Universidad Latinoamericana de Ciencia y Tecnología

Facultad de Ingeniería

Escuela de Ingeniería Informática

Trabajo final para optar por el grado de licenciatura en Sistemas de Información con énfasis en Redes y Sistemas Telemáticos

Tema: Firma digital y su estructura funcional en Costa Rica

Roberto Jara Corrales[1]
Cédula 1813-140

Profesor: Lic. Miguel Pérez Montero

Diciembre, 2006

[1] Bachiller de Ingeniería en Computación. Candidato a licenciatura en Informática, ULACIT. Correo electrónico: jaracr@bccr.fi.cr

Resumen Ejecutivo

La firma digital como herramienta informática a establecido niveles de seguridad, para llevar a cabo el traslado de información en formato digital a través de redes de acceso público, con un nivel de seguridad y que sido adoptado por muchos países.

En Costa Rica la firma digital es foco de discusión en los diferentes poderes, ya que se analiza la forma en la cual se reglamentará su uso; además, está por definir que organizaciones tendrían a su cargo la implementación y el control de la estructura que la soportará, puesto que ocasionaría un fuerte impacto sobre el procedimiento para tratar documentos de formato digital en Costa Rica.

El proceso de utilización de firma digital representa un gran paso, ya que permite establecer una fuerte cultura electrónica que involucra el hábito de acceso a Internet tomando en cuenta la seguridad e integridad de la información utilizando certificados digitales.

Descriptores

Firma Digital/Certificado/Internet/Integridad

Abstract

The digital signature is a computer tool designed to establish security levels in order to paste information in a digital format through public networks providing a level of security which has been adopted by many countries.

In Costa Rica, the digital signature is a focus of discussion among different authorities since its usage needs regulation. Besides, the decision of its control and implementation is pending, since it will cause a great impact in the way to manage digital format documents in Costa Rica.

The process of digital signature usage represents a milestone that provides a strong electronic culture involving Internet access practice that takes into account the security and completeness of using digital certifications.

Key Words
Digital signature/Certified/Internet/Integrity

Introducción

El crecimiento e implementación de redes (Internet) que tienen la posibilidad de unir dos lugares que geográficamente se encuentran separados, implica agregar seguridad en la transmisión de información mediante mecanismos de control que puedan proporcionar la suficiente confianza a los usuarios, para que sean utilizados con un rendimiento positivo de ganancias en las organizaciones lo cual hace más atractivo el uso de estos medios.

Por otro lado, el desarrollo de sistemas para la negociación de valores a través de enlaces públicos o privados introduce nuevos retos y comercializaciones donde no se ha llegado a implementar niveles de seguridad que se consideren óptimos. Dentro del mercado de las comunicaciones, y como tecnología emergente, se presenta la necesidad de garantizar el uso de una infraestructura de datos confiable y efectiva que, a su vez, cree un ambiente donde proveedores consideren su integración; de ahí nace la idea de utilizar cerificados digitales.

Dado lo anterior, el certificado digital surge a partir de los nuevos servicios digitales, que funcionan bajo un marco legal, según sean los lineamientos que rijan en el país donde se pretenda utilizar, garantizando estándares que permitan la calidad del servicio y una amplia implementación. Si a todo lo anterior se suma el fenómeno Internet, junto con el potencial de ahorro económico que este

tipo de tecnologías proporciona, el proyecto para utilizar certificados digitales se convierte en un tema de actualidad y estratégico para las organizaciones.

Este documento pretende analizar, desde un punto de vista funcional, la manera de operar la firma digital y los certificados digitales con el fin de obtener mejores conocimientos, además de investigar la forma en que se establece la estructura organizativa de firma digital en Costa Rica y la forma en que opera esta tecnología, basada en los reglamentos que le Gobierno de la República emita como requerimiento de funcionalidad.

¿Cómo funciona la firma digital?

Debido a que las tecnologías han permitido que la información sea enviada por redes de comunicación empresariales a lo interno y por redes internacionales hacia mercados mundiales (Internet), es necesaria una cultura de conciliación de los cambios que se producen debido a la desconfianza que se mantiene en relación con el trasiego de información por las diferentes redes, lo cual es factor que determina si una tecnología puede ser aceptada o no. Dentro de los productos que se han creado para solventar problemas de seguridad y confiabilidad, además de otros aspectos que, en un amplio sentido frenan el desarrollo tecnológico, nace una herramienta llamada firma digital. Esta se describe como la capacidad de aplicar componentes para encriptar información, de forma tal que asegure la identidad del autor de un documento digital y, si fuera necesario, evite que un documento pueda ser alterado.

Dentro de los requisitos para la utilización de la firma digital, se debe contar en primer lugar con un certificado digital, que es emitido por una entidad certificadora reconocida y de confianza para las partes involucradas y que garantiza seguridad en la emisión única de certificados. La firma digital basa su funcionamiento en un par de números, que son la clave privada y la clave pública, con una relación matemática entre ellos denominada *hash.* Esta función es la encargada de generar la huella digital, cuyo funcionamiento garantiza seguridad, ya que está cambiando en cada mensaje. Esto genera una huella diferente, y el resultado de todo ese proceso será la firma electrónica.

