Universidad Latinoamericana de Ciencia y Tecnología

Escuela Ingeniería Informática

Seminario de Graduación para el Grado de Licenciatura en Informática con énfasis de Telemática

Artículo Científico

Tema:

Aplicación de la Firma Digital en las Instituciones Autónomas de Costa Rica

Autor:
Carlos Castro Pérez
Cédula 7-081-162

Profesor: Miguel Pérez Montero

Año 2006

Dedicatoria

Por la paciencia, el amor y el sacrificio mostrado durante el periodo que duró mi preparación universitaria rindo un homenaje a mi esposa Edith y a mis hijos Bryan, Thais y Selwyn.

Agradecimiento

Primeramente doy gracias a Dios, el Padre de mi Señor Jesucristo, que con su amor infinito me da inteligencia y sabiduría para comprender y aprender los conceptos académicos universitarios expuestos con tanto acierto por mis profesores.

A Ulacit por la oportunidad de permitirme la preparación académica en sus aulas con calidad. Y por la preocupación de proveer a los estudiantes buenos profesores.

Gracias a mis profesores por la sabiduría que mostraron a la hora de transmitirnos sus conocimientos y experiencias.

A mis Jefes y compañeros de trabajo por la oportunidad de apoyarme en esta faceta de mi preparación académica.

Tabla de Contenido

Introducción

Cada año aumenta el número de transacciones financieras por la red mundial de Internet. Millones y Millones de dólares se invierten en la compra y venta de productos y servicios en la red en forma digital.

Las naciones hacen enormes esfuerzos para establecer leyes y acuerdos internacionales que regulen el comercio electrónico. El avance tecnológico y el número de transacciones digitales cada año va en aumento obligando a los países a no quedarse rezagados ya que el mundo comercial no espera.

El tema de seguridad en las transacciones digitales conlleva dos puntos de vista que van de la mano, la seguridad enfocado en el campo legal y la seguridad en el campo tecnológico.

Los tratados internacionales de comercio firmados por Costa Rica con el Caribe y con el Norte de América, las relaciones comerciales establecidas con Europa, Asia y Sudamérica, así como, el avance continuo de la tecnología, originan que las fronteras nacionales e internacionales se acorten o desaparezcan.

Costa Rica proporciona un Estado de Derecho garante de la seguridad en el comercio. En el caso del comercio electrónico se ha iniciado una serie de reformas, adiciones en algunos códigos, leyes del estado que regulan este campo y se mencionarán más adelante.

Los métodos de encriptación actual proporcionan a la firma digital toda la confidencialidad, integridad y la autenticidad necesaria para emplearla en diferentes aplicaciones que agilicen las transacciones comerciales, y permitan, a

nuestro país mostrarse altamente competitivo en el mundo del comercio digital.
En el presente trabajo se hace primeramente mención de la firma manuscrita y el sustento legal de nuestro país.

Seguidamente se analiza el tema de la firma digital desde el punto de vista del marco regulatorio de Costa Rica y el resto de los países, el cual promueve y define el entorno necesario para establecer la seguridad dentro del contexto legal y fundamental para impulsar a las empresas del Estado hacia esta nueva aventura del Gobierno digital.

Posterior a este tema se analiza el aspecto tecnológico de la firma digital desde la perspectiva de seguridad, considerándose los siguientes temas: encriptación, algoritmos, certificados digitales, normas, Claves públicas y privadas.

La Segunda parte del artículo se refiere a la aplicación de la firma digital en las labores diarias de las instituciones autónomas del país, la nueva forma de hacer el trabajo y economizar.

Se analiza toda la infraestructura tecnológica Nacional existente que soporte la implementación, el empleo y la aplicación de la firma digital que permite a las Instituciones Autónomas en sus diferentes sectores claves del Estado Costarricense mostrase competitivos, dinámicos y ágiles, que aseguren y garanticen los servicios tanto en el ámbito comercial como el ámbito financiero del Estado.

La Autoría de Documentos

La necesidad de identificar fehacientemente al autor de un documento ha llevado a la humanidad a crear métodos que intentan relacionar de manera única un documento con la persona responsable de su creación. En la antigüedad, los soberanos se imprimían un sello en los documentos como identificación única. En nuestros tiempos se utiliza la firma manuscrita como medio para validar un documento y en algunos casos, dependiendo del documento, se requiere la firma de un tercero (por lo general un notario) que certifique que la firma de un documento es auténtica.

Firma Manuscrita

Características:

La firma que se realiza a puño y letra sobre algún escrito o documento se le conoce como firma manuscrita, ésta puede ser legible o ilegible.

La enciclopedia Barsa define esta figura como la “expresión gráfica compuesta habitualmente del nombre, apellido y una rúbrica que sirve para identificar a una persona en la vida epistolar o de negocio” (Tomo VII, 1976).

La firma manuscrita tiene todo el reconocimiento legal y ésta se utiliza para dejar por establecido algún acuerdo entre dos o más partes.

Aspectos legales:

Mediante la firma manuscrita, el autor de la misma plasma en el documento su consentimiento de los términos estipulados en él y son de común acuerdo con la parte contractual.

Firma Digital

Características

La principal razón de la firma digital es servir como medio de identificación única, asegurando la autenticación absoluta del usuario y la integridad de los datos enviados, permitiendo así, asegurarse que el contenido del mensaje no ha sido modificado.

Tom Seldon conceptualiza este término y lo define como “los métodos de cifrado con dos propósitos, validación de contenido y el probatorio del contenido” (Networking, 1994).

En España la firma digital se ha definido como una figura de la legislación de esa nación. Utiliza una forma clara en su definición legal, mediante la ley 59/2003 se concreta como “la firma electrónica que permite identificar al firmante y detectar cual cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control” (Abogada Rebeca Peña, 2005)

La firma digital combina la utilización de dos claves la clave privada y la clave pública.

La clave privada únicamente la conoce el usuario o firmante y está bajo su custodia. Este tipo de clave puede ser simétrica o asimétrica y dado que en nuestro medio se requiere de una firma digital más universal se pasará a analizar únicamente la clave asimétrica que es la que se adapta a los requerimientos que esboza la ley.

