LIC. JOSÉ RAÚL GONZÁLEZ VELÁSQUEZ

El Comercio Electrónico y la Firma Digital

José Raúl González Velásquez

2007

17 DE SEPTIEMBRE DE 2007

EL COMERCIO ELECTRÓNICO Y LA FIRMA DIGITAL

Lic. José Raúl González Velásquez

RESUMEN

El presente artículo trata sobre las relaciones comerciales que se efectúan en Internet y analiza el problema de la incertidumbre e inseguridad que se genera al realizar transacciones en una red abierta.

Para evitar actuaciones accidentales o maliciosas de vendedores, consumidores y de terceras personas se necesita generar suficientes garantías a través de la elaboración de mecanismos de seguridad que sean compatibles y complementarios para reducir los riesgos en las transacciones comerciales

Para este tipo de actividades se necesita que exista confianza en las partes que lo integran, proveedores, vendedores y consumidores, por lo que se propone el uso de la firma digital, analizando su funcionamiento y las ventajas que se obtienen por su nivel de seguridad.

EL COMERCIO ELECTRÓNICO Y LA FIRMA DIGITAL

Desde su creación, el internet ha experimentado un crecimiento acelerado en el número de usuarios, y según registros estadísticos, del año 2000 al 2007 se ha incrementado en un 225% a nivel mundial, un equivalente a 1,173,109,925 usuarios (Exito Exportador, 2007). En Centro América este aumento es de 522.3% (20,021,900 usuarios).

El internet lo emplean a través de sus distintas aplicaciones como el World Wide Web y el correo electrónico con diferentes objetivos según las necesidades del usuario: didáctico, publicación de artículos, informativo, etc.; pero cierto número de personas además de lo anterior, lo emplean junto con otras aplicaciones como el Intercambio Electrónico de Datos (EDI, por sus siglas en inglés) para actividades de índole comercial e inclusive transacciones que no tienen un origen contractual (ejemplo: pago electrónico on-line)

Según Apol·lònia Martínez Nadal, citando la Comunicación de la Comisión de las Comunidades Europeas al Consejo, al Parlamento Europeo, al Comité Económico Social y al Comité de las Regiones sobre Iniciativa Europea de Comercio Electrónico en Bruselas del 16 de abril de 1997, hace referencia al concepto de Comercio Electrónico, el cual consiste en "realizar electrónicamente transacciones comerciales; es cualquier actividad en la que empresas y consumidores interaccionan y hacen negocios entre sí o con las administraciones por medios electrónicos. Se incluyen en esta forma de comercio actividades muy diversas como comercio electrónico de bienes y servicios; suministro en línea de contenidos digitales; las transferencias electrónicas de fondos; la compra y venta de acciones; los conocimientos de embarque; las subastas comerciales; los diseños y proyectos conjuntos; la prestación de servicios en línea; la contratación pública; la comercialización directa al consumidor; y los servicios postventa" (Martínez Nadal, 2001).

La utilización del Internet para fines comerciales ofrece ventajas, como por ejemplo: Al vendedor le permite reducción de costes y aumenta la celeridad de las mismas; por el lado del consumidor, permite comprar en cualquier parte del mundo, aumentando su capacidad de elección y por ende, la obtención de artículos y servicios a

precios más bajos. Sin embargo, debido a su naturaleza de ser una red abierta, plantea problemas de seguridad tanto a nivel técnico como jurídico.

Los problemas de naturaleza jurídica giran en torno a la validez y eficacia de las diferentes transacciones comerciales sean contractuales o no. Respecto de la transacción contractual se da el problema del perfeccionamiento de la misma, la cual es complicada si se adiciona el elemento de la extraterritorialidad de la operación (jurisdicción y ley aplicables) y problemas relativos al medio de comunicación en sí, como lo sería el rechazo de la misma ya sea del origen o del destino de un mensaje.

Los problemas a nivel técnico incluyen el uso, abuso y el error de la utilización del medio informático, por ejemplo: Suplantación de personalidad, transacciones fraudulentas, *phising*, alteración de mensajes, intercepción de mensajes por terceras personas.

Los riesgos más importantes del empleo del internet a nivel comercial son: la suplantación del autor o del mensaje durante cualquier momento, alteración del contenido de los mensajes, la negatoria de envió o recepción del mensaje por parte del emisor y receptor respectivamente y que el contenido del mensaje sea conocido por personas ajenas al receptor y emisor.

Según la Unión Internacional de Telecomunicaciones, las amenazas contra un sistema de comunicación de datos son las siguientes (Comité Consultivo Internacional Telegráfico y Telefónico, 1991):

a) Destrucción de información y/o de otros recursos;
b) Corrupción o modificación de información;
c) Robo, supresión o pérdida de información y/o de otros recursos;
d) Revelación de información;
e) Interrupción de servicios.

Este sistema de comercio necesita sustituir la documentación en soporte físico (papel) por su equivalente electrónico, para la generación de confianza entre proveedores, distribuidores y consumidores, delimitando y garantizando las responsabilidades de los mismos.

Respondiendo a estas inquietudes, una posible solución sería la firma digital. La firma digital es un derivado de la firma electrónica. Esta última se define como "cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita" (Martínez Nadal, 2001).

