Resumen

Los avances de la tecnología han proporcionado el desarrollo de las empresas, preparándolas para estar atentas, enfrentar y acoplar los cambios en ellas mismas, tanto individual como organizacionalmente.

Actualmente, nos encontramos con una sociedad controlada por Tecnologías de Información, donde contamos con la información en la palma de la mano; y es por esta razón que los mecanismos de seguridad deben de ser los más aptos, confiables, potentes y seguros que podemos utilizar.

El artículo presenta La Firma Digital como el mecanismo encargado de brindarnos esa seguridad en niveles tales como autenticidad de usuarios y plataformas, integridad, disponibilidad y seguridad en los datos, y no repudio por parte del usuario y del sistema.

En el presente trabajo se estudiarán los puntos para la implementación de dicha tecnología en Costa Rica, desde una perspectiva, la cual es tanto gubernamental como tecnológica, y sobre todo analizando la orientación de nuestro país hacia un gobierno digital.

Palabras Clave:

Firma Digital / Seguridad Web / Mecanismos de Seguridad / Gobierno Digital / Documento Digital.

Abstract

The advances of the technology have provided the development of the companies, preparing them to be kind, to face and to connect the changes in themselves, individually and with the organization.

Nowadays, we have a society controlled by Information Technology, where we count with the information in the palm of the hand, and is therefore that the security mechanisms must be the most apt, reliable, powerful and safe we can.

The article presents the Digital Firm like the mechanism in charge to offer us that security at levels such as authenticity of users and platforms, integrity, availability and security in the data, and relation between user and of the system part.

In this article the points for the implementation of this technology in Costa Rica will be study, from a perspective, governmentally and technologically and mainly analyzing the direction of our country towards a digital government.

Keyword:

Digital Firm / Web Security / Security Mechanisms / Digital Government / Digital Document.

Universidad Latinoamericana de Ciencia y Tecnología

Facultad de Ingenierías

Escuela de Ingeniería Informática

Trabajo Final para optar por el grado de Licenciatura en Ingeniería Informática con énfasis en Redes y Sistemas Telemáticos

“Firma Digital: Seguridad en la red y sus beneficios para brindar confianza a los usuarios en sus transacciones y procesos en la web.”

Sustentante:

Rodolfo José Morales Vargas

Cédula: 2-0606-0096

Prof. Miguel Pérez

I Cuatrimestre

2008.

Índice

Introducción

Como todos sabemos, cuando surge un elemento, servicio o mecanismo nuevo, siempre existe un tiempo de conocimiento y exploración; la tecnología y la informática pasaron por dicho proceso ya hace varios años y su acogimiento ha sido exponencial; sin embargo, existen usuarios que por temor y por no perder la rutina siguen rechazando la utilización de esta herramienta tan poderosa.

Hoy con el Gobierno Digital a la vuelta de la esquina, sabemos que la informática pasa a ser parte de nuestras vidas de forma tal que ya no es necesario hacer largas filas en un banco para realizar una transacción, sino más bien ya podemos, desde nuestros hogares, efectuar el mismo procedimiento a través de la Web.

La preocupación de la mayoría de los usuarios es la seguridad de su información y más aún la seguridad de su dinero, esto aparte del desconocimiento de la herramienta. Pero ¿cómo brindarles confianza y tranquilidad a los usuarios para incentivarlos a la utilización y al acogimiento de la tecnología?

La firma digital es una técnica muy segura de autenticación de usuarios en sistemas digitales que refuerza el uso del nombre de usuario y la palabra clave, la cual potencia todas las ventajas ofrecidas por los sistemas a través de Internet.

Dicha técnica es un mecanismo tan robusto que verifica autenticidad en las páginas, seguridad en los datos por medio de cifrados y encriptaciones, y el no repudio en las transacciones o procesos llevados a cabo por medio de aplicaciones informáticas y en especial las realizadas a través de Internet. De igual manera hablamos de un método para accesar a los datos importantes y privados de nuestra empresa.

La firma digital es una herramienta que ya se está utilizando en distintos países y gracias a ellos logramos ver cuáles conceptos positivos y negativos visualizamos, de manera tal que podamos mejorarlos o evitarlos al implementarla en nuestro país.

La función de la firma electrónica puede verse como la firma manuscrita, que permite identificar al autor de un documento, y garantizar que su contenido no ha sido alterado.

La firma digital llega para garantizar en sus procesos, seguridad y confianza, a los usuarios, tanto personal como organizacionalmente, podemos mencionar que el tema es amplio, poderoso y que es el mecanismo más seguro de principio a fin, hasta el día de hoy, para validar identidades.

Firma Digital: Descripción, Conceptos y Funcionamiento

Para adentrarnos más en el tema, podemos entonces definir la Firma Digital como la legalidad de un documento digital; es decir, es un método de encriptación de los datos, donde se relaciona el documento con su *autor*, lo cual permite el no repudio por parte del usuario.

La firma digital garantiza la integridad de los datos, la autenticidad de páginas web, y el contenido de las mismas, siempre brindando seguridad de principio a fin.

Para explorar el tema, es necesario mantener bien claros los conceptos utilizados en el proceso de la firma digital, por ejemplo: cómo está compuesta ella en nivel de hardware, software y qué procesos se llevan a cabo dentro de la misma, además de la participación del firmante. Los términos para este proceso son:

- Encriptar: es un proceso para transformar datos privados a un código privado e incoherente para los demás.
- Desencriptar: es el proceso contrario a la encriptación, conversión del código privado a los datos propios y legibles ya sea por el dueño o por cualquiera.
- Criptografía: se entiende por criptografía, una forma de escribir información que se desee enviar de manera secreta (encriptar), cifrando el documento, y se dice que la única forma de desencriptarlo es por medio de una llave pública (contraseña) que solo deberían conocer el emisor y el receptor. El problema radica en que la llave no sea descubierta por un tercero, ya que, quien la posea, podrá leer los mensajes.
- Clave Pública: es un número primo de gran magnitud, el cual es utilizado para decodificar un mensaje que mediante una llave privada fue codificado. De igual manera la llave pública puede también codificar un mensaje.
- Clave Privada: la clave privada, al igual que la pública, es un número primo de gran magnitud, el cual es utilizado para decodificar un mensaje que fue codificado mediante una llave pública. La llave privada puede también codificar un mensaje. La llave privada está contenida en un *token* y esta es desconocida por todos, inclusive por su dueño.
- Certificado Digital: un certificado digital es un sello de garantía, el cual es entregado y administrado por una Autoridad Certificadora, la cual investiga, y valida al portador del mismo, y a su vez le entrega el *token* con la llave privada y pública.

- Hash: es el resultado de un algoritmo matemático, a través del cual se generan claves que representan un documento, de manera casi unívoca.
- *Token*: un *token* es un dispositivo electrónico que se le entrega a aun usuario que realiza servicios en la web, para facilitar el proceso de autenticación. Es un dispositivo pequeño, y existen distintos tipos de *tokens:* desde unos a los que se les ingresa una contraseña, hasta los que guardan datos biométricos.

Básicamente estos son los conceptos que juegan en la distribución de *tokens*, por ejemplo: en la utilización del mismo, cómo trabaja, qué procesos lleva a cabo y mediante qué algoritmos se desarrollan las claves que son utilizadas en el proceso.

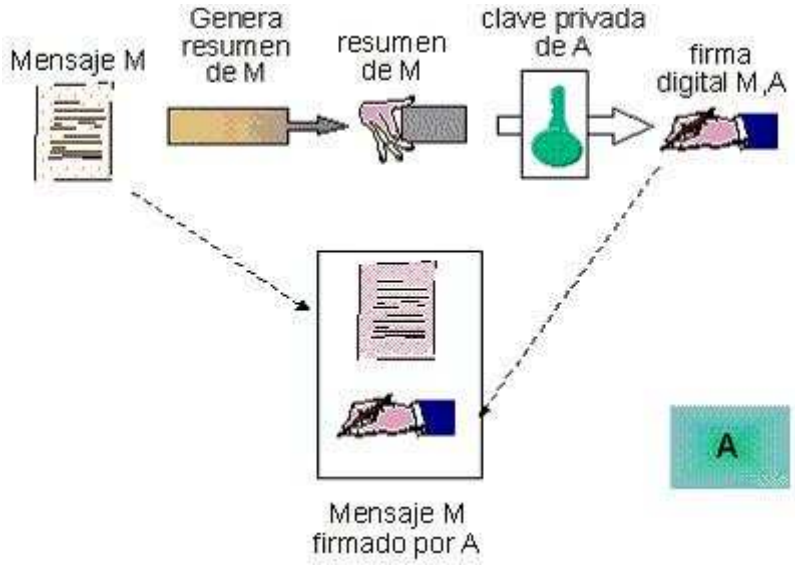
Al solicitar la firma digital, a la persona le es entregado un *token* y un certificado donde describe la funcionabilidad del mismo; así, un *token* puede ser utilizado en transferencias bancarias e inclusive en acceso a información confidencial de una empresa; hablemos de un dispositivo tipo *"llave maya"*, pero luego de que la Autoridad Certificadora haya estudiado y validado la entrega del *token,* al portador. El usuario por su parte tiene que solicitar el certificado previamente.

Para utilizar el *token*, debe ser insertado en una máquina, donde dentro del mismo tiene incorporado un software desarrollado por la misma Autoridad Certificadora, el cual se inicia con la solicitud de una contraseña, previamente definida por el portador. Un dato importante es que ambas claves; tanto la pública como la privada, se encuentran dentro del *token* y las mismas se hallan interrelacionadas entre sí; sin embargo, son desconocidas por el mismo portador.

Como se menciona en los conceptos, estas claves son números primos de gran magnitud, podríamos hablar de cientos o miles de dígitos. Desde el punto de vista virtual, la firma digital autentica tanto su contenido como la página a la cual se está accesando.