Clave Asimétrica:

Este método utiliza dos claves, primeramente la clave privada que únicamente conocerá el propietario o emisor, esta clave no se comparte con nadie. La segunda clave llamada pública por cuanto será dada a conocer a otros usuarios.

Ambas claves son complementarias y se obtienen de complejos algoritmos matemáticos. Básicamente la clave pública funciona de la siguiente forma, cada usuario, genera un par de claves, una clave privada y una clave pública. La clave pública está disponible a todos los usuarios del sistema, con el fin de poder enviar mensajes a un determinado usuario. El mensaje le llega al usuario con su clave pública y este utiliza su clave privada para desencriptar el mensaje.

Criptografía

Es un método muy antiguo, mediante el cual se toma un mensaje y se le aplica un algoritmo matemático para cifrarlo con el objetivo de que nadie lo pueda leer, únicamente la otra parte que conoce el algoritmo puede descifrar el mensaje.

La página Web TextosCientíficos.com define la criptografía como “la ciencia que estudia la transformación de un determinado mensaje en un código de forma tal que a partir de dicho código solo algunas personas sean capaces de recuperar el mensaje original. En general se utiliza para ello una palabra clave o 'password' con la cual se cifra el mensaje, el código resultante solamente puede ser descifrado por aquellos que conozcan la clave”.

Esta herramienta facilita la utilización de la firma electrónica en el mundo digital del ciberespacio de Internet.

La infraestructura de Clave Pública:

La infraestructura de clave pública es un término empleado en la criptografía, sus

siglas en inglés son PKI cuyo significado sería ***P**ublic **K**ey **I**nfrastructure*. Esta infraestructura se obtiene mediante la combinación de hardware y software, políticas y procedimientos que permiten asegurar la identidad de los participantes en un intercambio de datos usando criptografía pública.

Propósito:

Una PKI permite a los usuarios autenticar a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas (de otros usuarios) para cifrar y descifrar mensajes. En general, una PKI consiste en un software para los clientes, un software de servidor (como una autoridad de certificación), hardware (por ejemplo, tarjetas inteligentes o *smart cards*) y unos procedimientos operacionales. Un usuario puede firmar digitalmente mensajes usando su clave privada, y otro usuario puede validar dicha firma (usando la clave pública del usuario, contenida en un certificado que ha sido emitido por una autoridad de certificación de la PKI). Esto permite a dos (o más) entidades establecer una comunicación que garantiza la confidencialidad y la integridad del mensaje y la autenticación de los usuarios sin tener que intercambiar previamente ninguna información secreta.

Dado que la infraestructura de clave pública se basa en que el usuario debe poseer la clave privada, esta clave se genera en el equipo del usuario. Dicha clave puede almacenarse en el disco duro, en tarjetas inteligentes o en llaves USB (que son elementos de soporte externo).

Tecnologías utilizadas

La tecnología que se utilizará en la criptografía representa un aspecto de gran importancia y que deber ser analizado con sumo cuidado para garantizar la seguridad de todo el sistema.

Para la firma digital existen varios sistemas que se pueden emplear, los métodos y

algoritmos usados más importantes son los siguientes:

Sistema o Algoritmo RSA: Este algoritmo es el más conocido y fue creado en 1978 por Rivest, Shamir y Adlman quienes fundaron la empresa RSA Data Security Inc. Actualmente es una de las empresas más prestigiosas en la protección de los Datos en el mundo.

El Ing. Luciano Moreno explica este algoritmo básicamente:

> "El sistema RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,..., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya tendremos un divisor del número.
>
> Ahora bien, si el número considerado es un número primo, se tendrá que para factorizarlo habría que empezar por 1, 2, 3,....., hasta llegar a él mismo, ya que por ser primo ninguno de los números anteriores es divisor suyo. Y si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo.
>
> Basado en la exponenciación modular de exponente y módulo fijos, el sistema RSA crea sus claves de la siguiente forma:
>
> 1. Se buscan dos números primos lo suficientemente grandes: **p** y **q** (de entre 100 y 300 dígitos).
> 2. Se obtienen los números **n** = p * q y **Ø** = (p-1) * (q-1).
> 3. Se busca un número **e** tal que no tenga múltiplos comunes con Ø.
> 4. Se calcula **d** = e^{-1} mod Ø, con mod = resto de la división de números enteros.
>
> Y ya con estos números obtenidos, **n es la clave pública y d es la clave privada**. Los números p, q y Ø se destruyen. También se hace público el

> número e, necesario para alimentar el algoritmo." (http://www.htmlweb.net/seguridad/cripto/cripto_10.html)

Para una mayor seguridad, se recomienda la utilización de una longitud de 1024 bits.

Algoritmo de Firma Digital o DSA: Su nombre proviene de las siglas en inglés *Digital Signature Algorithm*. Este sistema lo utiliza el Gobierno de los Estados Unidos de América en sus transacciones únicamente para firmar y no para cifrar. Se hizo público el 30 agosto de 1991, y fue propuesto por el Instituto Nacional Americano de Estándares y Tecnología conocido como NIST. Este algoritmo ocupa más tiempo y requiere mayor poder de cómputo que el sistema DSA.

Curvas Elípticas:

Este método se basa en el Problema Logarítmico Discreto y es un sistema de claves asimétricas.

-Algoritmo de *hashing*: En vista de la lentitud que representa cifrar un documento ya que requiere poder computacional se han ideado las funciones matemáticas llamadas *hash*. Estas crean un resumen del documento y luego toman el resumen y lo cifran, con la particularidad que no es posible volver al documento original a partir del cifrado.

Existen varios métodos:

MD-4, Mensajes Digitales, su salida es 128bits. Diseñado por RSA Security, Inc.

MD-5, Mensajes Digitales, su salida es de 128bits y contiene optimizaciones.

SHA-1: Algoritmo Hash Seguro, su salida es de 160 bits, diseñado por la NICT. Diseñado por el Instituto Nacional de Estándares y Tecnología, USA.

RIPEMD-160: La salida que produce es 160 bits. Diseñado por Hans Dobbertin.

-Generación de números al azar: El BBS tiene la especial fortaleza de ser impredecible “a derecha e izquierda”.

