Capítulo 1

Introducción

Notario, es el profesional del Derecho investido de fe pública por el Estado que tiene a su cargo recibir, interpretar, redactar y dar forma legal a la voluntad de las personas que acuden ante él, y conferir autenticidad y certeza jurídica a los actos y hechos pasados ante su fe.

El Notario es el encargado de la creación de las Escrituras Públicas y las Actas Notariales que actualmente son registradas, en el Estado de Puebla, en el Instituto Registral y Catastral del Estado de Puebla y en el Archivo General de Notarios[1].

Se describe en este documento los detalles y minucias de cada uno de los procesos además de la implementación y las pruebas realizadas sobre la misma para así demostrar la efectividad de este proceso e implementación.

1.1. Objetivo

Existen dos problemas en la actualidad en la Notaria Pública en los que nos enfocaremos: La negativa en la aceptación de documentos y archivos digitales como instrumentos legales y la emisión de documentos físicos impresos cuya validez radica en el sello notarial original.

La negativa en la aceptación de documentos y archivos digitales como instrumentos legales para la asentación de actos o hechos implica la necesidad de proveer documentos físicos para la comprobación de la validez de los hechos o actos. Siendo así más importante para la comprobación del acto o hecho un documento físico que la información contenida en el mismo provocando así una barrera para la comprobación de los actos o hechos.

Por otra parte la emisión de las Escrituras Públicas y Actas Notariales en documentos físicos impresos cuya validez radica en el sello notarial original y en la existencia y conservación del documento físico, que implica el almacenamiento, conservación y organización de los documentos en el Archivo General de Notarios y en el Instituto Registral y Catastral del Estado de Puebla (IRCEP) que con la utilización de folios electrónicos, sigue sin permitir la verificación de un documento digital.

Además, el almacenamiento de copias en papel de documentos físicos que son primero copias entregadas a los interesados, los cuales, deberán almacenar el documento de una forma segura ya que la validez de los mismos como se mencionó anteriormente radica en la conservación del documento original y el sello notarial en el mismo. En segunda, como parte de los legajos y del Archivo General de Notarios y del IRCEP. Esto, no sólo representa un costo ambiental en papel (cuya producción representa 4,000 millones de árboles al año, algunos de ellos procedentes de bosques primarios que no pueden sustituirse) si no también como lo indica el Programa para un Gobierno Cercano y Moderno 2013-2018 del Gobierno Federal su reducción o eliminación "podrían generar ahorros aún mayores, por ejemplo, con el aprovechamiento del firmado electrónico de documentos para abatir los gastos en mensajería y en papel."

El objetivo de este trabajo es presentar una propuesta para la emisión de documentos y archivos digitales como instrumentos legales para la aceptación de actos o hechos en donde los distintos actores puedan firmar y se puedan autenticar.

1.2. Hipotesis

La definición de la palabra documento ha variado en los últimos años, remitiéndonos así a la definición más reciente donde la Real Academia Española (RAE) lo define, en el carácter público, como que "acredita los hechos que refiere y su fecha". Siendo así un documento de carácter público cualquier pieza que acredite los hechos que este refiere sin importar si existe en formato físico impreso o digital.

Un documento digital, entonces, tiene la misma validez para acreditar los hechos al que este refiere que un documento físico impreso. Solamente que este, al igual que un documento físico impreso, debe mantener la misma información con la que, desde un inicio, fue creado. A esto se le conoce

como integridad, es decir, el documento no debe sufrir cambios ya sea en su contenido o en su estructura manteniendo su integridad.

Aunque la aceptación de documentos digitales como instrumentos legales para la asentación de actos o hechos es posible, es decir, aceptar documentos digitales como pruebas de domicilio, nacionalidad, etcetera que no han sido verificados o autenticados previamente. La solución de raíz a este problema viene desde el momento en que emitimos documentos de manera física, entonces, la emisión de los mismos de manera digital solucionaría, además, la aceptación de los mismos en el mismo formato, dejando, al final, la utilización de los documentos digitales como instrumentos legales básicos para cualquier acto o hecho.

