

procedimientos seguidos hasta la fecha de la actualización por los titulares.

La FNMT notificará a los titulares con 2 meses de antelación las actualizaciones que pudieran causar modificaciones en los procedimientos de acceso a la dirección o de consulta del contenido depositado.

Precio del servicio.

El servicio de dirección electrónica será inicialmente, gratuito para sus titulares, ya sean estos particulares o empresas. La modificación de las presentes condiciones será comunicada a sus titulares, al menos con 12 meses de antelación a su entrada en vigor.

Prácticas del servicio.

La declaración detallada de prácticas del servicio se publicará en la dirección electrónica de la FNMT y podrá ser variada sin previo aviso. La variación no limitará el servicio.

Servicio de fechado digital.

El fechado digital es un método para probar que un conjunto de datos (datum) existió antes de un momento dado y además que ningún bit de estos datos ha sido modificado desde entonces.

Además, el fechado digital proporciona un valor añadido a la utilización de firma digital ya que ésta por sí sola no proporciona ninguna información acerca del momento de creación de la firma. Los certificados digitales utilizados por el algoritmo de la firma digital tienen un periodo de validez y por lo tanto, la firma sin el fechado digital, pasada la validez del certificado, siempre puede ser repudiada.

Para asociar los datos con un específico momento de tiempo es necesario utilizar una Autoridad de Fechado (TSA - Time Stamp Authority) como tercera parte de confianza. La definición del servicio del Fechado Digital está basada en las especificaciones del estándar RFC3161 - "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". A continuación se describen brevemente algunos de los puntos del mencionado estándar que tienen mayor impacto en la definición de la solución final del servicio.

Estándares aplicables.

El estándar RFC3161 define entre otros, el formato de la solicitud de un fechado digital y de la respuesta generada por la TSA. También establece los diferentes

requerimientos de seguridad que debería cumplir una TSA.

Uno de estos requerimientos, es que todos los fechados digitales generados por la TSA deberían estar firmados digitalmente por ella con la clave privada de un certificado digital válido emitido especialmente para este propósito.

Por otro lado el mencionado estándar especifica que los fechados digitales (tokens) generados por la TSA no pueden incluir ninguna identificación del cliente que ha solicitado la operación. Como consecuencia, no es necesario que los mensajes de solicitud de fechado digital que recibe la TSA contengan algún tipo de autenticación del cliente.

En casos especiales, la TSA necesita autenticar la procedencia de las solicitudes, el mencionado estándar recomienda para ello utilizar algún método alternativo, no especificado en RFC3161. El protocolo de fechado digital de la FNMT-RCM hace uso de autenticación basada en firma según Cryptographic Message Syntax (RFC 2630).

El estándar enumera diferentes mecanismos de transporte para mensajes de TSA. Ninguno de estos métodos es mandatorio; todos ellos son opcionales e incluso se contempla la posibilidad de soportar en un futuro nuevos mecanismos. Los mecanismos que se especifican el documento RFC3161 son:

- Protocolo utilizando correo electrónico
- Protocolo basado en la utilización de FTP
- Protocolo basado en sockets utilizando el puerto IP 318
- Protocolo vía http

También hay que recalcar que el estándar solamente define la operación de solicitud de fechado digital y de la respuesta correspondiente, dejando otros tipos de operaciones, como por ejemplo la validación del fechado, sin ninguna especificación, aunque se deba realizar la implementación de este tipo de operaciones.

La aplicación de Notificación y la aplicación de custodia hacen uso del protocolo basado en sockets utilizando el puerto 318. Los mensajes de servicio tienen la siguiente estructura: