC APE)
- Declaración de prácticas de certificación. FNMT-RCM. Versión 2.5. 3 Julio (DPC General)
- Documento de Despliegue de la PKI corporativa del MEH, de la Intervención.
- Especificación de la gestión de certificados de la PKI. Versión 1.00.
- Implantación de Oficinas de Registro para la Gestión de Certificados emitidos por la FNMT-RCM bajo la denominación de certificados para la Administración Pública Española Procedimiento de Registro v1.0.

Para poder iniciar el Despliegue se han tenido en cuenta los siguientes puntos:

- Solicitud de tarjetas nuevas para aquellas personas que no tengan el PIN/PUK de la tarjeta. Ya que el tiempo invertido en descubrir quién tiene PIN/PUK podría hacer fracasar el proyecto.
- El certificado no incluirá los datos del puesto de trabajo u organismo de dependencia.

2 CERTIFICADO PARA EL PERSONAL AL SERVICIO DE LAS ADMINISTRACIONES PÚBLICAS

El Certificado para el personal al servicio de las AAPP, es la certificación electrónica emitida por la FNMT-RCM que vincula a su Titular con unos Datos de verificación de Firma y confirma, de forma conjunta:

- la identidad del firmante y custodio de claves (empleado del MEH).
- el Titular del Certificado (MEH)

Se considera personal al servicio de las AAPP:

- Funcionarios.
- Personal Laboral.
- Personal estatutario a su servicio.
- Personal autorizado.

En nuestro caso, son partes interesadas:

- El Ministerio de Economía de Hacienda que dependiendo de la Ley de Emisión (si la hubiere) deberá conformarse como Titular responsable.
- Las Oficinas de Registro, que, a través del personal designado por Oficialía Mayor, serán responsables de los requisitos y condiciones que ostenten los Titulares y firmantes/custodios del Certificado.
- Oficialía Mayor como Responsable de Operaciones de Registro.
- Los firmantes y custodios del Certificado y sus Claves, que será el personal al servicio del MEH.
- FNMT-RCM, en cuanto Prestador de Servicios de Certificación.
- En su caso, resto de la Comunidad Electrónica y terceros.

Este certificado es distinto del previsto para identidad de persona física, con independencia de los aspectos comunes y coincidentes. De hecho, NO se podrá emplear este tipo de Certificados, por persona o entidad distinta a la FNMT-RCM, para:

- Firmar otro Certificado, salvo supuestos expresamente autorizados previamente.
- Usos particulares o privados.
- Firmar software o componentes.
- Generar sellos de tiempo para procedimientos de Fechado Electrónico.
- Prestar servicios a título gratuito u oneroso, salvo supuesto expresamente autorizados previamente, como:
    - Prestar Servicios de OCSP.
    - Generar Listas de Revocación.
    - Prestar servicios de notificación

3 DATOS PERSONALES EN MEDUSA PARA GESTIONAR LA PKI

El personal que se encuentra presentando sus servicios en el Ministerio está dado de alta en una Base de Datos de personal única, MEDUSA (Modelo Estructurado de Datos Unificados para Servicios de Acceso):

- ya sea de forma automática a través de BADARAL, o NEDAES en el caso de Altos Cargos y personal eventual.

- manualmente, a través de la aplicación de MEDUSA correspondiente de alta de personal, en el caso de Personal Externo.

Se utiliza la aplicación de MEDUSA de Alta provisional de Funcionarios, a la que solo tiene acceso el personal de Seguridad del Ministerio, para tomar los datos (DNI, Apellidos, Nombre y Unidad) de funcionarios o laborales, datos que se utilizarán durante los días que pasan entre la toma de posesión y la llegada de sus datos en BADARAL.

Cada Unidad Gestora de Mi Ficha, que gestiona al personal de su ámbito, deberá dar de alta al personal externo de su ámbito, mediante el correspondiente módulo de MEDUSA (Personal Externo).

Existe la situación excepcional de funcionarios con nombramiento en otros Ministerios que prestan servicios en el MEH (p.e. Servicio Jurídico). Sus datos deben ser dados de alta por el módulo de PERSONAL EXTERNO, diferenciándose por pertenecer a un tipo de familia distinto que el Personal Externo para poder tener localizados a todas las personas de esta naturaleza.