Figura # 1

Proceso de Encripción

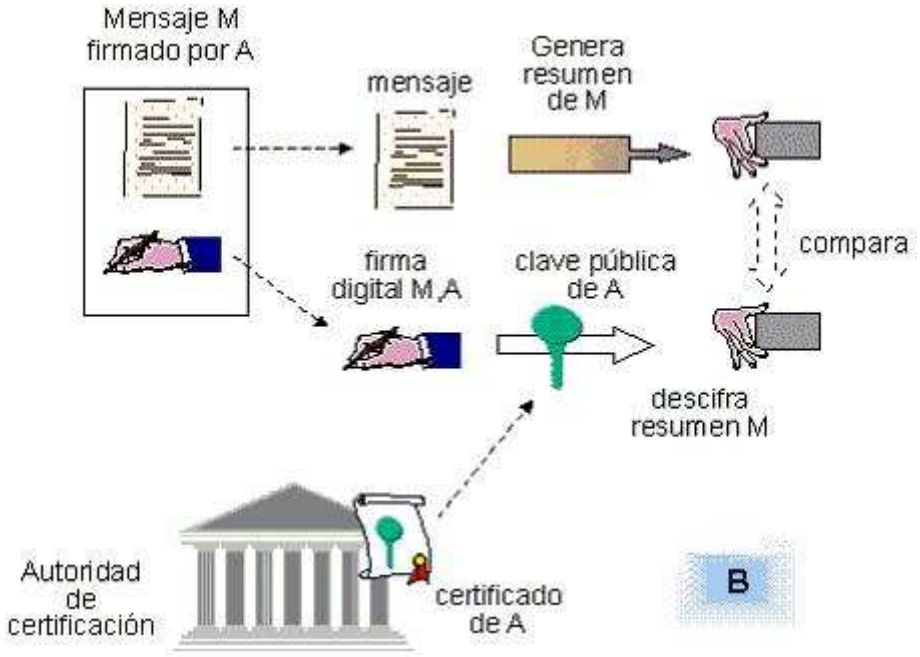


http://www.aecoc.es/web/Comercio.nsf/WPT/3F67B215152928F7C1257005003AA322?OpenDocument

El portador es dueño de la clave privada, de manera tal que le permite encriptar los datos por enviarse, y la clave pública es conocida por los remitentes o receptores y es administrada por la Autoridad Certificadora. Finalmente al paquete se le adjunta la firma y el mensaje.

Figura # 2

Proceso de Desencripción



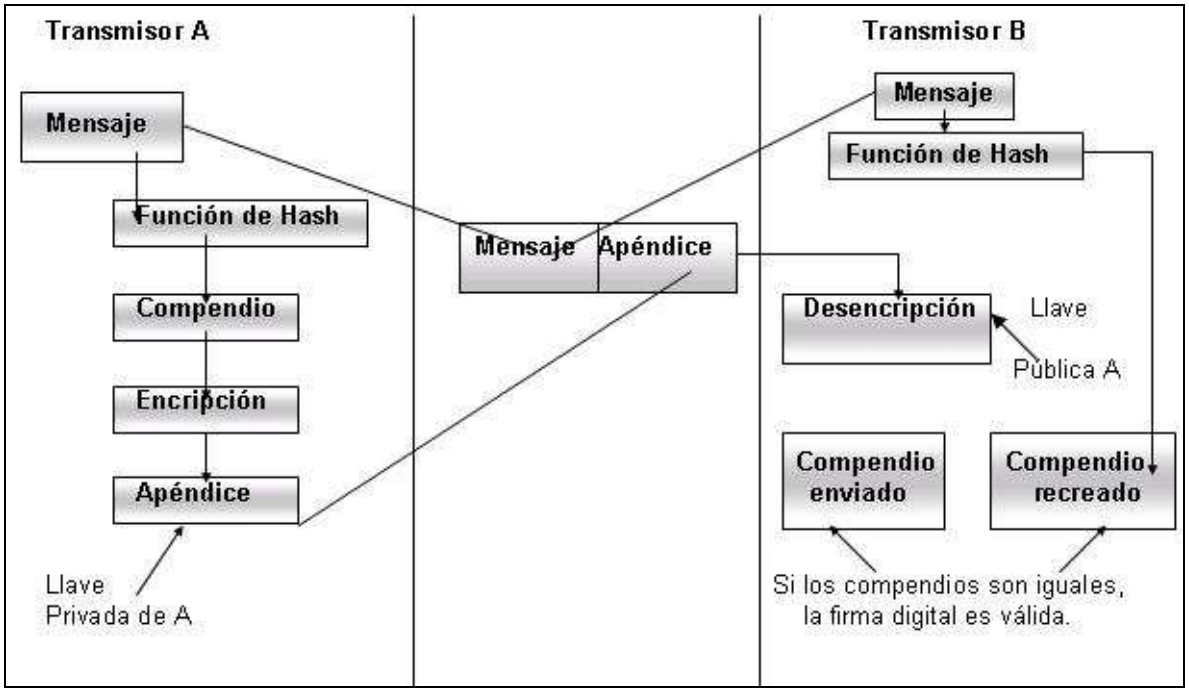
http://www.aecoc.es/web/Comercio.nsf/WPT/3F67B215152928F7C1257005003AA322?OpenDocument

El receptor al recibir el paquete, realiza dos procesos: primero, mediante la clave pública que es obtenida por el certificado digital del portador, se comprueba que la firma es correcta, y segundo, se utiliza la clave pública y la firma digital para obtener el hash del documento y le aplica el hash al documento recibido. Si ambos son iguales, entonces la firma es válida y se comprueba la integridad del mensaje.