Ahora bien, en un certificado digital (como requerimiento), se pueden incluir los siguientes datos:

- Asunto para el que se ha creado el certificado.
- Emisor del certificado.
- Fecha efectiva y fecha de caducidad.
- Huela digital.
- Protocolo de seguridad.
- Tipo de encriptación. 40 ó 120 bits.
- Tipo de *hash.*
- Intercambio de claves.

El funcionamiento de la firma digital se puede describir de la siguiente manera: por ejemplo, dentro de un mensaje electrónico se establecen dos pasos que se

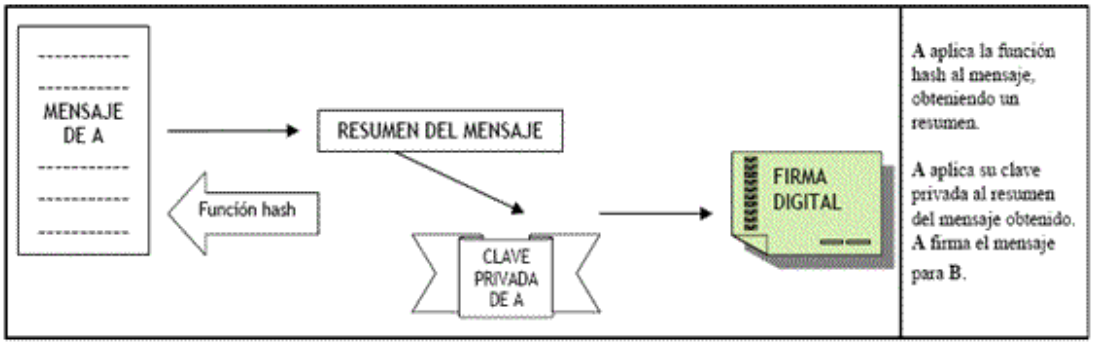
deben realizan en forma sucesiva: primero, la firma del autor del mensaje, y segundo, la verificación de la firma por la persona que recibe el mensaje. Todo este proceso de verificación permite la integridad del mensaje recibido, o sea, la adecuada seguridad al no poder modificarse su versión original (su autenticación), que equivale a la firma escrita a mano sobre el papel y el no repudio del origen, ya que el emisor no puede negar haber enviado el mensaje al haber sido creado por medios que sólo él controla y conoce. En otras palabras, en un documento electrónico el receptor aplicará la firma electrónica a los datos que ha recibido, o sea, la clave pública del autor con el fin de descifrarla; según la teoría, la huella (firma digital) debe ser igual a la huella del mensaje, lo cual garantiza la veracidad de la información.

Al analizar la evolución de los mercados a nivel comercial, se observa un fenómeno que viaja simultáneamente con la evolución de las tecnologías: la adaptación y la apertura de las organizaciones al sector tecnológico, en el sentido de que las organizaciones deben mantener actualizados sus equipos y procesos para mantener una economía que sustente su supervivencia y ofrezca a sus clientes los mejores mecanismos de seguridad y las medidas de protección más fiables para las transmisiones e intercambios por la red.

En la siguiente figura se representa el flujo que tiene la utilización de la firma digital.

Figura 1.

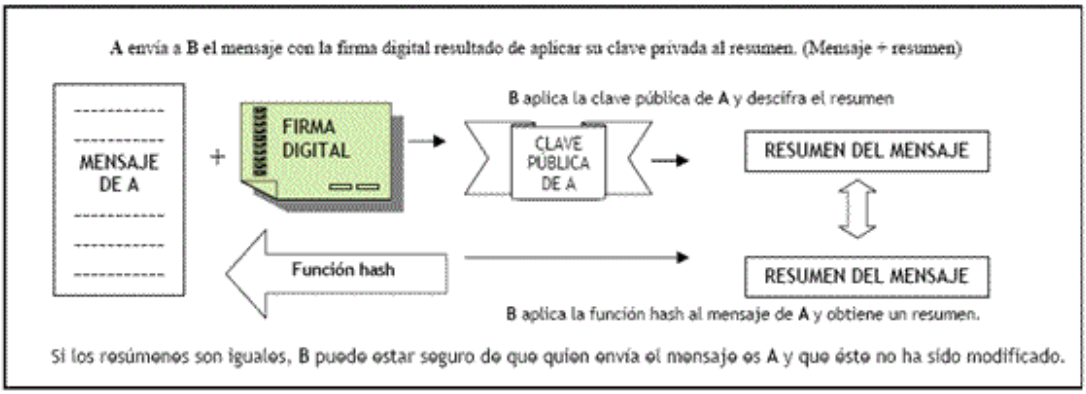
Primera fase de utilización de firma digital



Fuente: http://www.avogacia.org/w3/article.php3?id_article=1194

Figura 2.

