SISTEMA DE NOTARÍA DIGITAL: CERTIFICACIÓN, SELLADO EN EL TIEMPO Y VALIDACIÓN DE DOCUMENTOS DIGITALES

Mariví Higuero, Igor Pérez, Alejandro Muñoz, Luis Zabala, Juanjo Unzilla

Grupo de Ingeniería Telemática. Departamento de Electrónica y Telecomunicaciones
Universidad del País Vasco / Euskal Herriko Unibertsitatea
jtphiapm@bi.ehu.es, jtbcoora@aintel.bi.ehu.es, {jtpmumaa, jtpzaall, jtpungaj}@biehu.es

ABSTRACT

Nowadays digital records are the heart of every business. From e-commerce transactions with customers and suppliers to the accumulated intellectual property of R&D departments, a business depends on the integrity of its corporate data. This paper shows the design and implementation of a digital notary system. This system enables any client to notarize electronic files and records before its distribution, guaranteeing file content and enabling the customer to verify that content for years to come. It provides corporations and professionals with an easy to use, irrefutable way of verifying that electronic files and records were created when claimed and not altered since then.

1. INTRODUCCIÓN

Uno de los mayores inconvenientes que tiene la información digital se encuentra en su "volatilidad". Con la misma facilidad que puede ser tratada, procesada o transmitida, puede ser copiada, borrada y modificada de forma no autorizada. Si se pretende que esos datos sean reconocidos como válidos ante una entidad jurídica, se acaba recurriendo a métodos de notaría tradicional, en la mayoría de los casos muy costosos. Una solución a estos problemas la constituyen los servicios de notaría digital, un servicio que permita probar en cualquier momento, de una manera irrefutable matemáticamente, que en determinada referencia temporal unos documentos en formato electrónico existían y que no han sido modificados desde entonces.

2. OBJETIVO

El objetivo principal de este sistema consiste en ofrecer un sistema de Notaría Digital [1],[2] que permita almacenar cualquier tipo de archivo o registro digital de forma permanente y segura, certificando la fecha en que fue almacenado y su propietario. A su vez, este sistema ofrece a los usuarios la posibilidad de validar dicho registro en cualquier instante de tiempo posterior a la certificación, y de probar ante terceros que el archivo, que en su momento fue certificado, sigue siendo válido, es decir, no ha sufrido modificaciones.

3. ARQUITECTURA DEL SISTEMA

La arquitectura propuesta se muestra en la figura 1 y se basa en un modelo Cliente/Servidor que consta de los siguientes módulos:

3.1. Módulo Cliente

Se encarga de realizar las peticiones de certificación y validación a los correspondientes módulos del servidor. El cliente desde su navegador, podrá realizar dos acciones: a) mandar certificar un documento y, una vez certificado, b) comprobar la validez de dicha certificación.

3.2. Módulo Servidor de Certificación

Ante una petición de certificación del cliente, en primer lugar almacena el archivo que debe certificar, en un sistema de almacenamiento seguro. A continuación, aplica una función hash sobre el archivo y procede a certificarla [3]. Para ello accede al módulo de registro de datos, y toma el valor Hash Raíz (H.R.) de la última certificación. Concatena este valor H.R. con el valor hash resultante del archivo que vamos a certificar y calcula de nuevo el valor hash de esa concatenación; éste será el valor H.R. de esta nueva certificación que será utilizado en la concatenación de la siguiente. De esta forma, construimos una cadena de valores H.R., en la que cada valor resultante de una nueva certificación depende de todos los valores Hash Raíz de todas las certificaciones anteriores. Debido a las características de las funciones Hash, cualquier intento de suplantación o modificación de un archivo digital es detectado en el proceso de validación. Esta técnica garantiza la integridad y la imposibilidad de modificación del registro global de las certificaciones realizadas.

3.3. Módulo Servidor de Validación

Este módulo es el encargado de atender las peticiones de validación del cliente. Realiza el mismo proceso que el módulo de certificación comprobando que el documento que se pretende validar genera un H.R. idéntico al almacenado en la cadena de certificaciones en el momento de la certificación del original. Si cumple con la integridad del sistema, ese documento es válido y por tanto se informará al cliente de su validez y de su fecha de certificación, mediante el envío de un certificado firmado por la propia notaría digital. Este certificado podrá ser usado ante terceros como prueba de que un determinado archivo fue certificado en una fecha concreta y por un usuario determinado.

3.4. Módulo de Registro de Datos

Es el encargado de almacenar los datos necesarios para garantizar la integridad del sistema. Utiliza un sistema gestor de bases de datos MySQL [4], en el que se almacena para cada operación de

certificación un número de identificación de operación, otro de cliente, la fecha en la que se certifica (sello de tiempo), el valor hash del archivo que se certifica, y el valor H.R. de esa certificación. También guarda datos del estado de la propia base de datos, de los clientes y de los archivos almacenados.