En este contexto, los empleados en situación de alta existentes en MEDUSA, serán la base para planificar el despliegue de los certificados para el personal al serivico de las AAPP. Será el superior jerárquico de la persona externa, quien debe solicitar un certificado, al pedir la tarjeta.

Además de los datos recogidos anteriormente, son imprescindibles los datos correspondientes a su ubicación, dirección de correo electrónico o teléfono, para poder hacer automáticamente comunicaciones al personal (p.e. citaciones para carga del certificado, avisos de caducidad de certificado, etc.).

También el sistema recoge de forma automática cuando una persona cursa una baja en el MEH, de manera que se pueda saber cuándo hay que revocar el certificado correspondiente. Los datos de personal Funcionario y Laboral, no aparecen en BADARAL, y mensualmente se comprueban en NEDAES, que tiene el correspondiente dato de baja en nómina. Por parte del personal Externo, se tiene la fecha de 'fin de la colaboración'.

En cualquier caso, existe un mecanismo que avisa al Registrador de las próximas revocaciones/caducidades pendientes.

4 PROCESO DE SOLICITUD DE LA TARJETA

La FNMT-RCM proporciona al MEH, para su entrega al personal del su dependencia, Tarjetas criptográficas (Dispositivos Seguros de Creación de Firma) para la generación de sus Claves Privadas y el almacenamiento de los Certificados. Ya que la FNMT-RCM, bajo ningún concepto, genera ni almacena las Claves Privadas de sus Titulares, las cuales son generadas bajo su exclusivo control, y cuya custodia está bajo la responsabilidad de los diferentes firmantes, órganos, organismos y entidades a las que se encuentren vinculadas o de las que dependan.

Dicha tarjeta es entregada a los Usuarios y AAPP titulares sin ningún tipo de contenido, con las utilidades software necesarias para conseguir una integración con los Navegadores más usados. También se le proporcionan los códigos necesarios para el acceso a dicha tarjeta, Códigos que posteriormente desde el puesto de la propia Oficina de Registro, permitirán al usuario generar sus Claves e insertar el Certificado en la Tarjeta Criptográfica.

Como ya se ha mencionado con anterioridad, se pedirán Tarjetas Criptográficas nuevas, tanto para el personal que ya se encuentra prestando sus servicios en el MEH y no tiene PIN/PUK, como para el personal nuevo, el resto del personal usará la tarjeta que dispone actualmente.

El proceso será el siguiente:

- El personal que ya se encuentre prestando sus servicios en el Ministerio. Se personará, según le cite el registrador correspondiente, en la Oficina de Registro con la tarjeta. En caso de que no tenga el PIN necesario, la aplicación permitirá al registrador solicitar una nueva tarjeta para esa persona. Esa solicitud llegará a la Oficina de Seguridad, quién seguirá siendo punto único de contacto con la FNMT para el envío de los ficheros correspondiente y la recepción de las tarjetas.

- Para el personal recién incorporado, se solicitará una tarjeta nueva de la misma forma que se hace actualmente a través de las Unidades Gestoras de las Tarjetas definidas para este fin.

Habrá tantas Oficinas de Registro como sean necesarias, y en cada una de ellas habrá dos o tres Registradores.

En Madrid, por ejemplo, hay una Oficina de Registro en cada Edificio que albergue un considerable número de empleados. En cada provincia, hay al menos una Oficina Registro.

5 PROCEDIMIENTO DE OBTENCION DEL CERTIFICADO

En las Oficinas de Registro, el personal designado por el Organismo correspondiente realizará los trámites necesarios para facilitar al personal adscrito su certificado personal en la Tarjeta Criptográfica.

Todos los trámites que se detallan a continuación para la Obtención del Certificado se han de realizar en una misma citación en la Oficina de Registro, en el caso que ocurra cualquier problema durante el Procedimiento se volverá a comenzar desde el Principio

Además, para garantizar la confidencialidad de todo el proceso, el proceso se realizará desde dos terminales diferenciados. Uno para la persona que solicita el certificado, y otro para el Registrador.