Segunda fase de utilización de firma digital



Fuente: http: //www.avogacia.org/w3/article.php3?id_article

Autenticidad e integridad en la firma digital

Uno de los propósitos de la firma digital es sustituir el uso de cualquier sello, timbre, visto bueno u otra marca necesaria para identificar y validar un documento, como se ha hecho durante por muchos años en los escritos. En los documentos digitales se debe garantizar, de igual forma, la autenticidad e

integridad, dos factores de suma importancia que determinan la evolución de la firma digital debido a lo delicado de sus procesos. Estos factores garantizan la legitimidad y la rectitud de la información. Lo que se pretende con firma digital es que la información no sea modificada sin autorización durante todo el recorrido que ésta realice a través de las diferentes redes, tanto privadas como públicas. Por ello será necesario establecer mecanismos criptográficos adecuados para que la información no se degrade.

La autenticidad tiene como propósito comprobar irrefutablemente la identificación del autor tomando elementos como la identidad de la persona, su clave pública, el nombre de la autoridad certificante, la hora y la fecha de la creación del documento. Esto contribuye a evitar el repudio de la información y asumir consecuencias legales o de otra índole. Para ello se utiliza el certificado digital, con el que se pretende definir si un documento firmado digitalmente es auténtico. Dicho certificado digital, es emitido por una entidad denominada autoridad certificante (AC), que es la encargada de legitimar que una clave pública pertenece a una determinada persona o entidad. En general toda la información de las partes involucradas es validada por la autoridad certificante con el fin de asegurar la veracidad de la información.

La integridad implica comprobar que no se ha producido manipulación alguna en los mensajes originales y garantizar que lo que se ha enviado es lo que se recibe. Esto se logra aplicando métodos sofisticados como el algoritmo *hash* (se refiere a una extracción de datos que se toma de un mensaje y se envía a un

destinatario en forma electrónica, teniendo por objetivo verificar, por ejemplo, la inalterabilidad de un documento).

Tomando en cuenta los factores anteriormente mencionados, es importante señalar que, a diferencia de las firmas manuscritas, las firmas digitales que son generadas por una persona son diferentes entre sí, con el fin de asegurar la integridad de la información. En otras palabras, la firma digital cambia por cada documento firmado, según estro, la firma digital cumple con tres funciones de la firma manuscrita:

- La función *indicativa*, en virtud de la cual una firma revela la identidad del autor de un documento.
- La función *declarativa*, por medio de la cual se entiende que una firma implica la aceptación por parte del autor del contenido del documento.
- La función *probatoria*, que permite vincular jurídicamente un documento con su autor, para efectos demostrativos.

¿Qué es un certificado digitale y con qué fines nacen?

Es un requerimiento de utilización para la firma digital; consiste en un archivo electrónico que tiene un tamaño máximo de 2 Kb y contiene datos de identificación de una persona o entidad que emite información a través de un medio electrónico (Internet) de transmisión que contemple amenaza o riesgo de modificación de la información original, dentro del certificado digital se

encuentran datos del autor de la información que se transmite, como por ejemplo:

- Una Llave Pública.
- Información del dueño del certificado.
- Información del emisor de ese certificado.
- Periodo de validez.
- Un identificador único.
- La Firma Digital del emisor.

Un certificado digital es un documento electrónico que relaciona una identidad con una llave pública, la cual posee un tiempo de funcionamiento medido en horas o días, una vez transcurrido dicho tiempo, se deberá renovar. En el caso de que se llegara a perder el certificado digital, no se tendría la capacidad de probar la identidad. Por lo tanto, existen causas por las cuales el certificado se deberá renovar con anterioridad a su fecha de expiración; por ejemplo, cuando la clave privada ha sido conocida por terceras personas no autorizadas, o bien se ha extraviado, o se tienen sospechas de que está siendo utilizada en forma incorrecta; además de estos aspectos, se debe tomar en consideración que la llave privada puede perderse o puede ser copiada, por lo que debe protegerse.

Como se ha indicado, por medio de un certificado digital se obtienen un par de claves (privada y pública) para cifrar y descifrar los mensajes de forma tal que permita tener la certeza de que el mensaje recibido y descifrado con la clave pública haya sido enviado por la entidad que posee la llave privada capaz de

cifrar la información y que no haya sido alterada. El certificado digital se utiliza para verificar si una llave pública pertenece a una entidad, Para esto se apoya en información emitida por un tercero de confianza (similar a una cédula de identidad, que es respaldada por una entidad de confianza), y se comprueba la posesión de la llave privada correspondiente a la llave pública contenida en el certificado.

Desde que nuestros antepasados descubrieron la escritura, las generaciones han experimentado la necesidad de establecer en sus escritos la identificación de quien o quienes los generaban. Con el pasar el tiempo y la evolución de las nuevas tecnologías que ayudan a realizar de forma más ágil y rápida textos y documentación, se ha hecho necesaria la creación de nuevas tácticas para autenticarlos, siendo su finalidad el establecer un autor que asuma la responsabilidad.

La firma digital se puede definir como un conjunto de datos adicionados a un mensaje de formato digital que permite garantizar la identidad del autor y la integridad del mensaje. La firma digital conlleva algunos puntos que son importantes a la hora de entender el proceso de estampar el sello, garantía para la autenticación del mensaje o documento:

- El autor genera, mediante una función matemática, una huella digital en el mensaje.

