Firma digital avanzada de documentos jurídicos en actividades registrales

Advanced digital signature of legal documents in registered activities

Alexei Zubizarreta Pérez

Universidad de las Ciencias informáticas (UCI)

azubizarreta@uci.cu

Resumen

Se presenta una solución de firma digital avanzada para los documentos jurídicos en actividades registrales. Esta se integra con una Infraestructura de Llaves Públicas (PKI), otorgándole autenticidad, integridad, y no repudio a los documentos electrónicos haciendo uso de tarjetas inteligentes, garantizando seguridad jurídica en las transacciones. La solución se basa en dos partes fundamentales, la primera es la gestión de los certificados y la segunda es la firma digital de los documentos en el flujo registral. Los certificados digitales son generados en una Autoridad de Certificación y almacenados en tarjetas inteligentes, las cuales se entregan personalmente a los registradores (máxima autoridad en una oficina registral). Los usuarios podrán inscribir sus documentos y estos serán firmados digitalmente a través de un componente de software usando la tarjeta inteligente del registrador, luego son archivados y publicados. Actualmente la solución se encuentra funcionando en los Registros Mercantiles y Públicos de la República Bolivariana de Venezuela.

Palabras Clave: Firma Digital Avanzada, Firma Digital de Documentos, Certificado Digital, Infraestructura de Llaves Públicas.

Abstract

A solution of advanced digital signature for legal documents in registry activities is presented. This it is integrated with an Infrastructure of Public Keys (PKI), offering authenticity, integrity, and not repudiation to the electronic documents using smart cards, guaranteeing legal security in the transactions. The solution is based on two fundamental parts, the first one is the management of the certificates and the second is the digital signature of the documents in the registry work flow. The digital certificates are generated in an Certificate Authority and stored in smart cards, which they are delivered personally to the registries (maximum authority in registry office). The users will be able to record their documents and these they will be signed digitally through a software component using the smart card of the registry, then they are filed and published. The solution is currently found in production in the Trade and Public Registries of the Republic Bolivariana of Venezuela.

Key words*: Advanced Digital Signature, Documents Digital Signature, Digital Certificate, Public Key Infrastructure.*

Introducción

Con el crecimiento de las Tecnologías de la información y las Comunicaciones (TICs), la sociedad se ha ido involucrando cada vez más en las transacciones en la red. Esto ha permitido que muchos Estados se acerquen a los ciudadanos transformado sus relaciones, prestando mejores servicios, garantizando transparencia y celeridad en la gestión pública, mejorando la eficiencia y eficacia de los gobiernos.

La seguridad en las transacciones electrónicas de la administración pública es un aspecto de vital importancia, que permite a los ciudadanos confiar en el intercambio de información con el Gobierno. El empleo de la Firma Digital ha sido reconocido en muchos países, por su eficacia jurídica y valor probatorio.

Una **Firma Digital** es una firma electrónica que puede ser utilizada para autenticar la identidad del emisor de un mensaje o el firmante de un documento, y para asegurar que el contenido original del mensaje o el documento no ha sido alterado. La Firma

Digital no puede ser imitada por otra persona y puede tener un sello de tiempo el cual asegura que el mensaje firmado fue recibido y el emisor no puede repudiarlo más tarde.

La **Firma Digital Avanzada** es una Firma Digital creada mediante un dispositivo seguro de creación de firma, en este caso las tarjetas inteligentes, que es donde se encuentra almacenado el certificad digital con la llave privada.

Un **Certificado Digital** es un documento electrónico que permite vincular a una persona o entidad con su llave pública, este documento es emitido y firmado por un tercero confiable (Autoridad de Certificación). Sirve para garantizar la identidad de las partes involucradas en una transacción electrónica.

La **Tarjeta Inteligente (Smart Card)** es una tarjeta plástica con un microprocesador o "chip" empotrado que permite a la tarjeta almacenar información. En este caso almacena un certificado digital con la llave privada.

El **Sellado de Tiempo** permite la certificación de que una transacción electrónica ha ocurrido en una fecha y una hora determinada, en este caso, la firma digital de un documento.

