

- registro de usuarios
- emisión, revocación y archivo de certificados de clave pública
- publicación de certificados y del Registro de Certificados
- registro de eventos significativos

## GENERACIÓN Y GESTIÓN DE CLAVES

### Generación y gestión de las claves

En el procedimiento de obtención de certificados, la FNMT-RCM desarrollará los elementos necesarios para activar, en el puesto del solicitante, el software que genere a través de su navegador web, un par de claves, pública y privada, que le permitirá firmar e identificarse, así como proteger la seguridad de sus comunicaciones a través de mecanismos de cifrado.

Las claves privadas serán utilizadas bajo el control del software de navegación web del que disponga el propio usuario, enviando todas las claves públicas a la FNMT-RCM con el fin de integrarlas en un certificado.

Las claves privadas de firma, permanecerán siempre bajo el control exclusivo de su titular, y guardadas en el soporte correspondiente, no guardándose copia de ellas por la FNMT-RCM.

La FNMT-RCM garantizará que el usuario, Titular del certificado, puede tener el control exclusivo de las claves privadas correspondientes a las claves públicas que se consignan en el certificado, mediante la obtención de las pruebas de posesión oportunas, a través de la adjudicación del número de identificación único.

### Archivo de las claves públicas

Las claves públicas de los usuarios permanecerán archivadas, por si fuera necesario su recuperación, en archivos seguros, tanto física como lógicamente, durante un periodo no menor de 15 años.

### Exclusividad de las claves.

Las claves privadas son exclusivas para los Titulares de los certificados y son de uso personal e intransferible.

Las claves públicas son exclusivas para los Titulares de los certificados, independientemente del soporte físico donde estén almacenadas y protegidas.

### Renovación de claves.

La FNMT-RCM identifica una relación uno a uno entre la clave pública de un usuario y su certificado de clave pública, no previéndose utilizar distintos certificados para una misma clave. Es por esto que las claves se renovarán con los certificados cuando dicha renovación esté contemplada en la normativa específica aplicable.

## REGISTRO DE USUARIOS

### Registro de usuarios.

El registro de usuarios es el procedimiento a través del cual se identifica al solicitante de un certificado electrónico, se comprueba su personalidad y se constata su efectiva voluntad de que le sea emitido el "Certificado Básico" o "Título de Usuario" por la FNMT-RCM.

Este registro podrá ser realizado por la propia FNMT-RCM o cualquier otra Administración pública y, en su caso, por las demás personas, entidades o corporaciones habilitadas a tal efecto por las normas que resulten de aplicación. En todo caso el registro se llevará a cabo según lo dispuesto por la FNMT-RCM, al objeto de que este registro se realice de acuerdo con lo establecido por la normativa específica aplicable y homogéneo en todos los casos. De igual manera será la FNMT-RCM, quien defina y aporte los medios necesarios para la realización de este registro.

En el caso de que el registro lo realizara una Administración Pública, distinta de la FNMT-RCM, la persona que se encargue de la actividad de registro ha de ser personal al servicio de la Administración Pública. En estos casos la FNMT-RCM, dará soporte a la implantación de las distintas oficinas de registro que se establezcan cuando fuere necesario, en los siguientes términos:

- Aportación de la aplicación informática de registro
- Aportación de la documentación relativa a la instalación y manejo de la aplicación, así como toda aquella referente a los procedimientos y normas sobre el registro.
- Registro y formación de los encargados del registro, lo que supone la emisión de un certificado emitido por la FNMT-RCM para cada encargado del registro, que permita garantizar la seguridad de