- Esta huella digital se encripta con la clave privada del autor firmante, y el resultado es lo que se denomina firma digital la cual se enviará adjunta al mensaje original.

De esta manera el autor adjunta al documento una marca específica y única que solo él es capaz de producir, por otro lado, el receptor del mensaje comprueba que este no fue modificado desde su creación y que el autor es quien dice serlo a través del siguiente procedimiento: se genera la huella digital del mensaje recibido, luego se desencripta la firma digital del mensaje utilizando la clave pública del autor y se obtiene la huella digital del mensaje original. Si en la comparación de las partes involucradas coincide la información de autenticación, se deduce que el mensaje no fue alterado y que el autor es quien dice serlo.

Expuesto lo anterior es fácil deducir que la firma digital nace como el mecanismo para sustituir la tradicional documentación impresa por un documento electrónico, donde se emplee una clave secreta o privada (que sería la analogía con la cédula de identidad), además a través de la encriptación, se garantiza la autenticidad e integridad de la información implícita dentro de una firma digital; igualmente, sirve para verificar si el documento o mensaje es enviado al destinatario, quien puede descodificar la firma digital y confrontar el resultado con el texto original y comprobar que no ha sido alterado.

Hess Araya (2001) explica lo siguiente sobre la firma digital “Firmar digitalmente un documento electrónico tiene, entonces, dos propósitos centrales: garantizar

su autenticidad, probando fehacientemente no solo quién es el autor, sino eventualmente la hora y fecha precisas de su redacción, contribuyendo así a evitar una posible repudiación de sus consecuencias legales o de otra índole, y garantizar su integridad ya que garantiza que el contenido del documento no ha cambiado desde su firma"

¿Cómo utiliza un usuario la firma en un correo electrónico?

Como se ha comprobado, la transmisión de la información a través de redes públicas no es lo suficientemente segura como para garantizar que los datos no son leídos por personas no autorizadas. En Internet, un correo electrónico es como una tarjeta postal sin sobre, que puede leer todo el que tenga interés; por lo tanto, lo que se necesita es pone6rle ese sobre para evitar que sea leída. Esto se puede lograr a través de técnicas criptográficas que nacieron de la necesidad de mantener la privacidad en el manejo de una gran cantidad de información (personal, financiera, comercial y tecnológica) que se almacena en bases de datos y se transmite a través de las redes. Lo que se busca es que el contenido de un correo electrónico pueda enviarse encriptado, permitiendo así que sólo el receptor correcto del correo tenga la capacidad de abrirlo y leerlo.

La forma en que un mensaje electrónico hace su recorrido (figura 3) a través de una red utilizando la técnica de firma digital hace que se forme todo un protocolo de movimientos. En principio, basta cifrar el documento con una clave privada para obtener seguridad, puesto que nadie, excepto el transmisor, conoce dicha

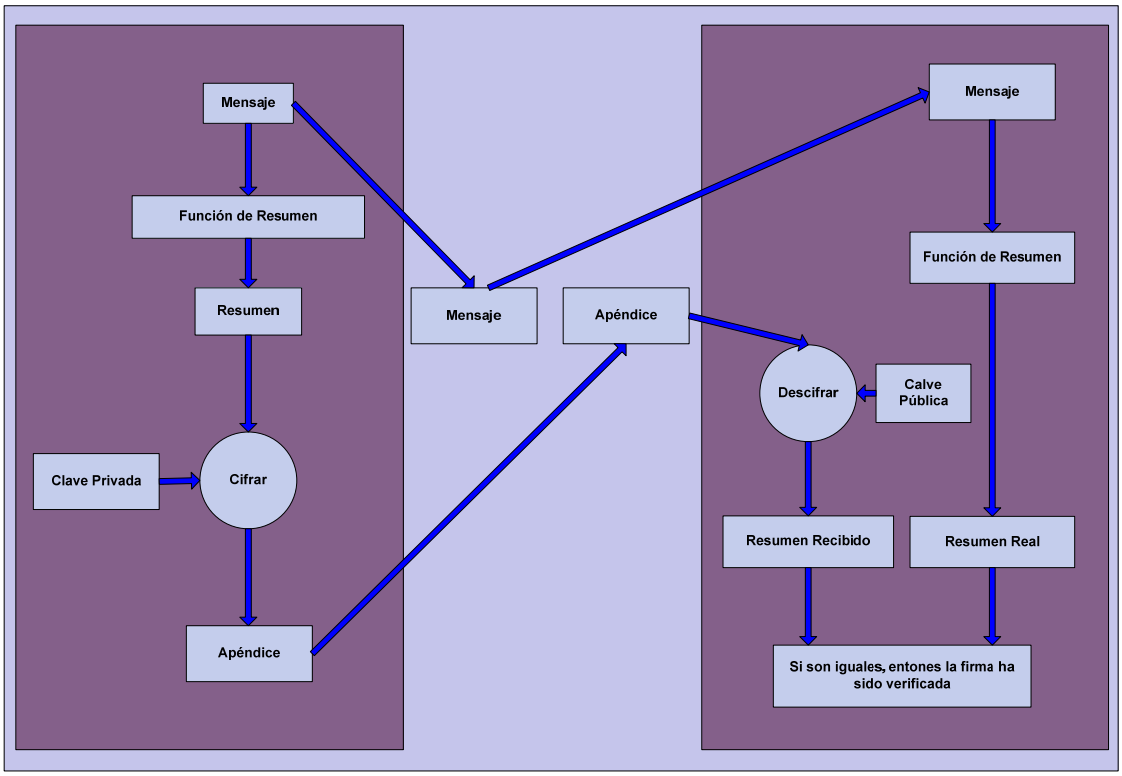
clave y, del otro extremo de la comunicación, cualquier persona podría descifrar el correo electrónico siempre y cuando posea la clave pública, manifestándose así la identificación del signatario.