5.1 Citación.

El registrador, a través, de la Aplicación le permitirá gestionar la Citación de la/s personas a las que va a realizar el proceso de obtención del Certificado.

Podrá seleccionar tanto el día como el medio de comunicación con el Empleado para el aviso, por lo que si se selecciona vía correo, le enviará un correo electrónico con los detalles de la citación.

5.2 Verificación de la Identidad.

Una vez que el empleado público se persona en la Oficina de Registro se ha de proceder a la verificación de la identidad del mismo, presentando el D.N.I. El Registrador introducirá el número en la Aplicación y mostrará la información del mismo, incluida los datos de la tarjeta que posee. En el mismo acto presentará la tarjeta Criptográfica para verificar el número con la tarjeta activa que muestra el sistema.

Si el D.N.I. corresponde al Empleado y la tarjeta que tiene es la misma que muestra el sistema como activa, está en disposición de iniciar el proceso de obtención del Certificado.

5.3 Solicitud.

El solicitante directamente o a través, de la persona de la Oficina de Registro, realiza la solicitud del Certificado introduciendo su NIF.

- En el proceso de envío de la solicitud, se generará el par de claves correspondientes, pública y privada, junto a la solicitud y de forma transparente para el solicitante (la Clave Pública firmada con su clave Privada).
- La FNMT generará un Código de Solicitud que será imprescindible para posteriormente realizar la Descarga.

https://ape.cert.fnmt.es/appsUsuario/solicitudmeh/solicitudCertInicio.do

5.4 Registro en la FNMT.

Una vez verificada la identidad del solicitante del Certificado, así como su condición de Personal de la Administración Pública se accederá a registrar la solicitud en la FNMT cumplimentado y firmando el formulario por parte del Registrador.

Una vez realizado el proceso y firmado por el Registrador se imprimirán tres copias del contrato, una para la Oficina de Registro, otra para la FNMT-RCM y la tercera para el interesado que serán firmadas por el solicitante y el Registrador.

https://registro.cert.fnmt.es/appRegistro/frameset1.html

5.5 Descarga de los Certificados.

Una vez que el certificado haya sido generado por la FNMT, tanto el solicitante como el registrador podrán realizar la descarga del mismo en la tarjeta criptográfica del empleado introduciendo el NIF y el Código de Solicitud generado en la solicitud.

El Certificado tiene una validez de 4 años contados a partir del momento de la emisión del Certificado.

http://ape.cert.fnmt.es/appsUsuario/descargameh/descargaCertInicio.jsp

5.6 Comprobación del estado del Certificado.

Una vez que el Certificado se ha descargado en la tarjeta criptográfica del empleado se podrá comprobar el estado mediante la opción que posibilita la Aplicación de Chequear que accede directamente a la FNMT.

https://apuseg.cert.fnmt.es/ChequearCerts/ChequearCert

6 IMPLANTACIÓN DE OFICINAS DE REGISTRO

La gestión de certificados emitidos por la FNMT – RCM, obtención, suspensión o revocación, supone la realización de determinadas tareas, las cuales han de ser realizadas por personas autorizadas, los Registradores, y llevadas a cabo en puestos de trabajo con determinadas garantías de seguridad, Oficinas de Registro.

Todo este proceso previo requiere, por parte de la FNMT – RCM, habilitar tanto a las Oficinas de Registro como a los Registradores, de forma que las operaciones de registro se realicen con toda seguridad y de acuerdo a los procedimientos establecidos.

6.1 Responsable de las Operaciones de Registro.

La actividad de registro, supone la apertura de Oficinas de Registro, alta de puestos de registro, nombramiento de Registradores, otorgamiento de los perfiles y políticas de registro, etc., así como la realización de diferentes tareas administrativas. Todas estas acciones han de realizarse bajo la responsabilidad de una persona, el Responsable de las Operaciones del Registro, con autorización del Organismo encargado de estas operaciones.

Es el interlocutor único con la FNMT-RCM para aquellos asuntos relacionados con la actividad del Registro.

