UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

Facultad de Ingeniería

Escuela de Ingeniería Informática

Proyecto final para optar al grado de Licenciado en Ingeniería de Sistemas con énfasis en Gestión de Recursos Tecnológicos

Seguridad en los medios de pago electrónicos

Olman Díaz Elizondo
Cédula 5-224-470

Profesor: Lic. Miguel Pérez Montero

Diciembre, 2006

Índice

Resumen ejecutivo

Este trabajo resume la importancia de la seguridad en los medios de pago electrónicos, ya que se han producido cambios sustanciales en los medios de pago tradicionales.

El tema de la seguridad merece especial atención; es un elemento clave en este tipo de transacciones, en tanto el medio por donde transita la información es inseguro. Aunque no está al alcance de cualquier persona, un operador experimentado puede interceptar la información. Por ello se han desarrollado distintos mecanismos para proteger la información que se transmite. Hasta el momento, lo más efectivo ha sido recurrir al milenario sistema de cifrar la información que se envía.

Con la aprobación de la Ley 8454, se están abriendo atractivas posibilidades a las empresas e instituciones que realizan o quieren realizar negociaciones en forma electrónica con un grado de seguridad mayor que el que hoy existe.

Abstract

This summary mentions the importance of security in the electronic ways of payment because there have been important changes on the traditional ways of payment.

The security theme deserves special attention; it is a clue element in these type of transactions, besides the mean in which the information is being transmitted in not safe. Although this is not reached by any person, an experienced operator can intercept the information. This is the reason why different mechanisms have been developed in order to protect the transmitted information. At this moment, the most effective method has been to use the millenarium system of numbering the information that is being sent.

With the approval of Law # 8454, there are some suitable possibilities which have been opened to the companies and institutions. These companies and institutions have been negotiated or will negotiate by electronic means with a better grade of security than the one already existing.

Frases descriptoras

1- Criptografía

2- Firma digital

3- Certificado digital

4- Entidad certificadora

5- SINPE

Introducción

Como es bien conocido, los medios de pago tradicionales sufren numerosos problemas de seguridad: falsificación de billetes, falsificación de firmas, cheques sin fondo, etc. Por otro lado, los medios de pago electrónicos, además de estar sujetos a los mismos problemas anteriores, presentan riesgos adicionales, pues, a diferencia del papel, los documentos digitales pueden ser copiados perfectamente y cuantas veces se desee, las firmas digitales pueden ser falsificadas por cualquiera que conozca la clave privada del firmante, la identidad de una persona puede ser asociada de forma inequívoca con la información relacionada en cada pago, etc.

Por ello es necesario establecer nuevos mecanismos de seguridad para los nuevos medios de pago electrónicos, si se quiere que tanto las entidades bancarias como los usuarios finales acepten de forma generalizada estos nuevos medios de pago. Por otro lado, si los sistemas de pago electrónicos son bien diseñados, pueden proporcionar una mayor seguridad y flexibilidad de uso que la ofrecida por los medios de pago tradicionales.

La criptografía está representando un papel fundamental en la incorporación de nuevos medios de pago a los ya existentes hoy en día, pues es la base sobre la que se sustenta la seguridad de estos nuevos medios. Por otro lado, la aparición de nuevos dispositivos físicos, como las tarjetas inteligentes y otros módulos de seguridad, permite y posibilita la implementación de los diferentes protocolos criptográficos de estos medios de pago.

En un futuro próximo los costarricenses veremos además cómo nuestras tradicionales tarjetas de crédito y débito, que normalmente funcionan a través de una banda magnética, serán sustituidas por tarjetas inteligentes con los más populares algoritmos criptográficos y que podrán contener, además, cualquier tipo de aplicación financiera.

Historia de la criptografía

La criptografía es el arte o ciencia cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que solo puedan ser leídos por las personas a quienes van dirigidos.

La finalidad de la criptografía es garantizar el secreto en la comunicación entre dos entidades y en asegurar que la información que se envía es auténtica. Que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado no haya sido modificado en su tránsito.

Tradicionalmente se ha hablado de dos tipos de sistemas criptográficos: los simétricos o de clave privada y los asimétricos o de clave pública.