Para los casos de los correos electrónicos extensos, los protocolos de firma digital utilizan funciones unidireccionales de resumen (*hash*), que tienen como objetivo hacer un resumen del documento original, que es firmado.

En la siguiente figura se describe el recorrido que hace un mensaje aplicando el procedimiento descrito para verificar la integridad.

Figura 3.

Funcionamiento de utilización de firma digital



Fuente: http://www.kalysis.com/hardware/mei/index.htm

1) El transmisor genera un resumen del documento.
2) El transmisor cifra el resumen con su clave privada, firmando por tanto el documento.
3) El transmisor envía al receptor el documento junto con el resumen firmado.
4) El receptor genera un resumen del documento recibido del transmisor, usando la misma función unidireccional de resumen. Después descifra con la clave pública de A el resumen firmado. Si el resumen firmado coincide con el resumen que él ha generado, la firma es válida.

De esta forma se ofrecen conjuntamente los servicios de no repudio (ya que nadie, excepto A, podría haber firmado el documento) y de autenticación (ya que si el documento viene firmado por A, se puede estar seguro de su identidad dado que sólo él ha podido firmarlo. Asimismo, mediante la firma digital se garantiza la integridad del documento, ya que, en caso de ser modificado, resultaría imposible hacerlo de forma tal que se generase la misma función de resumen que había sido firmada.

Ahora bien, como se ha descrito, el procedimiento de utilización de las llaves (pública y privada) es relativamente sencillo, para lo cual las personas involucradas necesitan portar siempre un dispositivo electrónico fácil de manipular y que sea compatible con los equipos computacionales existentes.

Descripción de los dispositivos más utilizados para portar las llaves en forma segura

Tokens USB: Parecido a un dispositivo USB de los utilizados para transportar información, más conocido como “llave maya”

Figura 4 .

Token USB

Fuente: http://www.kalysis.com/hardware/mei/index.htm

- *Tokens* Biométricos: Combina un módulo sensor de huella dactilar, un módulo de verificación de huella dactilar y un *token* USB.

Figura 5.

Token USB

Fuente: http://www.kalysis.com/hardware/mei/index.htm

- Tarjeta inteligente: Dispositivo que está compuesto de dos partes: un lector y una tarjeta donde está grabada la información, lo cual es una

desventaja, ya que se requiere tener los dos dispositivos para su utilización.

Figura 6.

Token USB

Fuente:http://www.kalysis.com/hardware/mei/index.htm

¿Qué es una entidad certificadora y de que manera operarán los certificados digitales sobre la tecnología de transporte de información?

Para que se dé un acuerdo de confianza dentro del proceso de transporte de información a través de redes como Internet, es necesario establecer un punto estratégico en común, una entidad de confianza, la cual estará reconocida como tercera parte confiable; es decir, un certificado digital es un documento electrónico que relaciona una identidad con una llave pública. Esta entidad funciona como árbitro de las comunicaciones es reconocida por sus siglas AC (autoridad certificadora) y es la encargada de firmar los certificados que poseen tanto las llaves privadas como públicas del emisor y del receptor.

Por ser una de las partes que integran el proceso de firma digital, y como parte fiable que garantiza la liga entre la clave (firma) y su propietario, funge como un abogado electrónico que valida y certifica la firma de una forma muy parecida a como lo haría un notario público que extiende un certificado reconocido legalmente para garantizar la autenticidad de la información, sumado a lo anterior, y por razones de seguridad, los certificados electrónicos poseen un periodo de validez, es decir, un certificado es tomado de igual forma que una cédula emitida por el Tribunal Supremo de Elecciones, ya que este es un principio básico en la emisión de cualquier tipo de identificación.

Todo este proceso de certificación parece un poco complicado a la hora de describirlo en papel, pero es todo lo contrario: cuando se aplica en la práctica, es totalmente transparente para las personas que lo utilizan. Esto da como resultado el crecimiento de la economía digital y el comercio electrónico, que dependen en forma directa de la capacidad para garantizar la seguridad mediante mecanismos como la firma electrónica y la criptografía.