Un punto importante es que la clave pública logra identificar la clave privada, sin embargo no puede deducirla, lo cual garantiza que nunca es revelada.

Figura # 3

Operación de la Firma Digital



http://www.monografias.com/trabajos43/administracion-redes/Image4964.gif

1. Transmisor A envía a Transmisor B el mensaje con la firma digital, resultado de aplicar su clave privada al resumen del mensaje (Mensaje + Resumen).
2. Transmisor B aplica la clave pública de Transmisor A y descifra el resumen del mensaje original.
3. Transmisor B aplica la función hash al mensaje recibido de Transmisor A y obtiene el respectivo resumen.
4. Si los resúmenes son iguales, Transmisor B puede estar seguro de que quien envía el mensaje es Transmisor A y que éste no ha sido modificado.

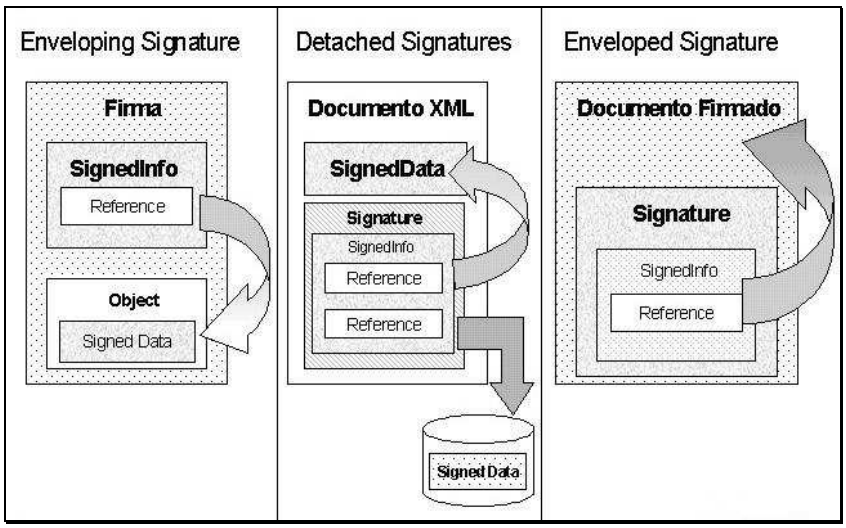
Tipos de Firma Digital

Cuando hablamos de firma digital, disponemos de 4 tipos; sin embargo, existen 2, que son los más reconocidos:

- **Firma Digital Simple:** autentica la identidad de la persona portadora del *token* y dueña del certificado digital o firmante; podríamos decir que es como un tipo de cédula electrónica, digital o virtual.
- **Firma Digital Avanzada:** no solo autentica la identidad de la persona portadora del *token* y dueña del certificado digital, sino también permite llevar a cabo transacciones avanzadas y contratos y garantiza integridad en los datos por medio del *PKI (Public Key Infraestructure)*. Se utiliza un método criptográfico para cifrar y descifrar el documento y éste debe ser validado por el ente certificador.
- **Firma Digital Reconocida:** tiene las mismas características que la firma digital avanzada, pero ejecutada con un dispositivo seguro de creación de firma (DSCF) y respaldada por un certificado reconocido, el cual es otorgado tras la verificación presencial de la identidad del firmante
- **Firma Digital Avanzada Certificada:** presenta de igual manera que la firma digital reconocida, las mismas características que la firma digital avanzada, con la diferencia de que el certificante se encuentra también acreditado.

Figura # 4

Escenarios de Firma Digital en XML



http://www.firmma.es/imagen/xmldsig.jpg.

Garantías de la Firma Digital.

- Autenticación de usuarios: la firma digital valida que el usuario es el portador del *token* y garantiza la identidad del emisor.
- Integridad de los datos: la firma digital garantiza la integridad de los datos desde el inicio del ciclo hasta la llegada de los datos al destino, al receptor, de manera tal que no puedan ser modificados por terceras partes.
- No repudio: el no repudio nos habla de ligar virtualmente al portador con la transacción que se realizó, es decir que el portador del *token* no puede negar una transacción.
- No repudio del sistema: en algunas ocasiones, el sistema puede generar un recibo de comprobación de que el portador realizó una transacción en específico.