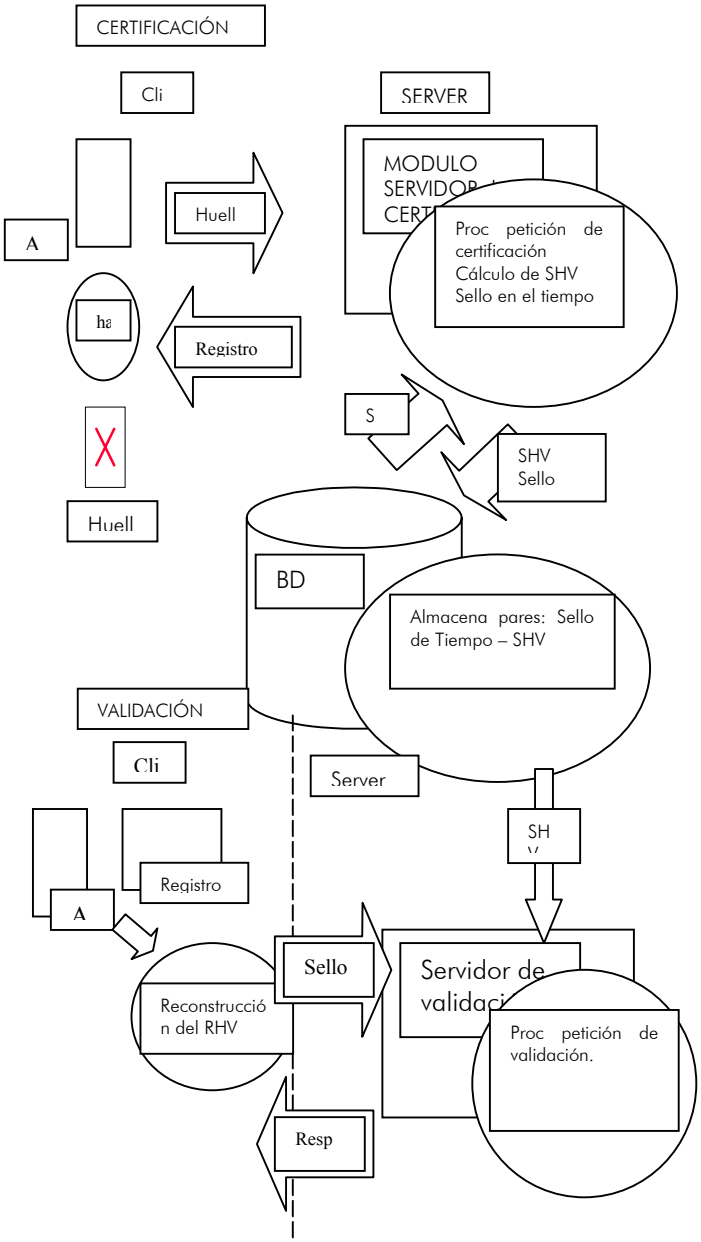

Figura 1: Arquitectura del sistema y esquema de operación.

3.5. Módulo de Almacenamiento

Recibe las peticiones tanto de almacenamiento como de recuperación de documentos digitales realizadas por los módulos de certificación y validación respectivamente. Su principal función es la de garantizar el correcto almacenamiento de todos los documentos digitales certificados en los sistemas de almacenamiento dedicados. Realiza todas las funciones de redundancia y de supervisión en las operaciones de almacenamiento que evitan cualquier posible error o mal funcionamiento de bajo nivel. Garantiza la integridad permanente de los datos mediante mecanismos de copias de seguridad y chequeos periódicos de consistencia entre copias. Asimismo, garantiza que un documento que ya ha sido almacenado no pueda ser modificado ni borrado. Para ello, dispone de funciones específicas para detectar y evitar cualquier intento de modificación o escritura sobre documentos ya almacenados, permitiendo únicamente almacenar nuevos documentos.

3.6. Módulo de Replicación

Este módulo se encarga de realizar copias de seguridad tanto del módulo de almacenamiento como de la base de datos del módulo de registro de datos. Permite mantener copias exactas de todo el sistema de notaría digital, incluso en servidores distribuidos, proporcionando mayores características de seguridad y garantizando la integridad total del sistema. [5]

4. APLICACIONES FUTURAS Y NUEVAS LÍNEAS DE DESARROLLO

Una vez implementado este sistema básico de notaría digital de documentos y, apoyándose en infraestructuras de clave pública (PKI), se está pensando en emplearlo como soporte para nuevos servicios, integrándolo con otros tipos de sistemas, como facturación electrónica, para la certificación de contratos, facturas, transacciones, sistemas de correo electrónico para la certificación de mensajes enviados y recibidos, etc.

5. CONCLUSIONES

Los sistemas de notaría digital pretenden convertirse en una seria alternativa a la notaría tradicional en medios electrónicos y en soporte fundamental para el surgimiento y generalización de nuevos servicios de comercio electrónico a través de Internet, pudiendo emplearse para la resolución de conflictos si se respetan las condiciones dispuestas por la legislación. Este servicio, además, pretende integrarse con las plataformas y escenarios habituales de un proveedor de servicios de Internet (ISP), ampliando su oferta de servicios al cliente, con soluciones tecnológicamente avanzadas.

6. REFERENCIAS

[1] Surety: Internet's Digital Notary and Timestamping Service, accesible en http://www.surety.com

[2] e-TimeStamp: Electronic Internet Notary, accesible en http://www.e-timestamp.com

[3] Schneier, B., "Applied Criptography", John Wiley & Sons, octubre 1995.

[4] MySQL DBMS, accessible en http://www.mysql.com

[5] Buretta, M., "Data Replication: Tools and Techniques for Managing Distributed Information", John Wiley & Sons, febrero 1997.