Los componentes principales de un certificado digital son:

- Una llave pública.
- Información del dueño del certificado.
- Información del emisor de ese certificado.
- Periodo de validez.
- Un identificador único.
- La firma digital del emisor.

Jerarquía nacional de certificación

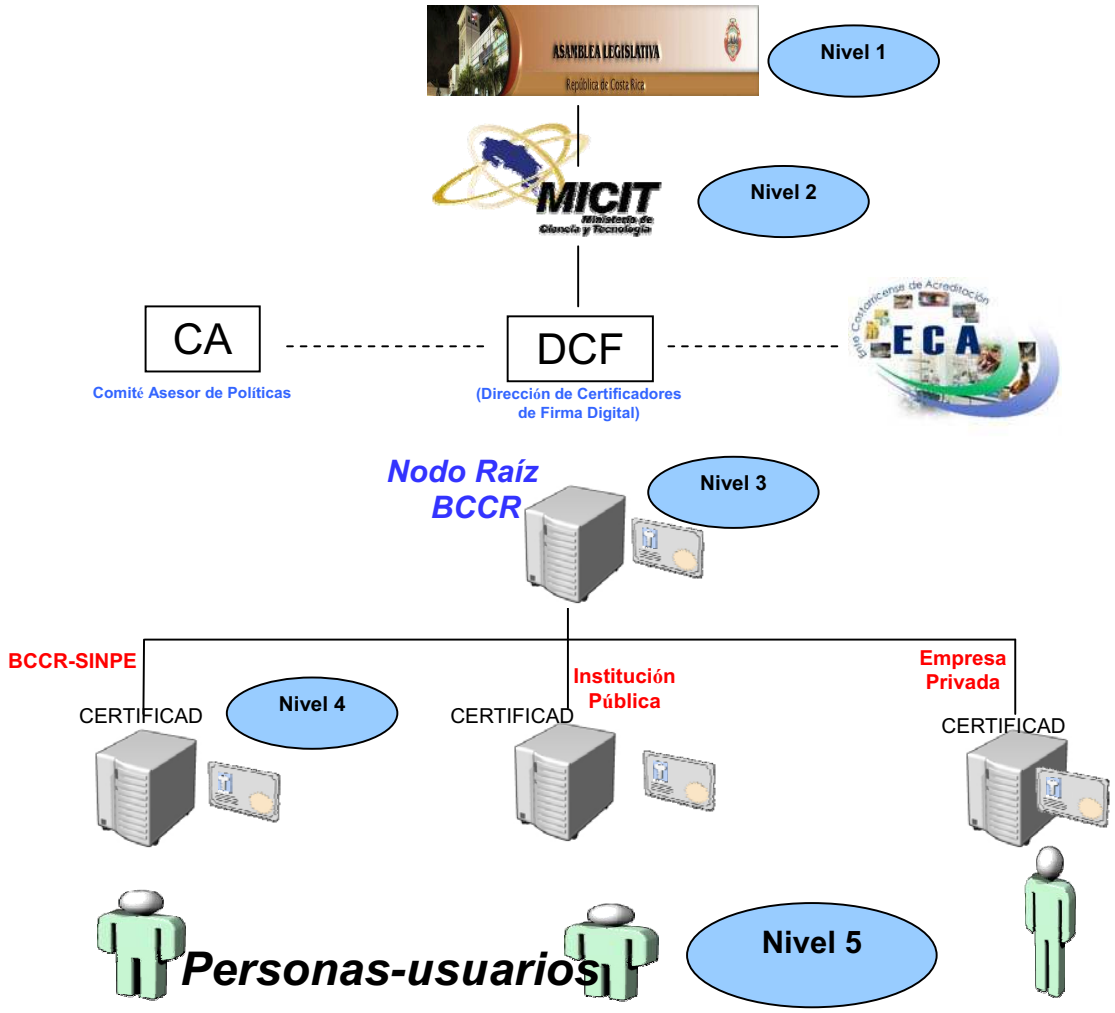
La estructura jerárquica nacional aún no esta bien definida, puesto que Costa Rica está iniciando su incursión en el campo de la firma digital; sin embargo, se está planteando utilizar un enfoque y una estructura que ya se haya probado en otros países donde se hayan obtenido resultados positivos con el fin de evitar las pruebas de investigación, donde actualmente ya se tiene establecido el la ley n° 8454 la cual poseerá el carácter y la jerarquía de reglamento general.

Respecto a la infraestructura donde la forma digital estará trabajando, el Banco Central de Costa Rica (BCCR) planteó, la opción para la implementación del sistema de la firma digital y la plataforma que soportará la infraestructura (figura 7). En lo que respecta al lugar donde se ubicarán la autoridad certificadora (AC) y sus posibles nodos de distribución, este planteo se visualiza la implementación del proyecto desde diferentes niveles, donde se puede definir un mecanismo de funcionamiento en forma clara.

A continuación se describe y detalla los aspecto que consideran los niveles que formarán la estructura:

Figura 7.