Una **Autoridad de Certificación (AC)** es un organismo que se encarga de la emisión de certificados digitales, los cuales son solicitados por una Autoridad de Registro. Permite la identificación de un usuario mediante su certificado actuando como tercero confiable. Además tiene la responsabilidad de publicar las listas de revocación de certificados digitales (CRL).

La **Autoridad de Registro (AR)** tiene la función de gestionar el ciclo de vida del certificado, comunicándose de manera automatizada con la Autoridad de Certificación. Es quien registra las peticiones de certificados de los usuarios y las envía a la AC para que sean procesadas.

Se entiende por **Lista de Certificados Revocados (CRL)** una lista que contiene los números de serie de los certificados que han sido revocados por la Autoridad de Certificación. Estos certificados ya no son válidos y no pueden ser usados en transacciones electrónicas.

Infraestructura de Llaves Públicas (PKI): Infraestructura que permite mediante el uso de procedimientos criptográficos ofrecer servicios de encripción y de firmas digitales. Contiene directorios de certificados digitales, Autoridades de Certificación, Autoridades de Registro, mecanismos de publicación de Certificados y CRL.

Se define por **Llave Pública** la parte conocida del par de llaves de un certificado, esta es publicada en directorios de llaves públicas. Es usada para encriptar información y verificar la autenticidad de una firma digital.

Se define por **Llave Privada** la parte privada del par de llaves de un certificado, esta solo es conocida por el usuario propietario del certificado digital. Es usada para desencriptar y firmar información.

Después de haber sistematizado las principales definiciones y conceptos básicos que nos permiten tener una visión más clara de los temas de certificación electrónica, pretendemos en el presente artículo exponer uno de los resultados alcanzados por el proyecto de Registros y Notarías para la República Bolivariana de Venezuela, específicamente en el tema de Firmas Digitales en los Documentos Jurídicos dentro del proceso de modernización y automatización de las actividades registrales.

En el marco de cooperación Alba entre Cuba y Venezuela se han puesto en curso varios proyectos para informatizar la sociedad venezolana en aras de dotar al gobierno de herramientas tecnológicas que le permitan mejorar la eficiencia y eficacia de los procesos internos y de vinculación con la sociedad. El proyecto de Registros y Notarías tiene como principal objetivo estandarizar la gestión de las oficinas de Registros y Notarías, para garantizar la certeza, confiabilidad y seguridad jurídica de los actos protocolizables de conformidad con las disposiciones legales que los regulan.

Dentro de la automatización de las actividades registrales aquí se presenta una solución de firma digital avanzada de documentos jurídicos. La misma se basa en tecnologías estándares de Infraestructuras de Llaves Públicas (PKI), garantizando la autenticidad del firmante, la integridad y el no repudio de los documentos electrónicos legales haciendo uso de tarjetas inteligentes.

Existen productos de firmas digitales para la gestión documental electrónica en el mercado internacional, estos productos están en manos de compañías que los comercializan a altos costos. La solución que se presenta es una alternativa a la inversión en dichos productos dentro del proyecto.

Metodología

Para el desarrollo de la solución se ha seguido la metodología siguiente:

1. Revisión bibliográfica y estudio del arte.
2. Diseño de la arquitectura de la solución.
3. Elección de las herramientas de desarrollo de aplicaciones.
4. Desarrollo de los componentes de la solución.
5. Implantación.

Revisión bibliográfica y estudio del arte

Se procedió a la revisión de la literatura especializada y estándares internacionales sobre la temática de firmas digitales con el objetivo de desarrollar una solución que cumpla con las necesidades actuales.

Para la generación de la firma digital de los documentos se utilizaron algoritmos basados en el Standard de Firmas Digitales (DSS Digital Signature Standard) FIPS PUB 186-2 desarrollado por el Instituto Nacional de Tecnologías y Estándares (NIST).

Se utilizó el Estándar de Criptografía de Llaves Públicas (PKCS#11: Cryptographic Token Interface Standard) desarrollado por los laboratorios de RSA, para la interacción con los dispositivos smart cards.

Teniendo en cuenta la necesidad de portabilidad de los documentos generados en las actividades registrales, se procedió a la conversión al formato PDF (Portable Document Format) ISO 32000-1:2008 con el objetivo de garantizar en cualquier lugar la confiabilidad, seguridad e integridad de todos los documentos jurídicos.