La criptografía ha venido siendo utilizada desde antiguo, fundamentalmente con fines militares. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares de forma que, si el mensajero era interceptado, la información que portaba no corriera el peligro de caer en manos del enemigo. Posiblemente, el primer sistema de criptografía que se conoce fuera documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, y es el método actualmente conocido como César, porque supuestamente Julio César lo utilizó en sus campañas, uno de los más célebres en la literatura. Otro de los métodos criptográficos utilizados por los griegos fue la *escitala espartana*, un método también de transposición basado en un cilindro que servía como clave en el que se enrollaba el mensaje para poder cifrar y descifrar.

Durante los siglos XVII al XIX, el interés de los monarcas por la criptografía fue notable. Las huestes de Felipe II utilizaron durante mucho tiempo una cifra con un alfabeto de más de 500 símbolos que los matemáticos del rey consideraban inexpugnable. Cuando el matemático francés Francois Viete consiguió criptoanalizar aquel sistema para el rey de

Francia, a la sazón Enrique IV, el conocimiento mostrado por el rey francés impulsó una queja de la corte española ante del papa Pío V en que acusaba a Enrique IV de utilizar magia negra para vencer a sus ejércitos. Por su parte, María Estuardo, reina de los Escoceses, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel.

Desde el siglo XIX y hasta la Segunda Guerra Mundial las figuras más importantes fueron la del holandés Auguste Kerckhoffs y la del prusiano Friedrich Kasiski. Pero es en el siglo XX cuando la historia de la criptografía vuelve a presentar grandes avances. En especial durante las dos contiendas bélicas que marcaron al siglo: la Gran Guerra y la Segunda Guerra Mundial. A partir del siglo XX, la criptografía usa una nueva herramienta que permitirá conseguir mejores y más seguras cifras: las máquinas de cálculo. La más conocida de las máquinas de cifrado posiblemente sea la máquina alemana Enigma: esta máquina de rotores automatizaba considerablemente los cálculos que eran necesarios realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. Por ende, los mayores avances tanto en el campo de la criptografía como en el del criptoanálisis no empezaron hasta entonces.

Después de la Segunda Guerra Mundial, la criptografía tiene un desarrollo teórico importante; y fueron Claude Shannon y sus investigaciones sobre teoría de la información esenciales hitos en dicho desarrollo. Además, los avances en computación automática suponen tanto una amenaza para los sistemas existentes como una oportunidad para el desarrollo de nuevos sistemas. A mediados de los años 70 el Departamento de Normas y Estándares norteamericano publica el primer diseño lógico de un cifrador que estaría llamado a ser el principal sistema criptográfico de finales de siglo: el Estándar de Cifrado de Datos o DES. Los sistemas criptográficos simétricos más utilizados son DES, TDES y AES.

El concepto de firma digital fue introducido por Diffie y Hellman en 1976. En esas mismas fechas ya se empezaba a gestar lo que sería la, hasta ahora, última revolución de la criptografía teórica y práctica: los sistemas asimétricos, el más utilizado es el llamado RSA, creado en 1978 por Rivest, Shamir y Adleman. Estos sistemas supusieron un salto cualitativo importante ya que permitieron introducir la criptografía en otros campos que hoy día son esenciales, como el de la firma digital.

Firma digital

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales y posibilita que estos gocen de una característica que únicamente era propia de los documentos en papel. En contrapartida, la firma manuscrita es barata, fácil de producir, fácil de reconocer tanto por el propietario como por otros y, además, es imposible de rechazar por el propietario.

La firma digital funciona utilizando complejos procedimientos matemáticos que relacionan el documento firmado con información propia del firmante y permiten que terceras partes puedan reconocer la identidad del firmante y asegurarse de que los contenidos no han sido modificados.

El firmante genera, mediante una función matemática, una huella digital del mensaje, la cual se cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital, que se enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento una marca que es única para dicho documento y que solo él es capaz de producir.

Para realizar la verificación del mensaje, en primer término el receptor generará la huella digital del mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que no hubo alteración y que el firmante es quien dice serlo.

La firma digital no implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.

La firma digital es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen.

Ley 8454

La *Ley de Certificados, Firmas Digitales y Documentos Electrónicos* recibió el primer ejecútese el 22 de agosto del 2005 y se publicó en el diario oficial *La Gaceta* n.º 197 del 13 de octubre del 2005.

El objetivo de esta ley es proporcionar un marco jurídico que brinde certeza y seguridad a las transacciones que se realicen a través de Internet, agilizar las transacciones públicas e incentivar las tecnologías de la información en Costa Rica.