Distribución de la estructura de conexión del nodo raíz



Fuente: Relaciones del Sistema de Pagos con el Gobierno Digital

En un primer nivel se encuentra la Asamblea Legislativa, que establece los lineamientos legales dejando bien definida la infraestructura tecnológica a utilizar, y un marco jurídico claro, ya que se pueden presentar discusiones a las malas interpretaciones en lo que respecta a las leyes si quedaran mal redactadas o bien definidas en forma muy general.

La ley para el control y reglamentos de firma digital fue presentada el 30 de agosto del 2005 con el número 8454 y se titula *Ley de certificados, firmas digitales y documentos electrónicos*.

En un segundo nivel se encuentra el Ministerio de Ciencia y Tecnología (MICIT), dará fortalecimiento a la Dirección de Certificadores de Firma Digital; además, se encargaría de gestionar estrategias para establecer un programa que motive y aumente la utilización de medios electrónicos y que apliquen en el fortalecimiento del proyecto de firma digital.

En el tercer nivel se encuentra la ubicación del nodo raíz, que, para mejor entendimiento, es la autoridad certificadora, encargada de almacenar los certificados, o sea, es la entidad en la cual las partes que conforman (emisor y receptor) el proceso de utilización de la firma digital deben confiar para asegurar su validez según sea el tiempo de vigencia de los certificados. Del nodo raíz dependen las autoridades certificadoras, que vendrán en un cuarto nivel.
Para este nivel el Banco Central de Costa Rica (BCCR) propone colocar el nodo raíz en sus instalaciones, de forma tal que, además, se utilice su plataforma tecnológica como carretera de comunicación, sumado esto a que actualmente hay una conexión ya establecida con una cantidad importante del mercado del sector financiero de Costa Rica, De esta manera se garantiza aún más que con el proyecto de firma digital las diferentes entidades financieras posean una cultura electrónica, disponibilidad de medios, hábito de acceso a Internet,

importante preocupación por la seguridad de estar conectadas a Internet y, como punto final, que este sector financiero esté dispuesto al cambio. Teniendo en cuenta los factores mencionados, se establece un convenio publicado en el Diario Oficial La Gaceta Nº 101 del 26 de mayo de 2006, donde el Ministerio de Ciencia y Tecnología (MICIT) establece que el hospedaje y la operación del nodo superior del Sistema Nacional de Firma y Certificación Digital será en el BCCR, y el MICIT será la autoridad responsable de administrar y supervisar ese sistema por medio de la Dirección de Certificadores de Firma Digital (DCFD).

En un cuarto nivel se establecen las entidades autorizadas por el nodo raíz (BCCR), lo cuales brindarán el servicio de firma digital a sus clientes. Estas entidades serán valoradas por el BCCR con el fin de asegurar que cumplan con una serie de requisitos que garanticen su correcto funcionamiento, acordes con los lineamientos establecidos en la ley 8454. En este mismo nivel el BCCR se autonombra autoridad certificadora, de tal manera que pueda emitir certificados para firma digital.

Como quinto y último nivel se encuentran los usuarios, quienes a través de un dispositivo de almacenamiento electrónico hacen uso de la firma digital. Sin embargo, también en este nivel se colocan las autoridades certificadoras que, por razones de fuerza mayor (llámense ubicación geográfica) tengan que emitir una cantidad considerable de certificados. En otras palabras, se plantea delegar

la facultad de emitir certificados siempre y cuando se cumplan requisitos de funcionamiento que garanticen la integridad de la información.

Consideraciones para utilizar la firma y el certificado digital

Puesto que la utilización de la firma digital está dirigida hacia el uso del correo electrónico y el comercio a través de Internet, es necesario establecer criterios claros sobre los posibles riesgos que representa el estar conectado a esta red, debido a que no se tiene conocimiento de los elementos negativos que pueden afectar a las organizaciones. Por tanto, es necesario tener consideraciones bien definidas sobre la seguridad, como, por ejemplo, los certificados digitales.

Gigli (2006), explica que en Costa Rica “a partir del 2007 los costarricenses pueden utilizar la firma digital para garantizar sus trámites hechos en Internet. El certificado digital es un instrumento con el cual las personas pueden garantizar en sus trámites hechos en Internet que ellos son quienes dicen ser, es decir evita el suplantamiento, uno de los problemas más grandes que hay en transacciones en la red. Se usan como una tarjeta de crédito, que contiene información del dueño y que puede ser usada sólo por él, ya que necesita una contraseña, firma o fotografía para identificar al propietario. Un certificado digital puede usarse para hacer pagos en instituciones bancarias, trámites de gobierno, académicos, comerciales, en fin... una gran gama de actividades que de otra manera necesitarían de la presencia física de la persona interesada”.

Así las cosas, dentro de los aspectos a considerar en la utilización de la firma digital, deben incluirse y establecerse estándares de seguridad que hayan sido acreditados a nivel internacional, puestos a prueba bajo rigorosos mecanismos que verifiquen, para el caso de la firma digital, que la identidad de la persona que firma es única y confiable.