Diseño de la arquitectura de la solución

Las actividades registrales se llevan a cabo en las oficinas de registros públicos y mercantiles, las cuales se centralizan en un Centro de Datos a nivel nacional. La inscripción de documentos es la principal función de los registros, estos tienen como objetivo garantizar la seguridad jurídica.

Los ciudadanos acuden a los registros para inscribir un documento legal redactado por un abogado en el cual se manifiestan en orden los actos registrales que deciden ejecutar. Este documento una vez presentado en una oficina de registros entra en un flujo de trabajo hasta que es inscrito como asiento registral.

Cada oficina cuenta con un sistema que automatiza los trámites registrales y convierte el documento que presenta el ciudadano a formato digital, este documento viaja digitalmente durante el flujo hasta ser archivado. La solución de firma digital avanzada que se propone es dotar al documento de las propiedades siguientes:

- Autenticidad: Asegura que el documento fue firmado digitalmente por el Registrador de la oficina donde fue inscrito.
- Integridad: Una vez firmado digitalmente, el documento no puede ser alterado.
- No Repudio: Una vez que el Registrador firma digitalmente un documento, este no puede retractarse del hecho.

Estas propiedades tributan a garantizar seguridad jurídica en las transacciones registrales que llevan a cabo los ciudadanos.

La gestión de los certificados digitales que son usados para las firmas digitales de los documentos es competencia de la Autoridad de Certificación (AC) y la Autoridad de Registro (AR) que son las encargadas de las actividades siguientes:

CA

- Emisión de certificados / generación de claves.
- Establecimiento y publicación de políticas.

- Emisión de la Lista de Revocación de Certificados (CRL).

RA

- Identificación y autenticación de los solicitantes.
- Impresión de las tarjetas inteligentes.
- Almacenamiento y Entrega de los Certificados en Tarjetas Inteligentes a los Registradores de cada oficina.
- Gestión de Revocación (CRL).
- Gestión del ciclo de vida de los certificados.

En el Centro de Datos se encuentra un servicio que interactúa con la Autoridad de Registro y a su vez Autoridad de Certificación, este se encarga de mantener actualizadas en la base de datos central la lista de certificados válidos que fueron emitidos a los registradores y la lista de de revocación de certificados (CRL). Cada certificado se replica hacia la base de datos de la oficina correspondiente donde el registrador posee su certificado con la llave privada en la tarjeta inteligente. La lista de revocación es replicada hacia todas las bases de datos de las oficinas para que esta pueda ser consultada localmente.