La Firma Digital cuenta también con varias características:

- La firma se encuentra presente cuando llenamos formularios, para garantizar que los datos introducidos no van a ser sustraídos o modificados.
- Genera un recibo firmado digitalmente.
- Cuenta también con la opción de una bitácora de los movimientos realizados con el uso de la firma digital.
- Es fácil la unión con otra autoridad certificadora.
- Fácil integración con aplicaciones web.
- El uso de la firma digital no afecta el uso normal de aplicaciones web.
- Existen distintos tipos de *token*, algunos de ellos con un más alto nivel de seguridad; por ejemplo, traen incorporado autenticación por medio de huella digital y contraseña.

Seguridad de internet y firma digital.

PKI (Public Key Infraestructura)

Su nombre en español: Infraestructura de llave pública.

En informática, es un conjunto de componentes, que incluyen hardware, software, políticas y procedimientos de seguridad y un marco jurídico, que permite a una persona, organismo o servicio, validar y garantizar las operaciones criptográficas como el cifrado, y el no repudio a las transacciones.

El término PKI se utiliza para referirse tanto a la autoridad de certificación como al resto de componentes. La tecnología PKI en lo que llamamos firma digital, permite a los portadores autenticarse frente a otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes, firmar digitalmente información y garantizar el no repudio.

Otros usos de la tecnología PKI

- Autenticación de usuarios y sistemas.
- Identificación del interlocutor.
- Cifrado de datos digitales.
- Firmado digital de datos.
- Asegura comunicación entre el emisor y el receptor.
- Garantiza el no repudio.

Los componentes de la llave pública son:

1. **La autoridad certificadora:** encargada de entregar y anular certificados.
2. **La autoridad de registro:** responsable de verificar el enlace entre los certificados.
3. **Los repositorios de certificados y certificados revocados:** estructuras encargadas de almacenar la información relativa a la PKI. Se incluyen aquellos certificados que por algún motivo han dejado de ser válidos
4. **La autoridad de validación:** aprueba la validez de los certificados digitales.
5. **La autoridad de sellado de tiempo:** encargada de firmar documentos con el fin de probar que existían antes de un determinado tiempo.
6. **Usuario y entidades finales:** consiste en dos llaves: pública y privada, un certificado asociado a la llave pública y un conjunto de aplicaciones que hacen uso de la PKI.

Los elementos presentes en la infraestructura de la llave pública de acuerdo con el gráfico son:

Figura # 5

Infraestructura del PKI

http://www.eurologic.es/soluciones/que-es-pki.htm

- **Política de Certificación:** son aquellas políticas o procedimientos establecidos para el funcionamiento de la PKI; establecen los compromisos entre la autoridad certificadora y los portadores.
- **Aplicaciones PKI Habilitadas:** son aquellas aplicaciones de software capaces de operar con certificados digitales.
- **La Autoridad Certificadora:** proporciona confianza en la PKI y está conformada por elementos como hardware, software, y recurso humano.
- **Soporte de Clave Privada:** el soporte de clave privada son aquellas entidades que brindan un servicio para que los portadores protejan su clave privada
- **Publicación de Certificados:** permite a los usuarios operar entre ellos, y es un requisito legal que cuente con una total disponibilidad de acceso.

Criptografía Asimétrica

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

Criptografía Simétrica: es un método criptográfico que utiliza una misma clave para cifrar y descifrar mensajes. Tanto el emisor como el receptor deben comunicarse y elegir una misma clave, la cual les va a ser de utilidad para cifrar o descifrar el mensaje.

La criptografía asimétrica es el método criptográfico que utiliza dos claves para el envío de mensajes: una clave privada y una clave pública. El portador del token, posee ambas claves; la pública se puede entregar a cualquier persona, esperando que ésta sea un receptor, mientras que la privada debe ser conservada, guardada y protegida por el portador, de manera tal, que nadie tenga acceso a ella.

El portador de la clave privada cifra el mensaje por ser enviado y el remitente mediante la clave pública y unos algoritmos logra descifrar el mensaje para ser visto; la clave pública está ligada completamente a la clave privada, sin embargo, la clave pública nunca va a revelar la clave privada.

El principal fin por el cual se inventó la Criptografía Asimétrica fue para evitar por completo el intercambio de claves entre dos entidades, es decir, el emisor y el receptor deben conocer y utilizar la misma clave. Viéndolo desde otra perspectiva, ahora emisor y receptor no tienen por qué ponerse de acuerdo con una misma clave, ya que con el proceso asimétrico, utilizan claves distintas, pero siempre relacionadas entre ellas.

Algunas desventajas de la criptografía asimétrica son que cuanto mayor sea la longitud de la clave, mayor va a ser el tiempo de procesamiento de la transacción. Otra desventaja es que en comparación con la criptografía simétrica, las claves, tanto pública como privada, deben ser de mayor longitud. Y la última, pero no menos importante, es que el mensaje cifrado es de mayor tamaño que el mensaje original.

Algunos algoritmos utilizados en dicha tecnología son, DSS (Digita Signature Standard), PGP (Pretty Good Privacy), GPG, SSH (Secure Shell), SSL (Secure Sockets Layer), TLS (Transport Layer Security).

¿Cómo Trabaja Firma Digital?