En la implementación presentada se autentica, verifica y almacena los documentos digitales dándoles así certeza y validez jurídica utilizando firmas digitales para la autenticación de los archivos digitales. Se utilizaron las firmas digitales que ya son expedidas por el SAT (Sistema de Acreditación Tributaria) en el caso de las personas físicas o morales y son validas como forma de identificación en trámites gubernamentales, en caso de Notarios existe el sello digital de Notarios visible en los documentos registrados ante el IRCEP.

Al utilizar entonces las firmas digitales se elimina la necesidad de utilizar documentos físicos para validar un acto o hecho debido a que no es necesaria la firma autógrafa de los actores para validar un acto. Además, a diferencia de las implementaciones hoy en día existentes donde se emiten sellos digitales únicamente validados por una parte del acto (el Notario) se realiza la validación del documento por todas las partes involucradas en el acto o hecho dando más certeza y confianza en el documento digital.

Se crea una versión digital firmada del documento digital, pero, el documento digital puede tener diversos formatos. Este trabajo se limita a la utilización de documentos en formato PDF (Portable Document Format). Existen varias opciones para obtener o crear una firma del documento, la primera opción es la utilización del contenido del documento, es decir, la extracción del texto o contenidos del archivo PDF, otra opción es la utilización de los bytes del documento. Esta opción es conveniente ya que el documento PDF podría contener, aunque no está especificado ni es utilizado por los notarios actualmente, imágenes u otro tipo de multimedio.

El proceso para la emisión de un nuevo documento digital certificado es, en orden secuencial, tras la creación de un documento en formato PDF se ingresa a la plataforma donde se transforma en un objeto buffer anexado a

otro objeto JSON. Se reciben de igual manera las llaves públicas y privadas y se transforman en un buffer de igual forma. Se genera un hash SHA-256 del documento recibido, se firma hash obtenido a través de un proceso de firmado RSA con llaves privadas utilizando cada llave privada recibida hasta obtener un nueva cadena. Se anexa esta nueva cadena, el hash generado, las llaves públicas extraídas del arreglo de llaves y el objeto buffer del archivo recibido a un objeto JSON que es enviado al servidor donde se realiza la verificación de la información donde, primero, se guarda al momento de recibir una nueva petición la hora en formato ISO 8601, se genera nuevamente el hash SHA-256 del archivo recibido y se realiza la verificación de la cadena firmada utilizando todas las llaves públicas recibidas en un órden inverso al orden en el que se realizo la creación. Se compara el hash recibido, el hash creado a partir del documento y la cadena obtenida tras finalizar el proceso de verificación. Finalmente, se verifica que una de las llaves públicas recibidas se encuentre en el registro interno de llaves públicas de Notarios para certificar la creación del documento por parte de un Notario y se almacena toda la información en la base de datos. Se regresa la hora de creación como comprobante de creación y se almacena todo en un archivo en formato JSON.

Para la verificación se utiliza el mismo proceso de verificación que se lleva acabo en el servidor donde el usuario sube el archivo original y el archivo JSON, se extrae el SHA original, el SHA firmado y las firmas públicas, se crea un nuevo SHA-256 del archivo original, se realiza el proceso de verificación RSA con las firmas públicas del SHA firmado y se compara el nuevo SHA generado, el SHA original del archivo JSON y la cadena obtenida del proceso de verificación RSA, en caso de ser idénticos se consulta con el servidor utilizando el SHA firmado la existencia de este en el registro del servidor para así dar una respuesta sobre la existencia y autenticidad del documento dado.

Este proceso de creación y verificación brinda certeza en autenticidad del documento generado y presentado. Además, permite no transmitir las llaves privadas de los interesados y el notario por ninguna red ya sea pública o privada para así proteger las identidades digitales de los mismos.