PKI* y firmas digitales: aplicaciones reales

PKI and digital signatures: True-to-life applications

Armando Carvajal
Master en Seguridad Informática Universidad Oberta de Cataluña. Especialista en construcción de software para redes - Uniandes. Ingeniero de Sistemas – Universidad Incca de Colombia. Gerente de Consultoria – Globalteksecurity.
armando.carvajal@globalteksecurity.com

Resumen

El uso de las claves públicas es la base para que se dé el comercio electrónico. Este documento busca sustentar que la administración de la infraestructura de llaves públicas o PKI es la solución para conseguir seguridad de la información en los negocios electrónicos, pues no se puede concebir el mundo digital sin los notarios del mundo análogo que garantizan la identidad de las personas. El artículo describe las características mínimas que debe tener el comercio electrónico, luego muestra filosóficamente las diferencias entre la criptografía simétrica y la asimétrica, describe en detalle los certificados digitales pero no hace una descripción matemática de la criptografía necesaria para su funcionamiento. Define PKI como la fusión de las dos criptografías simétrica y asimétrica mostrando sus aplicaciones más comunes del mundo real. Finalmente, hace un resumen de las leyes que al respecto se han dado en Colombia.

Palabras clave. Autoridad Certificadora CA, Claves públicas, Claves simétricas, Claves asimétricas, Certificado digital, Criptografía, OpenCA, PKI.

Abstract

The use of public keys is the basis of electronic commerce. This paper aims to support the administration of public key infrastructures (PKI) as a solution to secure data in electronic businesses. The digital world cannot be conceived without these notaries of the analogous world which guarantee people's identity. The article descrives the basic elements that electronic commerce must have, it demonstrates, in a philosophical way, the differences between symmetric and asymmetric cryptography. A detailed description of digital certificates is provided; however, it does not describe the mathematics of cryptography required for its operation. It also defines PKI as the merger of the two cryptographies (symmetric and asymmetric), showing its more common applications of the actual world. Finally, it summarizes the legislation and regulations on this topic in Colombia.

Keywords. Certification Authority CA, public keys, symmetric and asymmetric keys, digital certification, cryptography, OpenCA, PKI

*Public Key Infraestructure (Infraestructura de Clave Pública)

Introducción

Hace algunos años la preocupación se centraba en el perímetro pero, hoy el comercio electrónico está cambiando nuestra forma de pensar, y esto se debe a que el perímetro ahora está distribuido geográficamente, pues muchas organizaciones tienen por lo menos su portal web y el servicio de correo electrónico en hosting, es decir fuera de su perímetro local.

Hoy, no se pueden concebir los negocios electrónicos sin las claves públicas, pero las claves públicas generan otro problema, "El como asociar una clave pública de forma unívoca a una persona, servidor o cosa", es aquí donde la "Infraestructura de llaves públicas" o PKI interviene para resolver esta problemática.

Como en la vida real respecto de los directorios telefónicos las claves publicas también cambian, existen varios proveedores de certificados digitales como de directorios telefónicos, ¿por qué confiar en un proveedor de certificados de propósito específico? ¿Qué pasaría si un certificado es revocado? ¿Cómo se le informa a los proveedores y clientes que ese certificado ya no es válido? ¿Es válido el certificado público del cliente, con el que estoy haciendo transacciones? Este capítulo busca analizar estas preguntas y las aplicaciones reales de PKI en forma práctica, mostrando un ejemplo de la vida real.

Antecedentes

No se debería pensar mucho en el perímetro local, pues la seguridad debe estar implícita en los servicios fundamentales del comercio electrónico, los servicios digitales deberían incluir las siguientes características para ser equivalentes al mundo análogo:
Las características mínimas para hacer comercio electrónico son:

A. Identificación
Es el proceso de reconocer a una entidad o a un individuo dentro de un grupo.

Por ejemplo, cuando los empleados de ventas de una empresa viajan generalmente necesitan acceder a Internet, entonces lo hacen con la misma cuenta y contraseña compartida.