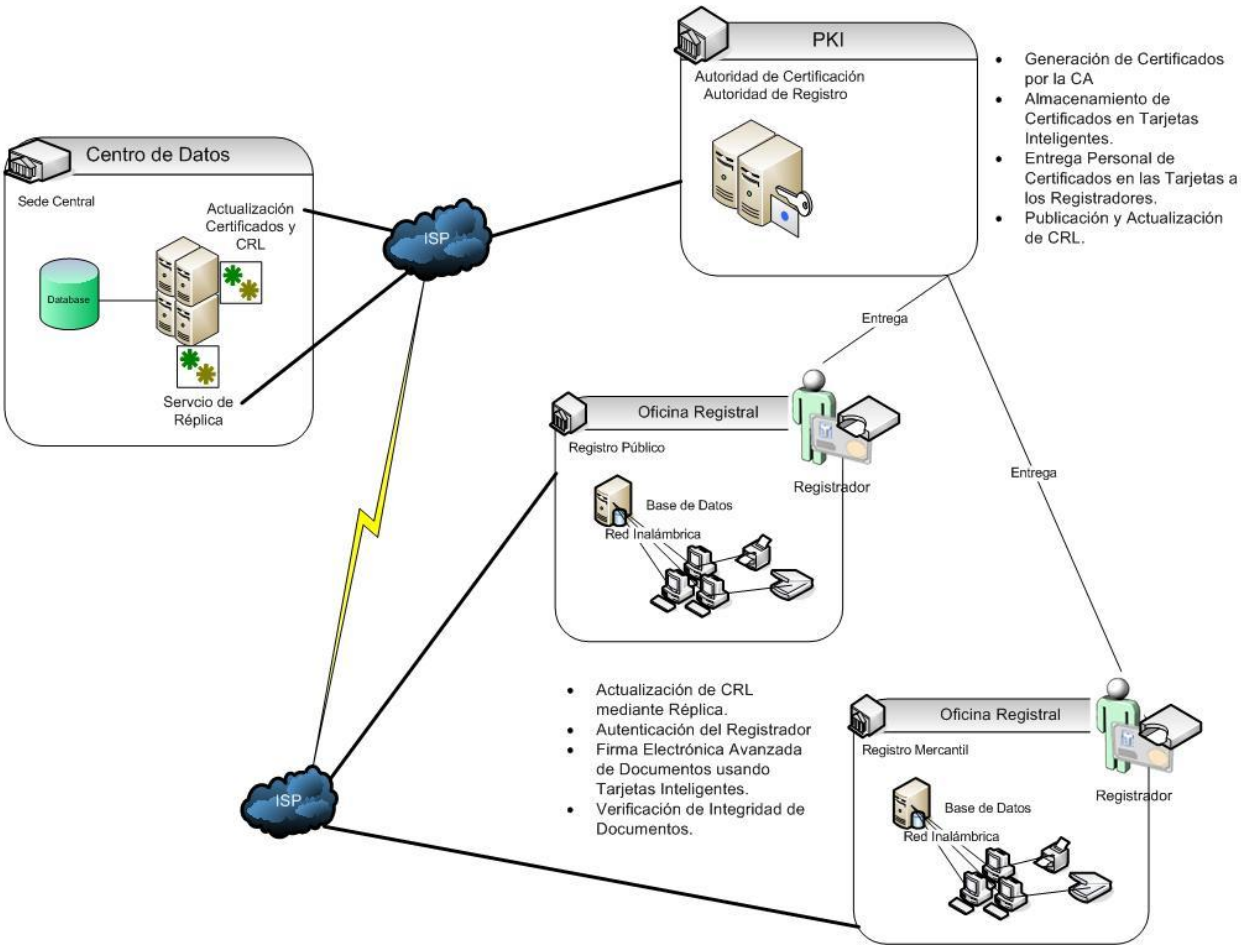

Fig. 1. Representación de la Arquitectura

Firma Digital Avanzada en el Flujo Registral

Una vez presentado el documento en una oficina de registros, este es escaneado y convertido en formato TIFF y almacenado en la base de datos local. Este documento sigue el flujo de trabajo dentro de la oficina. Luego de ser otorgado el documento original al ciudadano, su versión digital es convertida a formato PDF y pasa a ser firmado digitalmente por el registrador.

Funciones del Componente de Firma Digital Avanzada del Documento Jurídico

- Leer el Certificado Digital que se encuentra almacenado en la tarjeta inteligente del registrador.
- Verificar si el certificado no ha expirado su tiempo de uso.
- Verificar si el certificado pertenece realmente al Registrador que va a firmar el documento comparando la llave pública con la del certificado almacenado localmente en la base de datos.
- Verificar si el certificado fue emitido por la AC involucrada en la solución, comprobando si fue firmado con el certificado raíz de esta AC.
- Verificar si el certificado no ha sido revocado, consultado la lista de revocación emitida por la AC que se encuentra almacenada localmente.
- Firmar digitalmente el documento en formato PDF e incrustar la firma en el mismo archivo.

