

notificadotes de un sistema de no repudio en destino.

Las notificaciones practicadas serán selladas y custodiadas electrónicamente. Las especificaciones del servicio de sellado de tiempo son las que se recogen en este mismo anexo y están basadas en las especificaciones del estándar RFC3161 - "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". Las especificaciones del servicio de custodia son las que se recogen en este mismo anexo.

El servicio de notificación electrónica se podrá complementar adicionalmente con un servicio de notificación tradicional para completar una solución de correo mixto.

Acceso al servicio.

El servicio será accesible a través de Internet por el cliente siempre que esté dado de alta en el sistema y esté en posesión de un certificado de verificación de firma electrónica emitido por la Fábrica Nacional de Moneda y Timbre, válido y no revocado así como de su correspondiente clave privada, lo que le permitirá identificarse mediante el uso de firma electrónica.

Las especificaciones de los certificados de verificación de firma electrónica son las que se recogen en el Capítulo I de este mismo anexo y están basadas en un certificado reconocido según la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 9594-8 de 1997) de acuerdo con lo previsto en la legislación de firma electrónica.

El acceso a los servicios contará con las debidas medidas de confidencialidad de modo que solo los clientes sean capaces de practicar notificaciones a las direcciones electrónicas. Dichas medidas de confidencialidad podrán al menos cifrar la información mediante el uso de alguno de los protocolos de comunicación estándares SSL, TLS, AES o similares, con una clave simétrica de intercambio de datos de al menos 128 bits mediante el uso de los algoritmos de cifrado mas habituales.

La solicitud de acceso a los servicios se realizará por medios electrónicos y mediante firma electrónica. La FNMT guardará la firma generada así como la prueba sellada de tiempo que permita confirmar la identidad del cliente así como su solicitud y el momento de la realización. De igual manera, la solicitud de baja en el servicio se realizará mediante

los mismos procedimientos de firma y sellado de tiempo.

La FNMT guardará prueba firmada y con sello de tiempo de cada notificación practicada y pondrá dicha información a disposición del notificador, del notificado así como de las autoridades competentes de acuerdo a la legislación aplicable.

La FNMT, como prestador del servicio y a los únicos efectos de dar fe de lo acontecido, tendrá un acceso limitado a las notificaciones practicadas. Dicho acceso limitado no permitirá en ningún caso, a ningún empleado o colaborador externo de la FNMT, a título individual, el acceso a las notificaciones. El procedimiento de acceso se regulará en los procedimientos de seguridad internos y estará basado en un sistema de concurrencia de al menos 4 personas, con carácter ejecutivo dentro de la FNMT. Todo acceso será anotado en un libro de control de accesos donde se hará constar al menos, la fecha, la hora, el motivo justificado del acceso así como los intervinientes y su cualificación.

Práctica de notificaciones

Una Entidad Cliente podrá solicitar el servicio de Notificación para enviar a los ciudadanos una información determinada, la cual quedará depositada en la dirección electrónica única (DEU) de estos. Esta notificación puede ser el envío de un fichero, de un texto o ambos (fichero y texto).

A continuación se presenta el flujo de datos correspondiente a esta operación:

- El cliente solicita el servicio de Notificación enviando el mensaje requestNotificacion
- El servicio de Notificación realiza la autenticación y autorización de la solicitud.
- Gestor Transaccional almacena el documento en la base de datos, quedando éste bajo custodia hasta la fecha de expiración de la custodia.
- Gestor Transaccional genera y envía al cliente el mensaje de respuesta returnNotificacion.
- Gestor Transaccional genera y envía el mensaje de correo electrónico con la notificación. Adicionalmente y de manera opcional puede mandar un mensaje a diversos destinatarios informando de que la notificación se ha llevado a cabo.