Funciones:

- Responsable del buen funcionamiento de las Oficinas de Registro
- Envío y recepción de la documentación relativa a las Oficinas de Registro
- Envío y recepción de la documentación relativa a los Puestos de Registro
- Envío y recepción de la documentación necesaria para la gestión de Registradores.

Los datos necesarios y la autorización pertinente, se recogerán en un impreso específico.

Por otro lado, el Organismo se compromete a que en el momento en que la persona previamente nombrada como responsable de las actividades de Registro cese en estas funciones, será comunicado a la FNMT – RCM.

6.2 Oficinas de Registro.

Las Oficinas de Registro son los lugares físicos donde se va a desarrollar la actividad de registro. Se podrán tener tantas Oficinas de Registro como se estime oportuno.

En cada una de estas oficinas, existirán Puestos de Registro atendidos por Registradores en el número que se determine.

Además, cada una de estas oficinas podrá tener un responsable que se haga cargo de la actividad que en ella se realice. Habrá que decidir si esta persona es el Responsable de Operaciones de Registro del Organismo para todas las Oficinas, o bien nombra a otra/s persona/s distintas para cada una de ellas, grupos de oficinas, etc.

Con el fin de dar de alta a las distintas Oficinas de Registro, la FNMT – RCM, deberá recibir una comunicación del Responsable de Operaciones de Registro,

indicando la relación de oficinas a crear, su denominación y la dirección postal completa de cada una de ellas.

6.3 Puestos de Registro

Los Puestos de Registro son espacios atendidos por Registradores desde donde se podrá realizar cualquier actividad relacionada con el registro de certificados. Como ya se ha comentado, en el MEH se ha optado por incluir dos terminales por cada puesto, para agilizar el tiempo de obtención del Certificado y aumentar la seguridad de que se realiza la descarga en la tarjeta criptográfica del empleado que solicita el certificado.

Terminal 1, para el empleado que descarga el certificado, que se utilizará para realizar las operaciones de:

Solicitud de Certificado
Descarga de Certificado
Chequear Certificado
Carga de Datos en MEDUSA

Terminal 2, para el registrador, que se utilizará para realizar las operaciones de:

Citación
Verificación de la Identidad
Registro en la FNMT

Cada Puesto de Registro, podrá ser atendido por uno o varios Registradores

Las necesidades de Hardware y Software para cada uno de estos Puestos de Registro, debido a la evolución de la tecnología, serán las que determine la FNMT – RCM en cada momento, Será necesario una maquina (PC) con:

- Lector de Tarjetas PC/SC.
- Conexión a Internet.
- Conexión directa o mediante red local a impresora correctamente configurada.
- Impresora
- Tarjeta criptográfica con certificado de FNMT Clase 2 CA.

En este caso, para dar de alta los Puestos de Registro será necesario, que el Responsable de Operaciones de Registro, comunique a la FNMT – RCM, la relación del número de Puestos de Registro por Oficina de Registro, además de los Registradores asociados a cada uno de ellos.

Por otro lado, y con la finalidad de evitar que se pueda acceder a la aplicación de registro desde localizaciones no autorizadas, se deberá comunicar a la FNMT - RCM las **direcciones IP** o rangos de direcciones IP de todos los Puestos de Registro que se quieran implantar.

6.4 GESTION DE REGISTRADORES

Todas aquellas personas que vayan a ejercer como Registrador, deberán estar dadas de alta previamente en el sistema interno de la FNMT – RCM y estar en

posesión de un certificado de Persona Física emitido por la FNMT-RCM bajo la denominación de Certificado FNMT Clase 2 CA

Para llevar a cabo el alta de Registradores, la persona Responsable de las Operaciones de Registro, deberá remitir, a la FNMT-RCM, la relación de personas a dar de alta como Registradores. Esta relación se realizará en impreso específico, debidamente cumplimentado y firmado.

Igualmente en el momento de la baja, la persona Responsable de las Operaciones de Registro, deberá remitir al Área y Departamento de la FNMT-RCM correspondiente, relación de personas que causarán baja como Registradores. Esta relación se realizará en impreso específico.