Figura # 6

Función de Firma Digital en Procesos Comerciales

http://www.centrodeconocimiento.com/firmadigital/ejemplo.htm

Pasos de cómo funciona la firma digital en las empresas.

1. El comprador ingresan a la Internet
2. Da su firma, se confirma y se permite el acceso
3. Visualiza el catálogo
4. Se decide por un producto y pone la orden
5. El servidor ejecuta la orden
6. Se prepara pedido
7. Se transporta el producto
8. Se produce la entrega del pedido

Ventajas de la Firma Digital

1. Proporciona un alto grado, para no decir un máximo grado, de seguridad y confidencialidad en internet.
2. Identifica a las partes (emisor y receptor) que se conectan telemáticamente (Autenticidad).
3. Ofrece una gran y variada cantidad de servicios en el ámbito de la administración de los derechos de autor.
4. El procedimiento de verificación es exacto y es imposible su falsificación.
5. Portabilidad, es decir, que la firma digital puede ser utilizada en cualquier parte del mundo conectada a la red y sin necesidad de testigos.
6. Compatibilidad con dispositivos electrónicos actuales.
7. Verificación de las firmas y certificados.
8. En comparación con la firma manuscrita, elimina la pérdida de tiempo en procesos manuales de consulta de firmas.
9. Integridad de la transacción y su contenido.
10. No repudio por parte del usuario y del sistema.

Desventajas de la Firma Digital

1. La firma digital aún no es válida en muchos países, lo que conlleva a un rechazo de la tecnología.
2. La seguridad de la firma digital depende de la clave privada, y ésta puede comprometer la seguridad en los procesos en general.
3. El avance de la tecnología puede brindarnos una nueva firma digital más avanzada, de manera tal, que pueda comprometer algunos documentos.
4. Resulta vulnerable a un ataque web llamado *keylogger*, el cual puede ser por hardware o por software, donde el dispositivo o spyware captura sin autorización y secretamente todo lo que el usuario digita en la computadora y luego es enviado a un tercero.
5. Si el *token* no admite distintos certificados digitales de diferentes entidades certificadoras se puede dar el hecho de que los usuarios anden con “n” *tokens* en sus bolsillos.

Técnicas utilizadas en el fraude electrónico

En la actualidad existen numerosas formas, medios o técnicas de ataque; a continuación pueden visualizarse algunas:

- **Spoofing y phishing:** spoofing y phishing son muy similares y se refieren a la falsificación de documentos electrónicos. Spoofing es el delito de diseminar correos electrónicos modificados como para parecer que vienen de alguien quien no es el remitente original. Phishing, utilizado frecuentemente en conjunción con el spoofing, es la creación de un sitio web que sea idéntico al sitio web comercial original. Una vez en funcionamiento, el sitio web falso intentará que sus víctimas divulguen en él información importante como contraseñas, números de tarjetas de crédito y de cuentas bancarias. Las víctimas usualmente llegan al sitio copia a través de un enlace de un correo electrónico "spoofed".

- **Spam:** se define como la distribución ilegal de correos electrónicos no solicitados.

- **El timo del cheque falso:** se utiliza un cheque falso certificado, personal o corporativo, por una suma significativa para pagar mercancía, usualmente por una cantidad mucho mayor al precio de compra. Se le instruye a la víctima que deposite el cheque y regrese el cambio por transferencia bancaria, usualmente a un país extranjero. Debido a que los cheques certificados son respaldados por todas las instituciones, la víctima efectúa la transferencia bancaria con el cambio.

- **Fraudes con tarjetas de crédito o débito:** se define como el uso no autorizado de una tarjeta de crédito o débito para obtener dinero o mercancía de manera fraudulenta. Los números de estas tarjetas se obtienen de sitios web no seguros (cuyos urls no inician con "https://") o por sitios web que caen en la categoría phishing.

- **Robo de identidad:** este delito se da cuando un individuo se apropia de la identidad y la información personal de alguien más, sin su conocimiento, para cometer un robo o realizar un fraude. Los datos se obtienen en sitios web falsos de corporaciones o negocios legales.

- **Inversiones fraudulentas:** estos son anuncios en los cuales solicitan invertir en acciones o que prometen préstamos.

Firma Digital por Internet en Costa Rica

Es un proyecto que se establece con el fin de que los costarricenses podamos poseer la firma digital en nuestro medio. Tanto el Ministerio de Ciencia y Tecnología como el Banco Central están impulsando el proyecto. Todo esto con el fin de que los costarricenses poseamos un medio más seguro en Internet para poder realizar los diferentes trámites electrónicos.

Si un individuo, quiere adquirir el servicio de internet actualmente, éste deberá decidir entre las muchas tecnologías con las que cuenta el país, tarifas y velocidades, y de igual manera las nuevas y próximas tecnologías existentes en el mercado.

Entre las muchas posibilidades existen tarifas planas o de acuerdo con el consumo, o por ejemplo, si está dispuesto a instalar un equipo en su casa o si desea obtener el servicio por medio del teléfono, o inclusive si necesita obtener el servicio de internet inalámbrico. Estas son algunas de las tecnologías más conocidas y brindadas en conjunto por el ICE y Racsa.