En cambio, la firma digital es "una firma electrónica que utiliza una técnica de criptografía asimétrica tal que una persona que disponga de la clave pública del firmante puede determinar si: a) la transformación se realizó utilizando la clave privada del firmante que corresponde a la clave pública del firmante (esto es, autenticación); y b) el mensaje de datos ha sido alterado (es decir, integridad)" (Martínez Nadal, 2001).

Según el Diccionario de la Lengua Española, criptografía es el arte de escribir con clave secreta o de un modo enigmático. Una explicación más exacta es la de generar mensajes que no pueden ser entendidos a menos de tener cierto código que devuelva los mensajes a su forma original. La criptografía puede ser simétrica o asimétrica, la primera consiste en que ambas partes poseen el mismo código para cifrar y descifrar el mensaje.

La criptografía asimétrica consiste en asociar dos claves: Una privada, que sólo es conocida por el dueño y una pública que es conocida por las demás personas a través de registros, directorios, etc. La relación de las mismas es matemática, empleando algorítmos distintos, de tal forma, que vuelve imposible elaborar la clave privada basándose en la clave pública.

La criptografía asimétrica permite confidencialidad y la elaboración de firmas digitales. La confidencialidad se refiere al envío de mensajes a través de rutas inseguras en donde el emisor cifra el mensaje empleando la clave pública y el receptor lo descifra con su clave privada. Este proceso garantiza la confidencialidad, debido a que sólo con la clave correcta el mensaje tendrá sentido.

La elaboración de firmas digitales provee la autenticidad del mensaje, el no rechazo del origen y la integridad del mismo. El procedimiento para la elaboración de la firma digital consiste en: El emisor del mensaje (titular de la clave) lo cifra utilizando la clave privada y el receptor lo descifra utilizando la clave pública. Solamente con la

coincidencia de ambas claves se tiene la seguridad que dicho mensaje fue enviado por el titular.

A esto se le puede agregar un elemento nuevo, denominado *función hash*, que es la aplicación de algorítmos en una secuencia de bits para obtener una menor, en otras palabras, genera un resumen único del mensaje, que posee la característica de que no se puede replicar usando un mensaje diferente al original. Dicho resumen se cifra usando la clave privada[1] y se envía junto con el mensaje completo sin cifrar, el receptor descifra el resumen (*hash*) y aplica la *función hash* sobre el mensaje completo y si ambos hash son iguales, significa que el mensaje no ha sido alterado.

De esta forma, la firma digital adquiere superiores efectos a la firma manuscrita, porque identifica a la persona, la vincula con el acto y con el contenido del mismo. Sin embargo, es de aclarar que el par de claves deben ser seguras, entendiendo por "seguras" el hecho de no poder obtener la clave privada empleando la clave pública[2]. De igual forma debe ser seguro el procedimiento ocupado para la generación de las mismas.

Pero existen dos problemas que no puede resolver por si misma la firma digital: a) La autenticación, que involucra la seguridad de que la persona que firmó digitalmente el mensaje es quien dice ser y b) El rechazo de destino.

Se puede concluir que el aumento del uso del internet hace necesaria la firma digital, la cual forma parte de la solución frente a los problemas de incertidumbre e inseguridad, tanto jurídica como técnica, en las transacciones comerciales de proveedores, vendedores y consumidores.

El involucramiento de la criptografía asimétrica junto con la *función hash*, reducen los costos de operación y garantizan la confiabilidad, el no rechazo del origen e integridad del mensaje. Eso es posible, siempre y cuando existan niveles mínimos de seguridad para la elaboración de las claves y de la imposibilidad material de reproducir la clave privada a partir de la clave pública.

[1] Se cifra el resumen debido a que los costos de cifrado aumentan en proporción al tamaño del texto.
[2] Puede darse el caso de emplear programas para descifrar la clave privada, sin embargo, las claves fuertemente protegidas usan 1024 bits, lo que equivale a combinaciones de 300 dígitos (Angel Angel).

La firma digital, elaborada con estas cualidades, concibe una igual o superior seguridad y confiabilidad frente a la firma manuscrita, realizando las mismas funciones que consisten en identificar a la persona, relacionándola con un acto y con el contenido del mismo.

Se debe entender que la firma digital en si misma, no solventa todos los problemas relativos al comercio electrónico, como lo son el no rechazo de destino ni la vinculación de la persona con una determinada firma. Por esa razón, se deben elaborar mecanismos complementarios que actuando de forma conjunta, reduzcan la problemática antes mencionada.

BIBLIOGRAFÍA

- Angel Angel, J. d. (s.f.). *wikilearning*. Recuperado el 16 de Septiembre de 2007, de http://www.wikilearning.com/vocabulario_sobre_criptografia-wkccp-4306-10.htm
- Comité Consultivo Internacional Telegráfico y Telefónico. (1991). *Unión Internacional de Telecomunicaciones.* Recuperado el 16 de Septiembre de 2007, de http://www.itu.int/rec/T-REC-X.800-199103-I/es
- Exito Exportador. (30 de Junio de 2007). *Exito Exportador.* Recuperado el 15 de Septiembre de 2007, de Exito Exportador: http://www.exitoexportador.com/stats.htm
- Martínez Nadal, A. (2001). *Comercio Electrónico, Firma Digital y Autoridades de Certificación* (Tercera Edición ed.). Madrid, España: Civitas.
- Real Academia Española. (s.f.). *Real Academia Española*. Recuperado el 16 de Septiembre de 2007, de http://www.rae.es/