-Algoritmo de encriptación simétrica: El algoritmo IDEA. Aunque de reciente invención este algoritmo ha demostrado ser resistente a diferentes formas de ataque por fuerza bruta. Un ataque de fuerza bruta requiere 2^{128} intentos, este algoritmo esta registrado en el ISO Register of Cryptographic Algoritmhs”, ISO 9979/0002.

-Algoritmo de determinación de números primos: Existe un algoritmo probabilístico de alta convergencia, procurando asegurar que la probabilidad de generar un falso número primo sea inferior a 1 en 2^{32} (1 en 4 000 000 000).

-Protección de claves: las claves para encriptación (simétricas) se utilizan en una sola sesión de comunicación, por consiguiente, no quedan almacenadas en modo accesible en ningún archivo, su uso es transitorio y luego de utilizadas se descartan, las claves públicas, como es evidente no necesitan protección, los datos que necesitan un fuerte esquema de protección son las claves privadas y las “semillas” generadoras de números primos y números al azar, para ello, se prevén diversos esquemas de protección: en la aplicación “cliente”, los datos sensitivos se alojan en archivos encriptados; en lugar de utilizar contraseñas convencionales, el usuario accede a través de una “frase-contraseña”; ésta no es almacenada en ningún lugar del sistema, sino que en función de ella, en cada acceso, un algoritmo de hashing calcula un valor que sirve de índice. Este algoritmo es irreversible, lo que implica de a partir del resultado no será posible obtener el documento original.
Los más utilizados son MD2,MD4,MD5 y SHA con resúmenes de 128 y 160 bits.

Estándares Internacionales

La criptografía de clave asimétrica, también denominada criptografía de clave pública, forma parte de los siguientes estándares internacionales:

Los algoritmos han sido escogidos tomando en cuenta no sólo su seguridad sino también su compatibilidad con normas internacionales, en particular con las normas ISO y las del CCITT:

-Las firmas digitales que utilizan algoritmos de clase pública están reguladas por la norma ISO 9796 y el estándar de seguridad de la norma CCITT X.509.

-Los modos de operación de los algoritmos de encriptación están regulados por las normas ISO 8372 e ISO 10116.

-Los procedimientos de *hashing* están regulados por la norma ISO 10118-2.

Adicionalmente, el algoritmo RSA es parte de las normas de seguridad estándar de la “Society for Worldwide Interbank Financial Telecomunications s.c.”, de la norma francesa ETEBAC 5 para el sector financiero, de la propuesta de norma estadounidense ANSI X9.31 y de la norma australiana AS2805.6.5.3. Este algoritmo esta también incorporado a diversas funciones de sistemas operativos de Microsoft, Apple, Sun y Novell.

1. ISO 9796:

International Standards Organization ("Organización de Estándares Internacionales"), Norma ISO 9796 de Tecnología de la Información - Técnicas de Seguridad - Mecanismo de Firma Digital ("Information Technology - Security Techniques - Digital Signature Scheme") (Ver:http://www.iso.ch/cate/d17658.html).

2. ANSI X9.31:

Instituto Americano de Estándares Nacionales ("American National Standards Institute"), estándar X9.31 de Autenticado de Mensajes para Instituciones Financieras ("Financial Institution Message Authentication") para el sistema bancario estadounidense (Ver: http://www.x9.org).

3. ITU-T X.509:

La Unión Internacional de Telecomunicaciones, establece este estándar para la infraestructura de clave pública (*Public Key Infrastructure* o PKI)

X.509 especifica los formatos estándar para certificados de claves públicas y un algoritmo de validación de ruta de certificación. Es la pieza central de la infraestructura PKI, y es la estructura de datos que enlaza la clave pública con los datos que permiten identificar al titular. Su sintaxis, se define empleando el lenguaje ASN.1 (*Abstract Syntax Notation One*), y los formatos de codificación más comunes son DER (*Distinguish Encoding Rules*) o PEM (*Privacy Enhanced Mail*). Siguiendo la notación de ASN.1, un certificado contiene diversos campos, agrupados en tres grandes grupos:

4. PKCS:

Estándares de Criptografía de Clave Pública ("*Public Key Cryptography Standards*") desarrollados por RSA Corporation, en forma conjunta con Apple, Microsoft, Digital, Lotus, Sun y Massachussets Institute of Technology. (Ver: http://www.rsa.com/rsalabs/pubs/PKCS)

5. SWIFT:

Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales

Con la estandarización del los mensajes en el Comercio Electronico. ("Society for Worldwide Interbank Financial Telecommunications").(Ver: http://www.swift.com/index.cfm?item_id=3024) .

6. ETEBAC:

Sistema Financiero Francés, estándar 5. (Ver: http://www.afb.fr/catalog/p18b1.html).

Certificados Digitales:

Son los mecanismos electrónicos de seguridad y confidencialidad que garantizan la autenticación, la integridad, el no repudio y la vinculación jurídica de los documentos digitales en las comunicaciones electrónicas. Estos certificados se estructuran en forma jerárquica de modo que existe una entidad que emite los certificados y cumple el papel de certificador. Existe otra entidad en un nivel superior que autoriza los certificadores.

Así lo define el artículo 11 de la ley 8454, publicado en el Diario Oficial la Gaceta:

“Entiéndase por certificado digital el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente: la vinculación jurídica, la integridad, autenticidad y no alteración, la autenticación.”(San José, Octubre 2005).

Existen varios tipos de Certificados, que pueden ser implementados para diferentes aplicaciones, estos certificados son:

- *Certificados de Servidor*: comprueba la propiedad del dominio y la autorización del usuario.
- *Certificados Personales*: Permite navegar, comprar, enviar y recibir correo electronico.
- *Certificados Wap*. Se aplica a servidores Web, a las pasarelas Wap, que permiten enlazar las redes inalámbricas con las terrestres.

- *Certificados Timestamp*: Permiten estampar los tiempos en momentos precisos en el documento digital. Utilizar servidores de tiempo.
- Certificado Código: Permite a un administrador, desarrollador o empresa de software firmar su software y distribuirlo
- *Certificado VPN-IpSec*: Aprovecha la cualidad y ventaja de las redes VPN.

Según entrevista mostrada en los apéndice y realizada al Director de Certificados y Firmas Digitales de Costa Rica, se iniciará con el Certificado Personal.