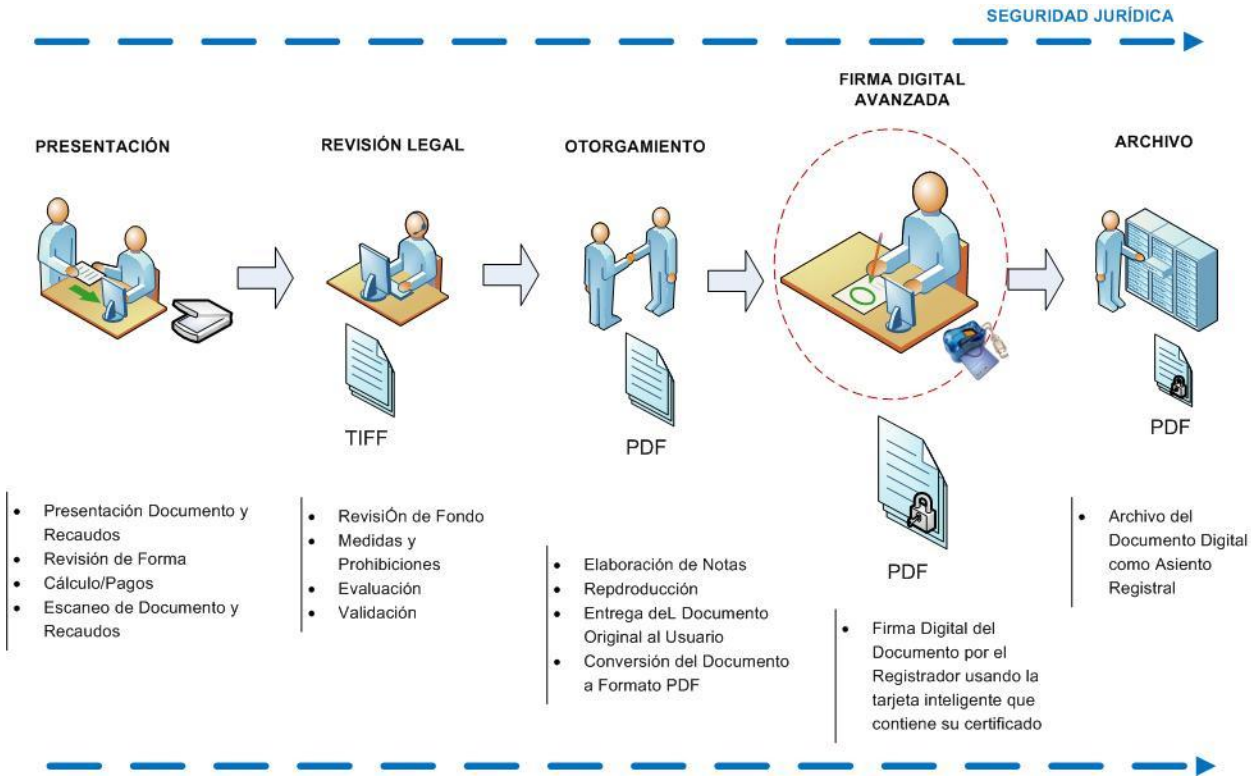

Fig. 2. Firma Digital Avanzada en el Flujo Registral

Este componente está integrado con el sistema que automatiza el flujo registral en cada oficina. El mismo fue desarrollado con la herramienta Visual Studio de Microsoft.

Este proceso ocurre en todas las oficinas registrales del país, lo cual tributa a la estandarización de los procesos de firmas y le otorga validez jurídica a los documentos electrónicos.

Resultados

La solución de Firma Digital Avanzada se encuentra integrada al sistema de automatización de los procesos registrales que actualmente está funcionando en los registros mercantiles y públicos de la República Bolivariana de Venezuela.