Su estructura es la siguiente:

- Capítulo I: Disposiciones generales
- Capítulo II: Documentos
- Capítulo III: Firmas digitales
- Capítulo IV: Certificación digital
- Capítulo V: Sanciones
- Capítulo VI: Disposiciones finales y transitorias

Esta redactada en forma general, que incluye aspectos medulares, y deja fuera temas específicos que pueden ser tratados a nivel de reglamento.
Para su implementación se apoya en instituciones ya existentes (MICIT y ECA).

La ley y el reglamento de la firma digital promueven la creación por parte del Estado de servicios que utilicen esta tecnología.

Se señala directamente que la firma digital se podrá utilizar para notificaciones, citaciones y otras comunicaciones judiciales, así como para la tramitación, gestión y conservación de expedientes del Poder Judicial.

También se permite emitir certificaciones y constancias por medios digitales, realizar los principales trámites del Registro Nacional y buena parte de los procedimientos relativos a los protocolos notariales.

Infraestructura

La "Infraestructura de Firma Digital" está formada por el conjunto de leyes, normativa legal complementaria, obligaciones legales, *hardware, software*, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades o individuos se identifiquen entre sí de manera segura al realizar transacciones en redes.

Realmente esta definición es conocida mundialmente con las siglas PKI, que significan *Public Key Infraestructure* o Infraestructura de Clave Pública.

Aplicaciones y beneficios de la firma digital

- Mensajes con autenticidad asegurada
- Contratos comerciales electrónicos.
- Factura electrónica.
- Desmaterialización de documentos.
- Transacciones comerciales electrónicas.
- Invitación electrónica.
- Dinero electrónico.
- Notificaciones judiciales electrónicas.
- Voto electrónico.

- Decretos ejecutivos (Gobierno).
- Créditos de seguridad social.
- Contratación pública.
- Sellado de tiempo.

Reglamento ejecutivo

El reglamento a la *Ley de Certificados, Firmas Digitales y Documentos Electrónicos.* Decreto ejecutivo n.º 33018-MICIT del 20 de marzo del 2006, que entró a regir en el país tras ser publicado en *La Gaceta* n.º 77 del 21 de abril del 2006. Su uso tiene como base los parámetros técnicos internacionales normas ISO 21188. El ministro de Ciencia y Tecnología conformó una comisión encargada de la redacción del reglamento, la cual contó con representación del sector público y del privado.

Su estructura se divide en dos partes:

- Primera parte: texto reglamentario propiamente dicho
- Segunda parte: Anexo único de "lineamientos técnicos"

Documentos electrónicos

El avance técnico y tecnológico ha permitido reconocer la necesidad de complementar al soporte en papel con otros medios.

El papel ha sido el respaldo fundamental de las actuaciones jurídicas durante siglos. Pero tiene muchas desventajas, además del costo social y ambiental. Se deteriora con el tiempo y los elementos, requiere manipulación física, su conservación exige espacio creciente, su recuperación es dificultosa y su duplicación es incomoda.

El Código Procesal Civil, en el artículo 368, Distintas clases de documentos, dice: "Son documentos los escritos los impresos, los planos, los dibujos, los cuadros, las fotografías, las radiografías, las cintas cinematográficas, los discos, las grabaciones magnetofónicas y en general, todo objeto mueble que tenga carácter representativo o declarativo".

La Ley 8454, artículo 3, afirma: "Cualquier manifestación con carácter representativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan, o transmitan por medios físicos".

De lo anterior se desprende que los documentos electrónicos tienen el mismo carácter declarativo y representativo del papel y poseen la misma consideración y validez de los documentos tradicionales. Por lo tanto, se debe poder garantizar su inalterabilidad no consentida, su accesibilidad, su estabilidad en el tiempo. Es decir, debe ser tanto más confiable que el documento de papel.

Hay algunas objeciones que consideran los documentos electrónicos como inseguros, pero los documentos de papel también lo son. Se pueden aplicar sistemas de seguridad que no existen en el papel, por ejemplo: la firma digital. La autenticidad de los documentos depende del emisor, no del soporte. En el caso de que se demuestre falsedad, carecerá de valor probatorio, igual que el papel.

Certificación digital

La "Dirección de certificadores de firma digital" pertenece al MICIT, tendrá carácter de órgano de desconcentración máxima y agota vía administrativa. Tendrá las funciones dadas en la ley y el reglamento, tendrá una jefatura y cuenta con el Comité Asesor de Políticas.