Autoridades de Certificación

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. Es por tanto necesaria, una infraestructura de clave pública (PKI) para cerrar el círculo de confianza, proporcionando una asociación fehaciente del conocimiento de la clave pública a una entidad jurídica, lo que le permite la verificación del mensaje y su imputación a una determinada persona. Esta infraestructura de clave pública consta de una serie de autoridades que se especializan en papeles concretos:

Autoridades de certificación (CA o *certification authorities*): que vinculan la clave pública a la entidad registrada proporcionando un servicio de identificación. Una CA es a su vez identificada por otra CA creándose una jerarquía o árbol de confianza: dos entes pueden confiar mutuamente entre sí, siempre y cuando exista una autoridad común que sea directa o transitivamente que los avala.

Autoridades de registro (RA o *registration authorities*): que ligan entes registrados a figuras jurídicas, extendiendo la accesibilidad de las CA.

Autoridades de fechado digital (TSA o *time stamping authorities*): que vinculan un instante de tiempo a un documento electrónico avalando con su firma la existencia del documento en el instante referenciado (resolverían el problema de la exactitud temporal de los documentos electrónicos).

Estas autoridades pueden materializarse como entes individuales, o como una colección de servicios que presta una entidad multipropósito.

ASPECTOS LEGALES:

Existe una serie de regulaciones por medio de leyes, normas y acuerdos nacionales e internacionales que han surgido para garantizar la seguridad legal de las comunicaciones y el comercio electrónico. Esto permite a los países ir adoptando la figura de la firma digital en sus transacciones digitales. Estas leyes adoptadas en el ámbito nacional e Internacional se mencionan a continuación.

1. Nacional

   En Costa Rica se publicó en el periódico oficial la Gaceta # 197 del día Jueves 13 de octubre del 2005, la Ley N° 8454 llamada “Ley de Certificados, Firmas Digitales y Documentos Electrónicos.

   En el artículo #1 de esta ley faculta al Estado y todas las entidades públicas a utilizar los certificados, firmas digitales y documentos electrónicos dentro de sus respectivos ámbitos de competencia.

   Este artículo permite a las empresas del estado incursionar con el suficiente sustento legal en el campo de las transacciones digitales ayudado de la tecnología actual.

   El Artículo #8 de esta ley define la firma digital como:

“Entiéndase por firma digital cualquier conjunto de datos adjuntos o lógicamente asociados a un documento electrónico, que permitía verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico” (La Gaceta,2005).

La actual ley también le da el suficiente sustento legal a los documentos electrónicos en los artículos # 3,4,5,6,7. En estos artículos se reconocen los documentos electrónicos como probatorios en las mismas condiciones de los documentos físicos.

Actualmente existen otros artículos en diferentes leyes de la nación que regulan el derecho a la privacidad, la confidencialidad de las comunicaciones y tipifican los delitos informáticos.

Estos artículos son utilizados por las Cortes de Justicia para reprimir y sancionar los delitos informáticos y se mencionan en:

La Constitución Política de Costa Rica menciona en el artículo 24 declara:

“Se garantiza el derecho a la intimidad y a la libertad y el secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales y de cualquier otro tipo de los habitantes de la República” (Jorge Córdoba Ortega, 1996).

El Código Penal establece también los siguientes artículos:

Artículo 196bis, hace referencia a la violación de comunicaciones electrónicas.

Artículo 217bis, menciona el Fraude informático.

Artículo 229bis, sobre la alteración de datos y sabotaje informático.

La ley 7425 sobre Registro, secuestro y examen de documentos privados. Esta ley faculta únicamente a las autoridades judiciales al examen y análisis de cualquier tipo de documento.

La reforma a la Ley General de Aduanas de 1995, contempla los artículos 221

y 222.

En el Código de Normas y Procedimientos Tributarios mediante las adiciones a esta ley, están los artículos 93 contra el uso indebido de la información. El artículo 94 sanciona el acceso desautorizado a la información. El artículo 95 sanciona el manejo indebido de programas de cómputo. El artículo 96 sanciona por facilitar el código y la clave de acceso a los sistemas de información tributaria.

La ley de Administración Financiera de la República y Presupuestos Nacionales menciona en el artículo 111 las sanciones por los delitos informáticos.

Costa Rica ha realizado los esfuerzos necesarios para establecer todo el marco jurídico necesario para garantizar la seguridad legal.

2. Internacional

Algunos estudios revelan que el comercio electrónico por Internet va en aumento, cada día son más los miles de dólares que se invierten en las ventas digitales.

La Revista ComputerWolrd muestra el siguiente informe:

“Las Ventas en el Comercio Electrónico generadas de 1.6 trillones de dólares para el 2003.” (computerworld,enero 2001).

Ante este marco económico donde la inversión cada vez es mayor los países hacen esfuerzos políticos para darle el sustento legal necesario a este tipo de transacciones, y para garantizar la seguridad de la información, de los clientes y los proveedores.

Entre los países que se pueden citar están:

México: La ley de Firma Electrónica Avanzada (FEA), se dictaminó en agosto del 2003 con su publicación en el Diario Oficial de la Federación. Define tres sectores generales de utilización el gubernamental, el mercantil y el financiero.

Panamá:
Mediante la Ley 43 del 2001, define y regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos.

Colombia:
Promulga la Ley 527 de 1999, en la cual define y reglamenta el acceso y usos de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen entidades de certificación
La Ley 588 del 2000 se reglamenta el ejercicio de la actividad notarial.

Ecuador:
Establece la Ley 67 del 2002 sobre la Ley del comercio electrónico, firmas y mensajes de datos.

Perú:
Establece la Ley 27269, citada como la Ley de Firmas y Certificados Digitales
Chile: En 1999 se promulgo la ley chilena sobre firma digital. Posteriormente en agosto del 2001 se aprobó la ley que regula la firma digital y las Entidades de Certificación.

Puerto Rico:
Se aprueba la ley 188 en 1998 nombrada como Ley de Firmas Digitales de Puerto Rico.

Venezuela:
En el 2001 establece un decreto con fuerza de ley, sobre mensajes de datos y firmas electrónicas.

Brasil :
Mediante la medida Provisoria 2.00-2 del 2001 instituye la ley de infraestructura de Claves Públicas Brasileñas.

