



Firma Digital: seguridad en el intercambio de información sobre Internet¹

+ Introducción

La aceptación masiva de nuevas tecnologías ha cambiado las formas de comunicación. Uno de los impactos mayores de esta realidad es la manera en que se intercambia la información: correo electrónico, transferencia de archivos en forma digital, descarga de datos en sitios Web, etc.

Sin embargo, esta migración hacia nuevos canales en los procesos de intercambio de información, no ha sido acompañado en todos los casos con la adopción de las medidas de seguridad apropiadas a los nuevos modelos.

En la mayoría de los casos, se sigue considerando la autenticación como un nivel “aceptable” para ciertas transacciones, utilizando como mecanismo el empleo de contraseñas, que fueron diseñadas para contextos totalmente diferentes de los actuales. Esta práctica esta siendo reemplazada por mecanismos de autenticación de dos factores debido a los innumerables fraudes que se producen en los circuitos comerciales.

Un mecanismo de autenticación robusto es el primer requisito para sistemas cerrados con operaciones de valor crítico. Sin embargo, uno de los ingredientes fundamentales para asegurar la confiabilidad de las transacciones en el comercio electrónico es la utilización de certificados digitales y la posibilidad de firmar digitalmente la transacciones efectuadas. Este mecanismo puede además ser utilizado para el intercambio de datos sobre redes abiertas de comunicación con las garantías de autenticidad, confidencialidad e integridad necesarias. Trataremos de describir en este artículo en qué consiste esta tecnología y como se derivan de ella los atributos de seguridad y confiabilidad imprescindibles.

¹ Por el Dr Norberto Marinelli. Licenciado en Administración y Contador Público (U.B.A.). Es socio fundador de CertiSur S.A., Afiliado Principal de VeriSign para la Región. Actualmente se desempeña como vicepresidente del Directorio y C.E.O. de dicha empresa.



ÍNDICE DE CONTENIDO

+ Introducción.....	1
+ Seguridad en los medios de soporte de la información	3
+ La criptografía y su aplicación para obtener la seguridad necesaria	3
+ Beneficios de la aplicación de la tecnología.....	4
+ La utilización de firmas y certificados digitales en nuestra Profesión	4

+ Seguridad en los medios de soporte de la información

Los documentos firmados en papel tienen atributos de seguridad que le resultan inherentes, como por ejemplo: la permanencia de la tinta embebida en las fibras celulósicas, la singularidad biométrica de las firmas manuscritas (en donde características tales como la presión, la forma, la dirección de la escritura, son únicas de parte del firmante) y la posibilidad de detectar modificaciones, enmiendas, interlineados o borraduras.

Los mensajes y registros digitales no cuentan con estos mismos atributos de seguridad. Los mensajes que se cursan en sistemas computarizados son simplemente cadenas de dígitos binarios (o bits), ceros o unos, que representan información, tal como palabras o números, de una manera codificada.

Sin la aplicación de mecanismos de seguridad externos y suplementarios resultaría imposible asegurar idénticos niveles de confiabilidad a los existentes en el mundo físico basado en el papel.

En contraste con lo anterior, los registros computacionales no son inherentemente únicos. Es más, uno de los principales beneficios de los datos digitales es la posibilidad de realizar múltiples copias, simplemente presionando una tecla. En este proceso no se puede diferenciar entre original y copia, características propias del papel y, en determinados casos, de distinto valor jurídico. Desafortunadamente, esta particularidad impide utilizar a un registro digital de la misma manera que un documento basado en papel.

Por lo tanto, las diferencias existentes entre ambos medios demandan el uso de mecanismos y procedimientos diferentes para arribar a las mismas condiciones de prueba, en términos legales. Mientras que un simple y único documento en papel es adecuado para negociar la transferencia de un título, en el mundo digital será necesario realizar una sucesión de mensajes, criptográficamente asegurados para alcanzar idénticos niveles de confiabilidad.

+ La criptografía y su aplicación para obtener la seguridad necesaria

Las técnicas criptográficas, tales como encriptación y firmas digitales, son importantes en la implementación de tecnologías de seguridad. La base de la criptografía la constituyen los denominados “algoritmos criptográficos” o “criptosistemas”.

Una firma digital es un dato que acompaña o se adjunta a un mensaje o documento digital y que es empleado para asegurar la identidad del emisor del mensaje y que el documento no ha sido alterado desde que se originó.

Una firma digital garantiza la integridad de la información firmada, algo bastante similar a lo que habitualmente conocemos como un dígito verificador. Sin embargo, la mayor diferencia estriba en que una firma digital permite asegurar el “no repudio” de lo firmado, es decir que el receptor de un mensaje firmado cuenta con los elementos necesarios para comprobar para sí o ante terceros, la identidad del emisor de dicho mensaje o documento.

Para asociar una firma digital a una persona es necesario contar con un elemento denominado certificado digital. Todo firmante, al general una firma, incluye en la misma una copia de su certificado que le permite al receptor validar de manera sencilla la identidad del firmante.

Cada firmante debe solicitar su certificado digital a un emisor. Un certificado digital, además de contener datos propios de la persona, puede incorporar información de uso, tal como su condición de profesional o el número de matrícula, de tal manera que el receptor pueda verificar no solamente la validez de la firma, sino también otros atributos del firmante.

Como se puede observar, el fundamento de toda la tecnología está dado por la disponibilidad de los certificados digitales de quienes pretenden utilizarla. En el proceso de emisión, la organización emisora debe garantizar que los certificados que se emitan cumplan con apropiados niveles de seguridad tecnológica. Los procedimientos y documentación legal que se aplican dentro de la comunidad deben



ser robustos y ajustados a la legislación vigente y al uso que se le pretenda asignar a los certificados.