Entre las tecnologías y servicios brindados por estas empresas nacionales están: ADSL (Línea de Abonado Digital Asimétrica), comúnmente llamado “acelera”, la cual ha tenido una gran aceptación por parte de los clientes y un vertiginoso crecimiento. Otro servicio con un potencial considerable es el servicio inalámbrico, por medio de la tecnología llamada WiMAX. Tenemos conexión los celulares y cable modem entre otros.

Se espera en los próximos meses de igual manera una nueva versión del servicio ADSL, llamado ADSL2+, el cual brindará un mayor ancho de banda; se espera alcanzar los 20 Mbps y va enfocado a un mercado de pequeñas y medianas empresas (PYMES).

Internet, como todos sabemos, es más que un medio de comunicación; ha adoptado la posición de un recurso facilitador y alentador al desarrollo tanto personal como industrial. Un aspecto importante es que los servicios brindados por estas entidades nos ofrecen una gran posibilidad de acceso a las tecnologías de la información.

Dados estos avances tecnológicos y nuevos servicios para conexión, se trabaja simultáneamente con los avances en el área de la seguridad web, lo cual se encamina hacia la firma digital.

En la firma digital, se genera un certificado que brinda la seguridad de que un individuo es el quien realiza el trámite y no otra persona que pueda suplantarlo. Los trámites realizados con la firma digital persiguen que ninguna persona pueda realizar trámites por individuos, esto con el fin de evitar robos o suplantación.

Esta nueva tecnología se utiliza como una tarjeta de crédito, que solo el propietario puede usar. Tiene la funcionalidad que necesita una contraseña para poder ser validada para todas las transacciones que realiza el dueño de la misma.

Por otro lado, se desea implementar el certificado electrónico para validar otro tipo de trámites que hacen las distintas personas en nuestro país, como por ejemplo: trámites bancarios, académicos, de gobierno, y otros. Esto último nos liberaría de la presencia física del individuo para poder realizar este tipo de actividades.

El Ministerio de Ciencia y Tecnología está trabajando en la capacitación de empresas que podrán ser capaces de dar certificados. Estos deben cumplir con una serie de estándares para poder validar la legitimidad de la firma digital.

Según un artículo publicado en La Nación el día 3 de marzo del presente año, *“Firma Digital reducirá inseguridad de banca en línea”,* el cual nos habla, de la implementación del proyecto y el estatus del mismo en nuestro país, y como éste brindará seguridad a usuarios que realizan trámites bancarios en la red.

Un punto para atacar por medio de esta tecnología es la vulnerabilidad que existe en el fraude electrónico, sin embargo, no se ha decidido si los bancos estarán obligados a acogerse al sistema; no obstante, no es un secreto que si alguno lo rechaza, perdería interés ante los clientes, esto debido a que los otros bancos contarían con mayor seguridad en sus transacciones.

Algunas entidades tales como el Banco Central, el Ministerio de Ciencia y Tecnología, el Tribunal Supremo de Elecciones y otros, esperan poner en práctica el proyecto a finales de este año, dado que la ley de Firma Digital se aprobó desde el año 2005.

Se dice que cada persona tendrá derecho a un certificado, el cual podrá ser utilizado en los sitios web. Los certificados serán emitidos por una entidad certificadora, que a su vez deberá cumplir con estrictas medidas de seguridad.

Luego de que el usuario realice el trámite de solicitud del certificado, éste deberá presentarse en la entidad certificadora y llevar su cédula y el *token* para su respectiva instalación. El costo del dispositivo oscila entre los $30 (unos ₡15.000) y es posible además un pago más, de bajo costo, por el trámite realizado.

INTECO, es la entidad encargada de la homologación de la norma ISO 21188, la cual establece los lineamientos y requisitos para garantizar la seguridad de las operaciones y transacciones financieras en línea por parte de las entidades certificadoras.

El Ministerio de Ciencia y Tecnología (MICIT), es un ente que juega un papel importante en la inmersión de esta tecnología, ya que es el órgano administrador y supervisor del sistema de certificación. El Banco Central también tiene participación en varias áreas, miembro del Comité de Política, y será el encargado de ofrecer el hospedaje de la raíz del Sistema de Certificación Digital y brindar el servicio a los usuarios.

El Ente Costarricense de Acreditación (ECA) tendrá la función de fijar los requerimientos técnicos para el estudio y evaluación de los interesados en fungir como certificadores registrados, de acuerdo con la *Ley N.º 8279*, y las prácticas y los estándares internacionales.

De acuerdo con todos los hechos mencionados previamente, es importante que el impulso de las comunicaciones y de tecnologías de seguridad robustas, brinden al usuario costarricense seguridad en sus transacciones o procesos en la web y que los incentiven al uso de las mismas. Es necesario continuar con la brecha digital, con el fin de que cada vez más costarricenses tengan acceso a las tecnologías de la información y la comunicación; así pueden utilizar el derecho que tienen de los servicios del Estado y de esta manera nos encaminamos, a un Gobierno Digital, donde los procesos que realizamos normalmente, en distintas entidades, los podamos efectuar sin ningún temor por medio de la web.