Uruguay:
Establece la firma digital en los artículos 695 a 698 de la Ley 16736 de la Administración Pública.

Argentina:
Aprueba la ley 25506 de 1998 llamada Ley de Firma Digital.
Japón. Ley Concerniente a la Firma Electrónica y los Servicios de Certificación. 2001.

Costa Rica:
Publica la Ley N° 8454 aprobada como “Ley de Certificados, Firmas Digitales y Documentos Electrónicos, en octubre del 2005.

Aplicación de la Firma digital

En la sección anterior se analizó la seguridad en la firma digital desde el punto de vista del marco legal nacional e internacional, así como, desde el punto de vista tecnológico enfocando temas como criptografía, certificados digitales, claves públicas, claves privadas asimétricas, algoritmos de firma digital, estándares internacionales, entre otros. Investigada la perspectiva de seguridad legal y

tecnológica queda por mencionar las entidades públicas, la infraestructura tecnológica del país y como puede combinarse cada uno de estos elementos para aplicarlos en la utilización de la firma digital permitiendo al país ampliar las oportunidades de alcanzar el mercado internacional y nacional en forma competitiva.

El Estado Costarricense cumpliendo el papel como ente integrador del sector público, privado y la sociedad civil es líder indiscutible y pionero en el uso de la firma digital.

El Gobierno de Costa Rica está realizando un esfuerzo de integración tecnológico de todo el aparato del estado y así lo indica en el informe del Taller de Alto Nivel sobre Comercio Electrónico y Tecnologías de Información y comunicaciones (TIC) para Centroamérica y el Caribe:

"...crear un punto de entrada al Gobierno, que integra todos los esfuerzos y servicios que ofrecen las instituciones estatales….De conformidad con lo anterior, este gobierno ha implicado la implementación de una serie de iniciativas. "(pág.7, Curazao, 25-27 Junio 2002).

Las Entidades Autónomas de Costa Rica involucran una serie de sectores estratégicos del país como el fiscalizador y controlador en manos de la Contraloría, el Sector Energético, Salud, Sector Turismo, Seguros, Telecomunicaciones, Productivo, entre otros. Estos Sectores son claves dentro de la economía nacional, por esta razón es importante promover un estado más ágil, dinámico y seguro que permita el ahorro de recursos y el alcance de ventajas competitivas en el mercado nacional e internacional.

Dichas instituciones estatales se mencionan en la siguiente unidad.

- Instituciones Autónomas de Costa Rica

El aparato del estado costarricense esta formado por instituciones públicas de las cuales algunas tiene autonomía en su administración y están sujetas a la ley en materia de gobierno.

Estas entidades están cimentadas en los artículos 188,189, 190 de la Constitución Política de Costa Rica y se les conoce como Instituciones Autónomas, se encuentran dentro de este rango las siguientes instituciones:

- Los Bancos del Estado.
- Contraloría General de la República
- Acueductos y Alcantarillados – AyA
- Caja Costarricense de Seguro Social – CCSS
- Compañía Nacional de Fuerza y Luz – CNFL
- Instituto Costarricense de Electricidad –ICE
- Radiográfica Costarricense – RACSA
- Instituto Costarricense de Turismo – ICT
- Instituto Nacional de Aprendizaje - INA
- Instituto Nacional de Fomento Cooperativo – INFOCOOP
- Instituto Nacional de Seguros – INS
- Refinadora Costarricense de Petróleo – RECOPE
- Consejo Nacional de Producción – CNP
- Consejo Nacional de Investigación Científica y Tecnológica – CONICIT

Es de suma importancia entonces destacar al Estado Costarricense como el responsable de velar por la Seguridad de la red, promoviendo e implementando todo el sustento legal requerido como se menciono en la sección anterior.

Complementariamente es necesario analizar también la infraestructura tecnológica con la que cuenta el país.

- Infraestructura Tecnológica Nacional

Actualmente Costa Rica ha realizado una serie de implementaciones en las diferentes tecnologías de telecomunicaciones con el fin de incursionar en el mundo digital del comercio electrónico.

- La conectividad del país se ha mejorado a través del sistema actual de telefonía y ampliando la conectividad con las compañías de televisión por cable.
- Se ha establecido anillos de fibra óptica en todo el territorio nacional, en el año 2001, que permitirán la cobertura nacional del 100%.
- La conexión al mundo digital por medio de las redes internacionales de telecomunicaciones se realizo por intermedio del Cable Submarino de fibra óptica Maya 1 y Arcos 1. Actualmente se está implementando un enlace de 4000 mbps, está conexión con la red Global Crossing, será en el océano pacífico y está prevista su operación a partir del año 2008.
- Se ha integrado la Red de Internet de Avanzada y otras redes como CRNET y GOBNET (conecta al congreso y al gobierno). EDUNET que conecta a colegios y escuelas. Y la Red de Internet 2 conecta a las universidades y centros de investigación del país.
- La red Internet de Avanzada utiliza los anillos de fibra óptica instalados en el país, los circuitos de SDH (Synchronous Data Hierarchical).
- Se pueden transmitir 122 mil documentos de 10 páginas por segundo o 610 mil correos electrónicos por segundo.
- Mediante acuerdos con la empresa Cysco System se ha logrado el 90% de conectividad de banda ancha a nivel nacional.
- También Costa Rica se convirtió en el primer país a nivel mundial en el año 2000, en ofrecer a todos los costarricenses una cuenta gratuita de correo electrónico por medio de www.costarricense.cr, con login y código de acceso; como política pública.

Ante este avance tecnológico, Costa Rica ocupa el tercer lugar en el mundo en materia de cobertura de banda ancha después de Corea del Sur y Canadá (Pág.15-23, “Establecimiento de la red e Internet de avanzada y creación de la red nacional de investigación avanzada” CAATEC 2001).

Este panorama nos muestra un Gobierno generador de iniciativas e imponiendo el desarrollo tecnológico de las telecomunicaciones y la información. Existen una serie de diferentes aplicaciones que pueden implementarse para aprovechar la firma digital en la estrategia de desarrollo tecnológico del país.