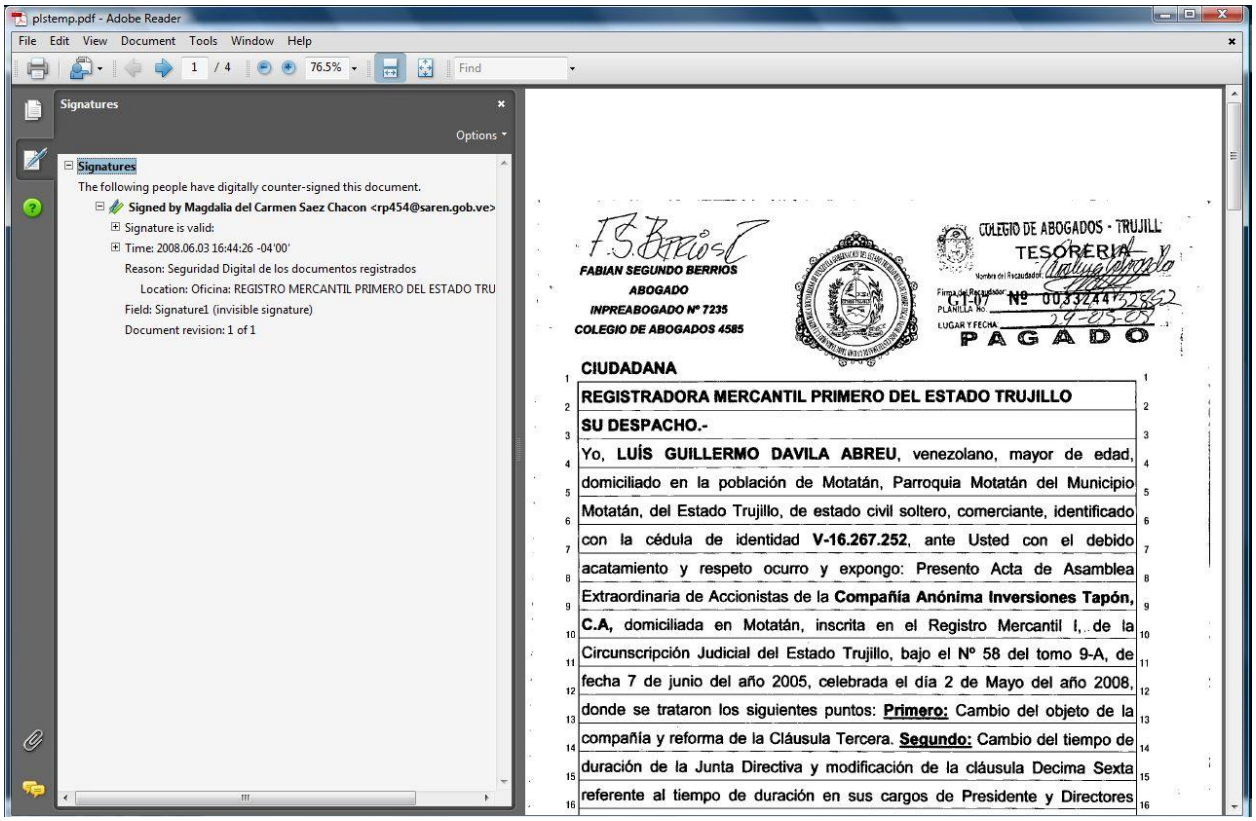

Fig. 3. Documento Firmado Digitalmente por la Registradora del Registro Mercantil Primero del Estado de Trujillo de la República Bolivariana de Venezuela.

Conclusiones

La seguridad de las transacciones y en específico el uso de las firmas digitales se convierte en una necesidad en el ámbito registral. La validez jurídica y probatoria que brinda a los documentos, permite además la verificación de la identidad del autor y comprueba que lo datos no han sido alterados desde que fueron firmados. Esto sin lugar a dudas constituye una herramienta que asegura la confiabilidad de los trámites registrales de la administración pública para con la sociedad.

La autenticidad, integridad y no repudio, son las propiedades fundamentales que brinda la firma digital avanzada de documentos jurídicos, lo cual constituye un componente fundamental para garantizar la seguridad jurídica en las actividades registrales.

Referencias Bibliográficas.

[1] Bruno Lowagie (2007) iText in Action Creating and Manipulating PDF.

[2] Carlisle Adams, Steve Lloyd (2002) Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition.

[3] Kapil Raina. (2003) PKI Security Solutions for the Enterprise: Solving HIPPAA, E-Paper Act, and Other Compliance Issues.

[4] García Gustavo (2007) Entrevista a Christian M. Pedreño "Gobierno Electrónico" [Versión Electrónica] Fecha de Consulta: 22 de junio de 2008, Disponible en: http://gustablg.blogspot.com/2007/11/algunas-de-las-preguntas-que-christian.html

[5] RSA Laboratories. *PKCS* #11: Cryptographic Token Interface Standard. Version 2.20, June 2004. URL: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf

[6] Raymond G. Kammer (2000) Digital Signature Standard (DSS).

[7] (2001) Ley de Registro P úblico y del Notariado de la República Bolivariana de Venezuela.

[8] (2001) Ley Sobre Mensajes de Datos y Firmas Electrónicas.