Aspectos importantes para el uso de firma digital:

- Habilitar protección segura de claves privadas.
- Establecer el nivel de seguridad alto.
- Tener conocimiento de cómo instalar un certificado digital.

Conclusiones

Debido al funcionamiento firma digital y, como resultado de la investigación, se observa que la estructura de esta tecnología está produciendo un cambio fundamental al transportar información en forma sana y confiable, Esto da como resultado que el tráfico de información en las redes de datos, se promueva el auge del comercio electrónico con servicios como acceso a bases de datos y gestión por medios digitales, lo cual era impensable hace algún tiempo. Así las cosas, la era de la firma digital ha traído normas y procedimientos que, dependiendo del país donde se establezca, permiten la digitalización de documentos de forma contraída a través de la adopción de pautas y reglamentos que tienen como objetivo verificar la autenticidad e integridad de los documentos

digitales que requieran firma para su validez, y así obtener un menor riesgo de fraude.

Ahora bien, la forma en que se plantea el establecimiento de la jerarquía a nivel nacional en cuanto a la firma digital, refleja una estructura que ya ha sido establecida en otros países como Argentina, lo cual garantiza resultados positivos en su implementación. Sin embargo, cabe destacar que el triunfo de un proyecto que incluya personas no siempre es el esperado, aun cuando se hayan utilizando estándares y parámetros de forma correcta. Esto se debe a la complejidad que representa cambiar la cultura de las personas, lo cual implica la aparición de un amplio espectro de problemas que están interrelacionados, como, por ejemplo, la resistencia al cambio, que se da por conformidad en la manera como se hacen los procesos, o bien por la cultura organizacional donde el individuo se ha desenvuelto. Estos dos factores pueden hacer que el proceso de la firma digital en Costa Rica no tenga los resultados esperados o requeridos.

Recomendaciones

Debido a que las comunicaciones han sufrido un gran cambio por los avances en la tecnología y la forma en que se transportada la información a través de las redes, se ha requerido establecer objetivos claros con respecto a los niveles de seguridad de software y hardware para garantizar que los datos no sean alterados. Así la firma digital es concebida con niveles de seguridad; por lo tanto, es de suma importancia tener bien definidas las normas y los reglamentos jurídicos con que se deben regir los procesos de utilización de la firma digital.

En cuanto en la forma de divulgar a la población el uso de la firma digital, es necesario establecer todo un programa que concientización, donde se promueva que el proceso de la firma digital es tan seguro como la firma escrita y que una vez enviado un documento digital a un destinatario, este puede descodificar la firma digital y confrontar el resultado con el texto original para asegurarse de quien es la persona correcta. Es decir, es necesario explicar conceptos sobre el uso que puedan facilitar el surgimiento y desarrollo de una cultura digital.

Bibliografía

Amparo; De La GUÍA, Dolores; Hernández, Luis; Montoya, Fausto y otros (1997), Técnicas Criptográficas de Protección de Datos. Madrid: Editorial RA-MA.

Augusto Pérez Merayo, Guillermo (2001), Comentarios acerca de las deficiencias que presenta él Proyecto de Ley sobre la Firma Digital. expediente Nº 14257, Junio 2001: http://www.centrodeconocimiento.com/firmadigital/index.htm.

Confirma .co.ar(2001), Firma digital, 30 de Noviembre de 2001: http://www.confirma.com.ar/Downloads/Firma%20Digital.pdf.

Enciclopedia Libre Universal en Español (2006), Hash, 01 de noviembre de 2006: http://enciclopedia.us.es/index.php/Hash.

Gigli Juan (2006), Firman convenio para utilizar firma digital en Internet, 26 de agosto de 2006: http://www.gobiernoelectronico.org/node/4972.

Hess Araya, Christian (2001), Firma digital. La Nación, 24 de agosto de 2001, p. 15.

Hess Araya, Christian (2006), Taller sobre implicaciones jurídicas de la firma digital, 02 de febrero de 2006: http://www.hess-cr.com/secciones/dere-info/index.shtml#otros.

Hess Araya, Christian (2006), Convenio MICIT-BCCR, 23 de agosto de 2006: http://www.hess-cr.com/secciones/dere-info/index.shtml#otros.

Hess Araya, Christian (2006), Ley de Certificados, Firmas digitales y documentos electrónicos, 30 de agosto de 2006: http://www.hess-cr.com/secciones/dere-info/index.shtml#otros.

Kalysis (2004), Firma electrónica, USB Token y lectores de tarjetas Criptográficas de Kalysis, Diciembre 2004, de http://www.tokenusb.com/.

La firma digital en Costa Rica (2006), lunes 10 de julio de 2006: http://www.empresas.co.cr/Articulos/Actualidad/La-firma-digital-en-Costa-Rica.html.

Masias, Jordi (2005), El no-repudio, Monografías (24 capítulos), 01 de agosto de 2005, http://www.wikilearning.com/el_no_repudio-wkccp-3270-12.htm.

Seguridad del empresario en la red, (2006). *La firma digital.* Publicado el lunes 5 de junio de 2006, de http://www.avogacia.org/w3/article.php3?id_article=1194.