- Aplicaciones de la firma

Actualmente entre los negocios electrónicos y financieros que funcionan en nuestro país, está el *Home Banking*, donde la banca del estado por medio del Banco Nacional de Costa Rica como líder indiscutible en este sector, así como, el Banco Popular, el Banco de Costa Rica y la banca Privada estos funcionan con la firma electrónica mediante la comprobación de claves y usuarios, la tecnología Set “*Secure Electronic Transaction*” norma utilizada por las transnacionales MasterCard y Visa, este método es empleado por el comercio electrónico *e-commerce*.

Con la aprobación de la ley de Certificados, Firmas Digitales y Documentos Electrónicos, se permite la utilización de la firma digital en varias aplicaciones tanto legales, comerciales, privadas y públicas.

Para la aplicación de la Firma Digital y los Certificados la ley 8454 faculta al Estado Costarricense y a todas las Entidades Públicas a su utilización. En

el reglamento emitido por la Dirección de Certificados y Firmas Digitales del Ministerio de Ciencia y Tecnología en el artículo 3 detalla que los órganos estatales son:

- Los Supremos Poderes.
- El Tribunal Supremo de Elecciones.
- Órganos Constitucionales.
- Todas las Entidades Públicas.

Ámbito de Aplicación:

El ámbito de aplicación de la firma digital la ley en su artículo #1 lo puntualiza de la siguiente manera:

- Toda clase de transacciones
- Los actos Jurídicos.
- Los Actos Públicos.
- Los Actos Privados

Analizada la firma digital bajo la perspectiva legal que autoriza la utilización de esta tecnología en las entidades y su ámbito de aplicación, se puede establecer situaciones disímiles donde el Estado puede sacar mayor utilidad para agilizar sus procesos, lograr economizar recursos, ampliar su mercado y mostrarse competitivo en el mercado internacional, considerando que todos los países del Continente Americano están adoptando esta tecnología. Entre las posibles aplicaciones se pueden identificar las siguientes:

- Identificación como usuario en las redes internas y externas: Mediante su identificación el usuario puede ingresar a intranet de su lugar de trabajo, a una red privada o pública, sin que requiera estar utilizando para identificarse diversos usuarios y claves.

- El correo electrónico.
- Identificación en Internet: Mediante la firma digital, el usuario tiene la posibilidad de realizar todas sus transacciones digitales por Internet con su propia identificación.
- Transacciones EDI: Empleando un formato normalizado las empresas intercambian datos comerciales como órdenes de compra, facturas, datos de proveedores, clientes, transportistas, bancos o agentes de aduanas.
- Transacciones financieras y bancarias: se podrán hacer transferencias electrónicas de fondos entre empresas, clientes, entidades. El E-Cash o dinero digital se utilizará con mayor medida, solicitando la posibilidad de descuentos en las compras en línea.
- Comercio Exterior: Las entidades públicas podrán incursionar en las transacciones digitales con diferentes entidades internacionales.
- Comercio Interno: Todas aquellas transacciones comerciales que las leyes de Costa Rica permite, podrán plasmarse electrónicamente agilizando trámites y economizando recursos.
- Contratos: Se pueden establecer contratos entre varias partes agilizando el trámite, la seguridad e integridad de los mismos.
- Reservaciones: La reservaciones de Hoteles, vehículos, tiquetes de avión en el extranjero y a nivel nacional.
- Facturación digital: la creación y emisión de facturas digitales enviadas a los usuarios o entidades del estado, permitirá realizar los pagos de inmediato una vez que se revise y apruebe el monto. Estas deducciones se realizarán directamente de las cuentas bancarias.
- Acceso a Sistemas de Licitaciones: Los pedidos de bienes y servicios, las condiciones de los carteles estarán disponibles a los interesados.
- Pago de Servicios: el pago de servicios de agua, luz, teléfono, servicios médicos se podrán realizar a través de todo el sistema integrado.

- Envió de documentación: A través de la firma digital es posible establecer una comunicación y transferencia de datos segura entre las entidades como la Contraloría General de la Republica, la Asamblea Legislativa, Poder Ejecutivo, Poder Judicial. Esto conlleva a la disminución de costos, al no repudio, la integridad y confidencialidad.
- Sufragio o votación electoral: Al ser un método seguro permitiría al Costarricense el poder emitir su voto con toda la seguridad y confiabilidad necesaria. La persona puede ejercer este derecho desde cualquier parte del país o del mundo sin tener que desplazarse al recinto de votación.

Beneficios:

- La Autenticación: permite identificar en forma inequívoca al signatario y verificar su identidad, fecha, hora, lugar.
- Imposibilidad de suplantación: nadie puede suplantar al signatario debido a que este administra su clave privada.
- Integridad: Este sistema de firma digital permite descubrir cualquier alteración o manipulación en la información enviada por pequeña que sea.
- No Repudio: Debido a la imposibilidad de suplantar al signatario, de manipular o alterar los datos, esto permite tener un testimonio real que solo él pudo firmar el documento.
- La Auditabilidad: para rastrear e identificar las operaciones, transacciones mediante la adhesión de la fecha y hora.

Certificador Nacional

Mediante la *ley de firma digital* se delega la Administración del Sistema de Certificación a la Dirección de Certificadores de Firma Digital. Esta instancia es una dependencia directa del Ministerio de Ciencia y Tecnología- MICIT.
La Dirección de Certificadores de Firma Digital o DCFD, por lo tanto será el ente sobre el cual recaen las credenciales de *Certificador Nacional*. Esta responsabilidad es asignada por el artículo 23 de la ley y establecida por el Reglamento de la Ley de Certificados, firmas digitales y documentos electrónicos, de la Dirección descrita.

Jerarquía de Certificación

Según la reglamentación emitida por la Dirección de Certificadores de Firma Digital, la jerarquía que se define para todas aquellas entidades públicas o privadas, nacionales o internacionales que deseen utilizar esta tecnología se desarrolla en un esquema de tres niveles. Para estos niveles según su importancia jerárquica se identifica el primer nivel citado como *el Certificador Raíz*, en un segundo Nivel esta el Certificador Autorizado o Registrado. En el tercer nivel está el Certificado Personal.

- Certificador Raíz:

  Esta posición la ejerce el Certificador en la posición superior de la jerarquía de Certificadores. La ley y el reglamento constituyen claramente esta labor a la Dirección de Certificadores de Firma Digital o DCFD.