El Ente Costarricense de Acreditación (ECA) es el encargado de verificar la idoneidad técnica y administrativa, de acuerdo con los lineamientos técnicos del anexo del reglamento y los restantes requisitos que esa dependencia establezca.

Certificados digitales

Un certificado digital es un archivo electrónico, intransferible y no modificable que tiene un tamaño máximo de 2 *Kilobytes* y contiene una clave pública y un nombre. Habitualmente, también contiene una fecha de expiración, usualmente la validez es de dos años, el nombre de la autoridad certificante que la emitió, un número de serie y alguna otra información. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por su emisor.

Su formato está definido por el estándar internacional ITU-T X.509. De esta forma, puede ser leído o escrito por cualquier aplicación que cumpla con el mencionado estándar.

Gracias al certificado digital, el par de claves obtenido por una persona estará siempre vinculado a una determinada identidad personal y, si sabemos que el mensaje ha sido cifrado con la clave privada de esa persona, sabremos también quién es la persona titular de esa clave privada.

En síntesis, la misión fundamental de los certificados es permitir la comprobación de que la clave pública de un usuario, cuyo conocimiento es imprescindible para autenticar su firma electrónica, pertenece realmente a ese usuario, ya que así lo hace constar en el certificado una autoridad que da fe de ello. Representan, además, una forma conveniente de hacer llegar la clave pública a otros usuarios que deseen verificar sus firmas.

Usos de los certificados digitales

Se usan para asegurar la integridad y confidencialidad de la información, así como autenticar los interlocutores de las transacciones en los sitios web. En general, comprobar

la integridad de documentos transmitidos electrónicamente, asegurar la confidencialidad de la información contenida en dichos documentos, autenticar el origen de un mensaje recibido y autenticar el destino de un mensaje enviado.

Componentes de los certificados digitales

El certificado y la llave privada pueden ser almacenados en tarjetas inteligentes seguras y en *Tokens*. Los *Tokens USB* son una especie de llave maya que contiene las claves del usuario y se utilizan para proteger la llave privada y el certificado de un titular. Realiza las operaciones criptográficas internamente. Las llaves privadas nunca son expuestas y se usa un PIN o clave para identificar al titular.

Entidades certificadoras (EC)

Es el tercero de confianza que emite certificados digitales y está debidamente autorizada según esta ley o su reglamento.

En este momento, los certificadores se están inscribiendo en el Ministerio de Ciencia y Tecnología, para garantizar que esa relación entre el documento y la firma sea válida. Dentro de pocos meses se ofrecerán los primeros servicios al usuario.

Esos organismos, por ejemplo, un banco privado o un organismo público como el Tribunal Supremo de Elecciones, estarán entonces en capacidad de ofrecer certificados de firma digital bajo el control del Sistema Nacional de Certificaciones.

Aunque solo esas personas jurídicas autorizadas podrán dar certificados de firma digital al público, ni la ley ni el reglamento especifican si el sistema será gratuito; puede ser que solo se cobre el *Token* o que se cobre por ambos servicios.

Para brindar confianza a la clave pública, surgen las autoridades de certificación, que son aquellas entidades que merecen la confianza de otros actores en un escenario de seguridad donde no existe confianza directa entre las partes involucradas en una cierta transacción.

Las Autoridades de Certificación (CA) son las que vinculan la clave pública a la entidad registrada y proporcionan un servicio de identificación. A su vez, identificada por otra CA, se crea una jerarquía o árbol de confianza: dos entes pueden confiar mutuamente entre sí si existe una autoridad común que directa o transitivamente las avala.
Las Autoridades de Registro (RA) ligan entes registrados a figuras jurídicas y extienden la accesibilidad de las CA.

Las Autoridades de Fechado Digital (TSA) vinculan un instante de tiempo a un documento electrónico avalando con su firma la existencia del documento en el instante referenciado. Estas autoridades pueden materializarse como entes individuales, o como una colección de servicios que presta una entidad multipropósito.

Una vez que la identidad del individuo ha sido comprobada, se generan un par de llaves criptográficas y se crea un certificado digital, el cual se firma con la llave privada de la EC.

La validez de un certificado digital dependerá de la confianza que se tenga en su emisor.

Los requisitos legales para los certificadores están dados en el artículo 12 del reglamento y los requisitos técnicos, en el anexo técnico de reglamento, norma INTE/ISO/IEC 62:2000.