Conclusiones

Con base en lo visto en los temas anteriores, nos dirigimos al buen uso de las tecnologías de la información, dados los avances y las facilidades y comodidades que nos brinda la misma. Como en todo lugar siempre existen recursos que se oponen al cambio, sin embargo, en el mundo tecnológico en el cual vivimos es inevitable no adaptarse a las tecnologías actuales y venideras.

La tecnología de firma digital se ha utilizado en muchas aplicaciones, no obstante, en Costa Rica aún estamos en proceso de implementar esta herramienta. El marco jurídico refleja el poco respaldo que tiene la tecnología en nuestro país y esto recae en la jurisprudencia, dando a las personas jurídicas y también a las personas físicas, poco respaldo, al obligarse a implementar políticas estrictas.

Esto no termina aquí, la infraestructura física y lógica de las empresas públicas del país debe ser mejorada, ya que estas darán soporte y garantía a los usuarios finales de esta tecnología.

Sin embargo, si colocamos en una balanza las dos caras de la moneda, tanto los usuarios como los opositores, podríamos hablar de tener un mayor peso en los usuarios, y podemos ver el favorecimiento, la seguridad y la tranquilidad que brinda dicha herramienta.

La firma digital es actualmente el mecanismo más seguro en nivel de autenticación de usuario y proveedores de servicios, no repudio, tanto por parte del usuario como del cliente, integridad de la información de principio a fin y siempre contando con un máximo nivel de confidencialidad.

El desarrollo de las tecnologías de telecomunicaciones, desarrollo, prestación de servicios y soporte, y administración de base de datos han generado amplitud y facilidad de acceso a la información; y las nuevas formas de integrar el uso de Internet a la vida cotidiana hacen necesaria la implementación de nuevos mecanismos de seguridad como lo es la firma digital, los cuales garanticen la confidencialidad e integridad de los datos que circulan por la red y sistemas web, así como la identidad de sus emisores; es por esto que el mecanismo de firma digital es considerado como el más robusto de nuestro tiempo, el cual además cumple con todos los requisitos para brindar el más alto nivel de seguridad requerida.

Bibliografía

1. Aecoc. (2008). Aecoc GS1 Spain. Recuperado el 26 de Febrero de 2008, de http://www.aecoc.es/web/Comercio.nsf/WPT/3F67B215152928F7C1257005003AA322?OpenDocument

2. Capture the Advantage. (2000). Quadrem. Recuperado el 26 de Febrero de 2008, de http://www.quadrem.com/quadrem.asp?bid=6450

3. CEDIL, Centro de Documentación e Información Legislativa. (2001). Asamble Legislativa. Recuperado el 4 de Marzo de 2008, de http://www.asamblea.go.cr/biblio/cedil/temasbasicos/firmadigital/proyecto.htm

4. Costa Rica avanza hacia la Innovación Tecnológica. (2004). MICIT, Ministerio de Ciencia y Tecnología. Recuperado el 9 de Abril de 2008, de http://www.micit.go.cr/Noticias/foroinnovacion2007.html

5. Firma Digital. (1999). Notaría Digital. Recuperado el 26 de Febrero de 2008, de http://www.notariadigital.com/boletin015.htm

6. Firma digital reducirá inseguridad de banca en línea. (2008). La Nación. Recuperado el 4 de Marzo de 2008, de http://www.nacion.com/ln_ee/2008/marzo/03/economia1444077.html

7. INTECO NORMA FIRMA DIGITAL. (2004). MICIT, Ministerio de Ciencia y Tecnología. Recuperado el 9 de Abril de 2008, de http://www.micit.go.cr/ministra/discursoInteco.html

8. La Firma Digital. (2003). VirusProt, José de Jesús Ángel Ángel. Recuperado el 26 de Febrero de 2008, de http://www.virusprot.com/Art36.html

9. Marco Contextual Ley de Firma Digital y Certificados Digitales. MICIT. Recuperado el 4 de Marzo de 2008, de http://www.conicit.go.cr/boletin/boletin4/marco.html

10. MICIT recibió norma de firma digital: INCREMENTARÁ SEGURIDAD EN TRANSACCIONES EN INTERNET. (2004). MICIT, Ministerio de Ciencia y Tecnología. Recuperado el 9 de Abril de 2008, de http://www.micit.go.cr/firmadigital/entreganorma21188.html

11. Proyectos con menos papeleo. (2008). La Nación. Recuperado el 4 de Marzo de 2008, de http://www.nacion.com/br/2007/septiembre/22/suplemento-m1247660.html

12. Que es una PKI?. Eurologic. Recuperado el 26 de Febrero de 2008, de http://www.eurologic.es/soluciones/que-es-pki.htm

13. Wikipedia La Enciclopedia Libre. (2001). Jimmy Wales y Larry Sanger. Recuperado el 26 de Marzo de 2008, de http://www.wikipedia.com