  Esta Dirección, establecerá junto con el Comité Asesor las políticas de operación y deberá cumplir el Certificador Raíz y que serán heredadas a los certificadores autorizados. El Comité Asesor es un órgano interdisciplinario conformado por:

- Banco Nacional de Costa Rica.
- Tribunal Supremo de Elecciones.
- Poder Ejecutivo.
- CONARE o Consejo Nacional de Rectores.
- CANTIC o Unión Costarricense de Cámaras y Asociaciones de la Empresa Privada.

Las políticas y requerimientos técnicos del reglamento deberán ser revisados y evaluados por el *Ente Certificador Autorizado o ECA* de conformidad con lo que establece la ley 8279 referida como la *"Ley del Sistema Nacional para la Calidad".*

- Certificador Registrado y Acreditado.
  Esta figura es aquella entidad pública o privada, Nacional o Extranjera que esta inscrito y autorizado como certificador por parte de la Dirección de Certificadores de Firma Digital.

- Certificado Personal
  Es el emitido por el Certificador Autorizado y Registrado con todas las calidades y detalles de la persona física y firmada por este.

Implementación de los Certificados y Firmas Digitales en las empresas

Una vez establecida y aprobada la reglamentación y los requerimientos técnicos de parte de los entes estipulados en la Normativa Costarricense. El Certificador Raíz establecerá en un Módulo Raíz que es un aparato de Hardware donde se incorporan estas plantillas y serán heredadas a los módulos hijos de los Certificadores Autorizados.

Este módulo Raíz deberá estar ubicado en un lugar totalmente acondicionado bajo estrictas normas de seguridad.

Cuando una entidad desea convertirse en un certificador autorizado y registrado deberá acudir a la Dirección de Certificadores de Firma Digital, para retirar toda la documentación al respecto, los requerimientos operacionales y técnicos.
Una vez que la entidad cumpla con todo lo requerido en el reglamento, operacionalmente y técnicamente deberá ser evaluado por el ECA, encargada del Sistema Nacional de la Calidad. El ECA dará el visto bueno a la entidad en el entendido que cumple con todo lo establecido.

Posterior a la Aprobación de ECA, la entidad deberá trasladar su Módulo de Certificación al lugar que la Dirección de Certificadores le indique. Este lugar será donde se custodia el Módulo de Certificación Raíz. Ambos módulos se conectan físicamente, estableciéndose la comunicación entre ambos.

Una vez conectados el Módulo Raíz deberá heredar todas las plantillas con los requerimientos operacionales.

A partir de este momento la entidad pública o privada pasa a ser un Certificador Autorizado y Acreditado por la Dirección. Su Módulo Certificador será instalado en sus oficinas, estando en la condición de ofrecer al público los servicios de certificación y firma digital. Existen varias soluciones de infraestructura de clave pública en el mercado que las empresas pueden analizar como sistemas gestores, entre ellas están: OpenCA, Microsoft Windows 2003 Certificate Services, SunONE Certificate Server. Estos certificados deberán cumplir con ciertas consideraciones como longitudes de claves de 1024 bits, con el estándar X.509, el periodo validez de los certificados.

La entidad certificadora deberá establecer los puertos seguros para los administradores como por ejemplo los puertos 8200 y 8100. También los puertos para la interacción con los usuarios finales tales como el 1027 para las conexiones https y el 1024 para conexiones http.

La persona física que desea un certificado deberá ir personalmente a la entidad certificadora, llenar la solicitud, cumplir con lo requerido y firmar el certificado.

Este contrato tendrá una validez de un año. A partir de este momento las credenciales digitales del usuario pueden almacenarse en uno de tres dispositivos: el disco duro, en tarjetas inteligentes o llaves especiales.

Mediante este análisis, se ha comprobado el esfuerzo que realizan otros países con la aprobación de la firma digital como leyes, si olvidar los aspectos técnicos en cuanto a la infraestructura tecnológica, técnicas y algoritmos de encriptación avanzados, nuestra capacidad de ancho de banda, el esfuerzo de nuestro Gobierno, con, la aprobación de la ley de firma digital y su reglamentación, la integración de la Dirección de Certificados y firmas como el ente Certificador de nuestro país, como impulsor del desarrollo de la firma digital en las instituciones autónomas de Costa Rica.

Todo este marco tecnológico, legal y estratégico nos permite augurar que pronto nuestra economía dará un salto hacia el mundo digital, en un mediano plazo. Las condiciones se están dando, solo queda tomar la iniciativa y aventurarse con confianza hacia un futuro inevitable.

Conclusiones

Las naciones de Latinoamérica están realizando esfuerzos considerablemente grandes en la implementación de la firma digital. Las leyes y normativas aprobadas demuestran el deseo de incursionar en el mundo digital. Nuestro país no se ha quedado atrás, la aprobación de la ley de certificados y firmas digitales permitirá a las instituciones del estado incursionar en este campo, permitiendo agilizar sus procesos, aumentar su competitividad y economizar tiempo y dinero al ahorrar recursos que se generan con toda la documentación que se crea en el diario hacer de la administración pública.

El desarrollo de iniciativas legales y tecnológicas que permiten al Estado Costarricense garantizar la seguridad de sus transacciones electrónicas e impulsará a la Instituciones Autónomas a ser parte del Gobierno Digital.

Con el establecimiento de la Dirección de Certificados y Firma Digital en manos del Ministerio de Ciencia y Tecnología, se consigue un órgano estatal y administrador, cuya misión será fungir como Autoridad de Certificación, en el más alto nivel de nuestro país, garantizando normalizar y estandarizar la emisión de Certificados y Firmas Digitales en todas aquellas instituciones que deseen convertirse en entes certificadores.

Con la adopción de Certificados y firmas digitales en las Instituciones Autónomas, se podrán satisfacer los requerimientos de la economía nacional dado que la brecha digital disminuirá con relación a las otras naciones.

El Estado Costarricense se ha convertido en el líder garante de la seguridad y de los derechos de los ciudadanos y el comercio.