Sistema de pagos costarricense

Actualmente el sistema bancario comercial está formado por 3 bancos estatales, 16 bancos privados y 2 bancos creados por leyes especiales. Todas estas instituciones están integradas al SINPE. Las dos leyes principales que rigen al sistema bancario son la LOBCCR y la Ley Orgánica del Sistema Bancario Nacional (LOSBN). Adicionalmente, las entidades bancarias están sujetas a la normativa de la SUGEF y el CONASSIF. Con la reforma de 1995, particularmente los bancos privados ampliaron la gama de productos financieros que pueden ofrecer a sus clientes, con lo cual el sector bancario se volvió más dinámico y competitivo en los últimos años, aunque con claro dominio de la banca estatal.

Además de los bancos comerciales, otras instituciones que realizan intermediación financiera y que participan en el SINPE son las entidades financieras no bancarias, las mutuales y las cooperativas de ahorro y crédito. Estas entidades son supervisadas y fiscalizadas por la SUGEF. Las financieras son entidades no bancarias, las cuales son personas jurídicas constituidas como sociedades anónimas que realizan actividades de intermediación financiera, excepto aquellas que la ley reserva en forma exclusiva para los bancos, como la captación de depósitos en cuenta corriente o de ahorros. Las mutuales se originaron para fomentar el ahorro con el fin de recaudar recursos para financiar la construcción de viviendas. Las mutuales están facultadas para captar recursos en cuenta de ahorros y mediante certificados de inversión y solo pueden otorgar préstamos para vivienda. Los recursos que captan las financieras y las mutuales están sujetos al requisito de encaje mínimo legal. Por esta razón mantienen cuentas de reserva en el BCCR y deben estar enlazadas con el SINPE. Las cooperativas de ahorro y préstamo son asociaciones voluntarias de personas y no de capitales, con plena personalidad jurídica, de duración indefinida y de responsabilidad limitada. Estas entidades pueden captar en cuenta de ahorros y a plazo, pero no en cuenta corriente.

Los certificados digitales en los medios electrónicos de pago

Hace nueve años fue creado el Sistema Interbancario de Negociación y Pagos Electrónicos, SINPE. Es una plataforma tecnológica desarrollada y operada por el Banco Central de Costa Rica, que conecta a las distintas entidades del Sistema Financiero Nacional a través de una red privada de telecomunicaciones.

El SINPE ofrece a sus entidades, asociadas, y a los clientes de estas, las ventajas de pertenecer a una red de servicios financieros eficiente, con tecnología de avanzada, de bajos costos transaccionales, altamente segura y funcionando dentro de estándares internacionales de calidad, que la convierten en una opción muy competitiva para las personas y empresas que demandan los servicios de movilización de fondos en las entidades del Sistema

Financiero Nacional.

Actualmente están asociadas más de 65 instituciones, incluyendo todos los bancos privados y públicos de Costa Rica, todas las mutuales, las siete cooperativas más grandes del país, el Instituto Nacional de Seguros, la Caja Costarricense de Seguro Social , el ICE, la Junta de Protección Social, el Ministerio de Hacienda y el Instituto de Fomento y Asesoría Municipal (IFAM). Esta última institución inició el proceso de negociaciones con el Banco Central, el 5 de octubre del 2005.

El SINPE permite, entre otros servicios, que todas las transacciones se realicen en forma electrónica. Este sistema cuenta con idóneas características de seguridad que le ha permitido gozar de la confianza de todo el sector financiero nacional.

Los contribuyentes pueden hacer sus pagos en forma ágil, segura y eficiente, ya que no necesitarán visitar las oficinas de la municipalidad o de los bancos para realizar sus pagos por servicios e impuestos, con lo que, además de ahorrar tiempo, contribuirán al desarrollo de sus localidades.

Los requisitos de seguridad pueden variar ligeramente de un sistema de pago a otro, dependiendo tanto de las características propias del sistema como de la confianza que exista entre sus diferentes elementos. Así, un sistema de pago realizado en un entorno en el que las comunicaciones se realizan a través de una red de área local o metropolitana sin salir al exterior, no requiere el mismo nivel de seguridad que un sistema de pago en el que las transacciones se envían a través de Internet, pudiendo recorrer el mundo entero.