Si la tecnología empleada no es la correcta o no se cuenta con el respaldo legal apropiado, generado a partir de los contratos aceptados por cada una de las partes intervinientes dentro del sistema, los identificadores que se emitan o los documentos que se firmen digitalmente no contarán con los atributos cuya obtención se procura.

Por ejemplo, si no es posible afirmar que el certificado que se utilizó para encriptar una comunicación o verificar una firma digital es efectivamente el correspondiente al legítimo usuario destinatario del mensaje (en el caso de encriptación) o el legítimo firmante del mensaje (para verificar una firma digital), toda la confianza en el sistema desaparece. Si un intruso pudiera suplantar un certificado válido por otro, podría acceder a información confidencial o falsificar una firma. En otras palabras, la protección que brinda esta tecnología estaría totalmente comprometida.

+ Beneficios de la aplicación de la tecnología

El beneficio primario que se obtiene con un servicio de certificados es que cualquier usuario puede confiar en una cantidad muy importante de certificados de otros usuarios, simplemente contando con el certificado de la autoridad emisora de los certificados de la comunidad. Por ello, los certificados son un medio para asegurar la escalabilidad, es decir el incremento de tamaño de una comunidad de usuarios en donde la tecnología pueda ser usada sin inconvenientes.

La supresión del papel como elemento de soporte de la información representa un proceso de cambio cultural muy profundo y con consecuencias económicas altamente significativas. Pormenorizar los efectos de dichos cambios excede el alcance de este artículo.

No obstante, a modo de resumen podemos afirmar que en una profesión en donde el intercambio de datos e información es permanente, la reducción de tiempos de transporte al poder efectuar el mismo sobre redes abiertas y en formato digital con condiciones de resguardo y confidencialidad aseguradas, representa ahorros de costos muy significativos. Las distancias desaparecen

automáticamente, como así también los condicionamientos horarios.

+ La utilización de firmas y certificados digitales en nuestra Profesión

Como se pudo apreciar de la breve descripción del funcionamiento de la tecnología de firmas y certificados digitales, su utilización en el campo de las profesiones en Ciencias Económicas es sumamente amplio. Como ya se puntualizó, el ejercicio de la actividad profesional supone la elaboración y el intercambio permanente de documentos y datos. En algunos casos, se trata de datos sensibles cuyo conocimiento debe estar limitado a una audiencia sumamente reducida: información de gestión, análisis de fortalezas y debilidades competitivas, proyectos de inversión, etc.

No son pocos los profesionales que, actualmente, utilizan las bondades de Internet y del correo electrónico para intercambiar información sensible. Pocos tienen presente que enviar ese tipo de información sobre la Web (ya sea que se trata de Internet o de Intranet) implica la posibilidad de que cualquier tercero pueda acceder a la misma y utilizarla de manera inapropiada.

Por lo tanto, una de las funcionalidades importantes que tiene la tecnología de certificados digitales es la posibilidad de encriptación aprovechando los medios tecnológicos disponibles para acelerar el proceso comunicacional pero restringiendo el conocimiento de información sensible a los destinatarios legítimos de la misma.

Existen casos donde la información generada o validada por los profesionales, a diferencia de lo comentado anteriormente, está destinada a ser compartida por comunidades más amplias o incluso abiertas (por ejemplo, el público en general) y en donde el atributo más importante es asegurar la integridad de la información comunicada y la identidad de las personas, profesionales u organizaciones que han intervenido en la preparación y certificación de la misma.

Así, por ejemplo, una empresa puede compartir sus Estados Contables de manera digital en forma pública o entregar los mismos en ese formato a otras organizaciones (por ejemplo, instituciones financieras), pero con mecanismos que aseguren



que efectivamente los mismos han sido confeccionados por la empresa y debidamente auditados y certificados por el profesional correspondiente. La manera de lograr este mecanismo es muy simple: certificados digitales para los funcionarios y profesionales responsables de la firma de los Estados. Los destinatarios de la información pueden satisfacer de manera inmediata, a través de los mecanismos que provee la tecnología, sus necesidades de controlar la integridad y autoría de la información recibida.

En nuestro país la legislación posibilita la participación de las organizaciones profesionales en la implementación de la tecnología. Por ejemplo, la Ley 25.506 de Firma Digital, en su artículo 18, establece que “las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las efectuadas en forma manuscrita”.

Esta facultad no excluye que otras organizaciones que agrupen a profesionales puedan ofrecer servicios que posibiliten la utilización de la tecnología y de esta forma facilitar el acceso a la misma, por ejemplo para la protección de las comunicaciones confidenciales con sus clientes.

Existen antecedentes en nuestra región que muestran la utilización de firmas digitales asociadas al intercambio o presentación de información contable. El Banco Central de la República Oriental del Uruguay estableció, mediante Comunicación 37/2002, que las entidades financieras deben presentar sus estados contables en formato digital y que la autenticación del documento deberá realizarse por firma digital, para lo cual los representantes legales de cada institución y el auditor externo deben contar con la certificación correspondiente.

En nuestro país, la tecnología se encuentra disponible y son múltiples los casos exitosos en los que la misma ha sido implementada: las Bolsas de Cereales, a través de Confirma (www.confirma.com.ar) brindan un servicio sobre Internet para la firma de contratos digitales en el mercado de granos, reduciendo costos, optimizando sensiblemente los tiempos operativos y disminuyendo los riesgos de manera notable. Varios miles de millones de pesos son transados anualmente de manera digital y con mayores niveles

de seguridad y confiabilidad que mediante la utilización del papel.

Entendemos que nuestra Profesión no puede demorar más la implantación de este tipo de servicios, de modo tal de continuar a la vanguardia en el empleo de las tecnologías más modernas.