El crecimiento continuo en la demanda del ancho de banda ha provocado que nuestro gobierno desarrolle estrategias que fortalezcan la infraestructura tecnológica de la nación, adoptando medidas como la cobertura nacional del anillo de fibra óptica, implementación de los enlaces submarinos de fibra en el caribe como Arcos y Maya, así como, el enlace con la red Global Crossing por el pacífico programado para efectuarse en el año 2008 esto permitirá obtener una conexión continua y redundante de ancho de banda con el mundo electrónico.

Las técnicas de encriptación actuales, las claves asimétricas, los algoritmos de firma digital como RSA, SHA-1, los algoritmos hashing, son tecnologías que garantizar la seguridad en las transacciones actuales, estableciendo confianza en la integridad, confidencialidad y no repudio de la información.

La Dirección de Certificados y Firmas Digitales ha establecido para la emisión de certificados las siguientes normas internacionales ISO/IEC 18033 que define las cláusulas y definiciones acerca de la encriptación, las diferencias entre cifrados simétricos y asimétricos, administración de claves y sus problemas asociados. La norma ISO 15408 que define para las tecnologías de información la seguridad funcional y el aseguramiento de los requerimientos. La norma ISO 18032 que especifica los métodos para la generación y evaluación de los números primos que son utilizados en los algoritmos de encriptación. La norma ISO 15782 define el sistema de administración de los certificados digitales, autoridades de certificación, definición de llaves públicas, entre otros.

Recomendaciones

Realizar una evaluación sobre la tecnología actual en los diferentes sectores claves del Estado Costarricense, para determinar los requerimientos y proponer políticas e iniciativas tecnológicas, financieras y económicas que satisfagan e impulsen la implementación y el desarrollo en la firma digital de todo el aparato costarricense.

Realizar investigaciones y comparaciones con otros países, para determinar los problemas y soluciones que han surgido durante los procesos de implementación de firma digital en sus naciones, con el fin de lograr el menor impacto negativo en nuestra economía al adoptar un plan de firma digital en nuestras Instituciones Autónomas.

Para implementar en nuestras Instituciones Autónomas el desarrollo de una estrategia de firma digital se recomienda promover un plan piloto de firma digital en algunas instituciones del Estado Costarricense con el propósito de medir el impacto en los procesos, en el campo financiero y tecnológico, a fin de determinar aquellos factores que se deben de fortalecer, modificar, cambiar o suprimir.

Será necesario analizar los requerimientos técnicos en cada institución que desee convertirse en un ente certificador. Estos requerimientos deben de contemplar como mínimo un estudio de los Sistemas Gestores de Certificados, los tipos de certificados digitales, los dispositivos externos de almacenamiento.

En una implementación es necesario definir un grupo de participantes, la cantidad de personas que integran este grupo, el sector dentro de la empresa que se va a implementar la firma digital, se debe analizar la dinámica de los procesos involucrados y que intervienen en dicha aplicación, a fin de no dejar por fuera

algún detalle relevante que afecte el normal desarrollo de la institución.

Durante la implementación de la firma digital se debe se mantener en forma paralela el sistema manual o sea la firma manuscrita, hasta que los resultados sean evaluados, probados y garantizado como confiable y seguro.

Es importante para cualquier institución que desee convertirse en un ente certificador, analizar cada una de las soluciones de certificación en el mercado, con el fin de determinar y proponer aquella que mejor se ajuste a su entorno de trabajo.

En importante definir durante el diseño de implementación cada uno de los puertos de ingreso para los administradores del sistema, así como los puertos de los usuarios finales. La interacción que se da entre la solución de certificación y los navegadores de Internet como Netscape, Internet Explorer, Firefox entre otros, es importante tomarla en serio e investigarla a fin de prever situaciones que afecten todo el sistema.

Debe considerarse aquellas situaciones donde la firma digital de algún usuario deba llevar un visto bueno de una jefatura o gerencia. Las firmas digitales anidadas se definen con el estándar ISO 15782

Bibliografía

Asamblea Legislativa(2005).Ley de Certificados, Firmas Digitales y Documentos Electrónicos. Ley 8454. San Jose,C.R.

Asamblea Legislativa(2002).Ley de Sistema Nacional de Calidad. Ley 8279, San Jose,C.R.

Carlos Fernando Berbaran. Estudio Firma Digital (2004). http://www.hfernandezdelpech.com.ar/Leyes/Trab.Firma%20Digital.Deusto%202004.htm

Chinchilla Sandí, Carlos (2004). Delitos Informáticos: Elementos básicos para identificación y su aplicación. San José, CR. Editorial Ediciones Farben.

Código Civil (1996).San José. CR. Editorial Porvenir S.A.
Imprenta Nacional (2005). La Gaceta. San José, CR.

Comisión Asesora en Alta Tecnología (CAATEC).”Costa Rica en el Mundo Digital: Retos y Oportunidades”. San José. Noviembre 2001.

Córdova Ortega, Jorge (1996). Constitución Política de la Republica de Costa Rica, Concordada, anotada y con resoluciones de la Sala Constitucional. Zapote : Editorial Investigaciones Jurídicas S.A.

Hugo Daniel Carrion. Firma Electrónica, recuperado 22 de marzo de 2006, de http://www.delitosinformaticos.com/firmaelectronica/analisis2.shtml

Ing.Luciano Moreno(2004). Articulo bajado en marzo 2006.
http://www.htmlweb.net/seguridad/cripto/cripto_10.html

Instituto Americano de Estándares Nacionales (2005). http://www.x9.org/news.cfm

Internacional Organization Standardization (2006). Digital Signature Schemes.
http://www.iso.org/iso/en/ISOOnline.frontpage

IPSCA(2006).Articulo Protocolo SSL. http://www.ipsca.com/es/certificates/ssl.asp.

Ministerio de Ciencia y Tecnología(2006). “Reglamento a la ley de certificados, firmas digitales y documentos electrónicos”.
http://www.micit.go.cr/biblioteca/index.htm

Pc-News.com(2003). Los Ticos se cuelan por la Banda Ancha.
http://www.pc-news.com/detalle.asp?sid=&id=5&Ida=945

Anexos

1. Ley de Firmas y Certificados Digitales. Ley 8454
2. Reglamento de Firmas Digitales. MICIT.
3. Mapa de Enlaces de Fibra Óptica.

Apéndices

1. Entrevista a la Dirección de Certificados y Firmas. MICIT.