En cualquier caso, podemos decir que los requisitos de seguridad de un sistema de pago electrónico en general son los siguientes:

Autenticación

En todo sistema de pago los participantes del sistema deben demostrar que son los que dicen ser. Así, en un sistema de pago basado en tarjetas de crédito, el comercio comprueba la autenticidad de la tarjeta antes de proceder con el pago.

En el caso de tarjetas inteligentes con microprocesador, dotadas, por tanto, de una capacidad de cálculo, esto se realiza mediante algún protocolo criptográfico de autenticación, mientras que, en el caso de tarjetas con banda magnética, se realiza mediante una verificación visual de ciertos datos grabados en la superficie de la tarjeta, por ejemplo: hologramas, firmas, foto, etc.

En el caso de sistemas de pago basados en monederos electrónicos, es frecuente también que se produzca una autenticación del comercio ante el portador del monedero electrónico, debido al riesgo existente de creación de dinero falso en este tipo de sistemas. Para ello el terminal del comercio suele disponer de un módulo de seguridad, que en ocasiones es una tarjeta inteligente pero puede ser otro tipo de dispositivo, el cual almacena las claves y realiza los cálculos necesarios para la autenticación del comercio.

En los sistemas basados en tarjetas, se suele verificar también la asociación correcta de la tarjeta con su poseedor. Esto se realiza normalmente a través de números de identificación personal utilizando el PIN. Lo mismo ocurre en los sistemas de pago a través de redes donde se necesita una autenticación de la persona física que utiliza en un instante determinado el sistema.

La autenticidad del resto de agentes de un sistema de pago electrónico está normalmente garantizada mediante protocolos criptográficos de autenticación, actualmente basados en algoritmos de clave simétrica como el DES, pero que poco a poco están siendo remplazados por algoritmos de clave pública como el RSA con el fin de favorecer la interoperabilidad de los sistemas.

Integridad

Otro aspecto importante en todo sistema de pago electrónico es la integridad de los datos intercambiados entre los agentes del sistema, máxime cuando esos datos se refieren a importes de un pago, a un número de cuenta bancaria, etc. La integridad de las comunicaciones es garantizada mediante códigos de autenticación de mensajes (MAC), funciones, resumen y firmas digitales. En el caso de la relación entre cliente y comercio, esto solo es posible cuando el cliente está en posesión de un dispositivo con capacidad de cálculo y de almacenamiento seguro de claves, como es el caso de una tarjeta inteligente.

Además, es también importante salvaguardar la integridad de los datos almacenados en los dispositivos asociados a cada agente. Las claves criptográficas, los certificados, las listas negras, los datos para el intercambio de operaciones, etc. necesitan ser protegidos contra su alteración voluntaria o involuntaria. Esto se consigue de muy diversas maneras según el tipo de agente y según el dispositivo asociado a él. Así, por ejemplo, las claves criptográficas de clientes y comercios suelen almacenarse en tarjetas inteligentes y módulos de seguridad (SAM), respectivamente. Las listas negras en los comercios se verifican y renuevan periódicamente y los datos en los servidores de las entidades financieras que intervienen en el sistema de pago son almacenados en búnkers de seguridad que normalmente se encuentran duplicados para evitar las posibles pérdidas de información como consecuencia de posibles fallos.

Confidencialidad

Ciertos datos intercambiados durante una transacción de pago necesitan ser ocultados a la vista de todo el mundo, salvo para el agente al que van destinados dichos datos. Es el caso de la información asociada con la cuenta bancaria de un titular que se transmite a través de una red y que solo concierne al titular y a la entidad bancaria depositaria de dicha cuenta. También ciertos datos asociados con los bienes o servicios adquiridos son susceptibles de ocultación en cuanto a que pueden constituir datos sensibles que, en manos de terceros, pudieran causar un grave perjuicio directo o indirecto al cliente.

En ciertos casos se requiere que el pago se realice de forma anónima de tal modo que sea imposible, a partir de ciertos datos, elaborar una traza que permita descubrir el autor de un determinado pago. Estos sistemas requieren protocolos criptográficos más complejos cuando el pago se realiza a través de una cuenta bancaria, pues los datos del titular son almacenados en el momento de la autorización del pago o de la retirada de dinero, en el caso del monedero electrónico. Actualmente el anonimato es garantizado en todas aquellas transacciones que se realizan con dinero no ligado a una cuenta bancaria, como, por ejemplo las tarjetas de prepago en las cabinas telefónicas.

Prueba de la transacción

Cuando se produce una transacción electrónica en la que una cantidad de dinero se mueve de un agente a otro de la transacción, es necesario una prueba de ella que permita al pagado reclamar ese dinero y evite que el pagador reniegue del pago. Generalmente, el banco depositario de la cuenta del cliente el banco emisor debe pagar una determinada cantidad de dinero al banco depositario de la cuenta del comercio del banco adquirente por las transacciones llevadas a cabo en sus terminales. El banco emisor reclamará, entonces, una prueba de que dichas transacciones fueron efectivamente realizadas por titulares de cuentas de ese banco y por el importe reclamado.

La prueba de la transacción suele ser realizada por el cliente en los casos en que este dispone de un dispositivo con capacidad de cálculo (tarjeta inteligente, PC, etc.). Suele consistir en una firma digital realizada mediante algún algoritmo de clave pública con el fin de evitar el repudio de la prueba.

Gestión del riesgo y autorización

Otro aspecto muy importante a la hora de autorizar o no un pago es realizar una estimación del riesgo que supondría autorizar un pago fraudulento. Para ello, todos los agentes que intervienen en el momento de realizarse la transacción realizan un análisis de la situación en la que la transacción se produce con el fin de autorizar el pago o no. En este caso

tenemos dos situaciones bien distintas, según que la autorización se realice directamente por el banco emisor tras una conexión en línea con el comercio, o se realice por otro agente y sin conexión con el banco emisor (fuera de línea).

En el caso de autorizaciones en línea, el banco emisor puede verificar directamente la autenticidad del cliente, por ejemplo, mediante una verificación del PIN en los sistemas actuales de retirada de dinero con tarjeta en cajeros automáticos y puede consultar los datos de este, listas negras, saldo disponible, límites establecidos, etc., para autorizar el pago o no.

En el caso de autorizaciones fuera de línea, no se conoce exactamente la situación financiera del cliente, por lo que se tiene que realizar una estimación del riesgo basada en el análisis de algunos parámetros como, por ejemplo, el importe de la transacción, la procedencia (nacional, comunitaria, extranjera) del cliente, la consulta de listas negras actualizadas periódicamente por las diferentes entidades bancarias emisoras, etc. Normalmente este tipo de autorizaciones resultan mucho más económicas debido al ahorro en la llamada telefónica solicitando la autorización, pero conllevan un mayor riesgo y exigen, por tanto, unos protocolos criptográficos más robustos que permitan al comercio autenticar al cliente sin necesidad de consultar a su banco.

Disponibilidad y fiabilidad

Todas las partes implicadas en un sistema electrónico de pago requieren la habilidad para realizar o recibir pagos cuando sea necesario. Por otro lado, las transacciones deben ser atómicas, en el sentido de que o se producen satisfactoriamente o no se producen, pero no pueden quedar en un estado desconocido o inconsistente. Ningún cliente o comercio aceptaría una pérdida de dinero por culpa de un error en el sistema. La disponibilidad y la fiabilidad del sistema dependen de la disponibilidad y fiabilidad de los dispositivos y de las redes sobre las que se sustenta. La recuperación ante fallos requiere un sistema de almacenamiento estable en todas las partes del sistema y protocolos específicos de sincronismo.

Conclusiones y recomendaciones

Es indiscutible que las nuevas tecnologías de la información se presentan como una oportunidad inmejorable para que los países menos desarrollados o emergentes puedan achicar la brecha que los separa con los denominados países del primer mundo.

Es importante que las organizaciones de nuestro país ofrezcan un mejor nivel de servicios a sus clientes y simultáneamente reduzcan sus costos, aumentando su productividad y su competitividad en lo que hoy son mercados cada vez más globalizados y competitivos.

Los certificados digitales y la firma digital son instrumentos que permiten la adaptación a este nuevo paradigma socioeconómico-cultural, que posibilita la expansión del comercio dentro de esta nueva economía digital globalizada, rediseña las relaciones laborales y la interacción humana y, a su vez, en el ámbito administrativo o gubernamental, optimiza la eficiencia a un bajo costo, con intervención y participación de los ciudadanos, lo que importa dotar al sistema de una mayor transparencia, obtener la consecuente reducción del gasto público y restablecer la credibilidad en las instituciones democráticas, algo que debe garantizar todo Estado social de derecho.

La incorporación de la firma digital en Costa Rica promete grandes cambios en el quehacer nacional, por las ventajas que trae esta para la realización de negocios a través de Internet.

La firma digital no es un fin en sí misma, sino un medio; su utilización será progresiva y beneficiará a la administración, sector productivo y los ciudadanos. Implica un cambio en la forma de prestar y obtener los servicios. El límite en este tema será fijado por todos nosotros, el sector público y el privado.

La firma digital proporciona un amplio abanico de servicios de seguridad, que superan con creces a los ofrecidos en un contexto físico por el de las firmas manuscritas.

Por ser tan innovadora, muchas personas no entienden en qué consiste o la confunden con la firma manuscrita digitalizada. Pero lo cierto es que la firma digital se hace necesaria cuando se maneja información en el entorno electrónico.

Uno de los atributos de esta firma es ser única para quien la usa, es decir, que no puede haber una firma digital para más de una persona. Por lo tanto, quien debe cumplir con la firma de un documento electrónico debe obtenerla individualmente.

Puede decirse entonces que, para que los pagos a través de medios electrónicos puedan continuar desarrollándose y se consoliden definitivamente, es necesaria la implementación de una infraestructura adecuada que le permita sobreponerse a su peor enemigo, la inseguridad propia del medio por el que transita la información.

Finalmente, se puede decir que la masificación de la firma digital en nuestro país será solo una cuestión de tiempo y que pronto se incorporarán al sistema documentos como firmas de contratos, relación con proveedores, facturas electrónicas, entre otros.

Bibliografía

Busso, Carlos, *Firma digital*, Disponible en
http://www.emb.cl/gerencia/articulo.mv?sec=5&num=61&mag=1&wmag=14

Hess Araya, Christian, *Comentarios al dictamen legislativo sobre, proyecto de firmas electrónicas,* San José, Costa Rica, Mayo del 2005, Disponible en
http://www.hess-cr.com/secciones/dere-info/dictamenfirma.shtml

Hess Araya, Christian, *¿Y la firma digital?,* San José, Costa Rica, 18/05/2005, Disponible en
http://www.hess-cr.com/secciones/dere-info/nacion-050318firma.shtml

Hess Araya, Christian, *Retomar la agenda digital*, San José, Costa Rica, 2/04/2006, Disponible en
http ://www.hess-cr.com/secciones/dere-info/nacion-060402agenda.shtml

Hess Araya, Christian, *ODF y gobierno digital*, San José, Costa Rica, 25/06/2006, Disponible en
http://www.hess-cr.com/secciones/dere-info/nacion-060625opendocument.shtml

La firma digital en Costa Rica, San José, Costa Rica, 10/07/2006, Disponible en
http://www.empresas.co.cr/Articulos/Actualidad/La-firma-digital-en-Costa-Rica.html

La firma digital en México, Disponible en
http://www.arenotech.org/2005/actu_2005/firma_digital_en_mexico.htm

Lara S, Juan Fernando, *Listo reglamento que impulsará factura digital*, San José, Costa Rica, 25/09/2006, Disponible en
http://www.nacion.com/ln_ee/2006/septiembre/25/economia835642.html

Ley de Firma Digital y Certificados Digitales, San José, Costa Rica, Disponible en
http://www.conicit.go.cr/boletin/boletin4/ley.html

Ley de Certificados, Firmas Digitales y Documentos Electrónicos, San José, Costa Rica, 23/08/2005, Disponible en
http://www.micit.go.cr

¿Qué es la firma digital?, Argentina, Disponible en
http://www.pki.gov.ar/index.php?option=content&task=view&id=91&Itemid=102

Quijano Zapata, Milena, *Despega la firma digital en Colombia*, Disponible en
http://www.i-uris.com/Articulos/firma2.html

Ramos Suarez, Fernando, *La firma digital: aspectos técnicos y legales*, Disponible en
http://www.marketingycomercio.com/numero14/00abr_firmadigital.htm

Reglamento de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, San José, Costa Rica, 20/03/2006, Disponible en
http://www.micit.go.cr

Valverde García, Antonio, *Seguridad en los nuevos medios de pago*, Disponible en
http://www.iec.csic.es/criptonomicon/articulos/expertos30.html

Wikipedia, *Historia de la criptografía*, Disponible en
http://es.wikipedia.org/wiki/Criptograf%C3%ADa

REVISIÓN FILOLÓGICA DE FERNANDO DÍEZ LOSADA, filólogo