B. Autenticación
Es el proceso mediante el cual se comprueba y verifica que algo no ha cambiado y que es el original.

Por ejemplo, un usuario puede firmar un documento antes de enviarlo y tener la certeza de que el documento original no ha sido modificado puesto que ha sido firmado. Si se alterara el mensaje la firma no sería válida y se puede constatar o verificar que el mensaje ha sido firmado por una determinada persona.

C. Autorización
Es el proceso de determinar lo que puede hacer una entidad o persona.

Por ejemplo, un usuario que tiene una cuenta corriente en un banco no debería tener acceso a cuentas de ahorros, títulos valores, préstamos, banca, seguros, etc

En el mundo electrónico la autorización depende de la autenticación que en conjunto de las reglas del negocio determinan si el usuario o entidad tiene acceso al servicio electrónico.

D. Integridad
Es el proceso de garantizar que la información no ha cambiado en la transacción electrónica.

En el ejemplo de la "firma electrónica" de documentos antes mencionada, se debe tener la particularidad de que dependa no sólo de la identidad del remitente sino también del contenido del mensaje, por lo que si este es alterado, la firma ya no será válida.

E. Confidencialidad

Es el proceso de mantener la información en secreto. La confidencialidad genera privacidad, de hecho se consideran sinónimos.

El ejemplo de la firma electrónica de documentos, antes mencionada, permite a un usuario mediante cifrado garantizar que solamente el destinatario podrá leer el mensaje. La criptografía ayuda a que las personas no autorizadas vean el contenido de sus mensajes cifrados, es la característica mas conocida en criptografía.

F. No repudio

Es el proceso que garantiza que el emisor no pueda negar lo que hizo. No repudio equivale al término de "Aceptación" y es una de las características más difíciles de garantizar. En el ejemplo de la "firma electrónica" de documentos antes mencionada, el emisor no podrá negar que él firmó o cifró el documento enviado.

Criptografía, la base de los certificados digitales

La criptografía es la ciencia que estudia la escritura secreta, una cifra o criptosistema es un método secreto de escritura mediante el cual un texto en claro se transforma en texto cifrado o criptograma. Se le llama cifrado al proceso de transformar texto claro en texto cifrado, mediante claves criptográficas.

La criptografía se ocupa del análisis y diseño de algoritmos para cifrar y el criptoanálisis se encarga de romper esos algoritmos.

Cuando se hacen escuchas pasivas o "eavesdropping" se esta atacando el secreto, esto se hace mediante herramientas denominadas sniffers, pero cuando se hace escucha activa o "tampering" se ataca la autenticidad de la comunicación.

G. Criptografía Simétrica

La criptografía simétrica es la mas conocida pues fue utilizada por los egipcios hasta los romanos pasando hoy por las aplicaciones comerciales de telefonía móvil, cifrado de documentos en ofimática, cifrado de canales de red y cifrado de datos en aplicaciones de bases de datos. Algunos ejemplos muy conocidos son DES, 3DES y AES.

Sus características principales se podrían enunciar como:

- Utiliza la misma clave para cifrar y descifrar documentos
- El cifrado simétrico es muy rápido y seguro
- El texto cifrado es compacto.
- Tiene el problema de que la clave simétrica puede ser interceptada cuando el transmisor envía al receptor la clave secreta.
- Las claves no son escalables para grandes poblaciones.
- Las claves requieren una administración compleja.
- La criptografía simétrica no cumple con el requerimiento de aceptación o no repudio.

H. Criptografía asimétrica

La criptografía asimétrica es la mas moderna y es el futuro del comercio electrónico; los ejemplos mas conocidos son RSA y ECC.

A diferencia de las claves simétricas donde emisor y receptor usan la misma clave o contraseña, en las claves públicas asimétricas el emisor (E) y el receptor (R) crean un par de claves que consisten en una clave privada y una pública.

Se debe hacer un "requerimiento de certificado digital" por cada elemento que interviene en la transmisión de datos electrónicos seguros

Emisor y receptor guardan su clave privada con recelo y hasta con una contraseña (autenticación) para evitar que sea legible a personas no autorizadas

Emisor y receptor ahora tienen su clave pública, esta la puede y la debe tener cualquier persona que desee enviar documentos seguros a sus dueños, los directorios de los proveedores contienen esas claves públicas.

La Figura 1 muestra las fases de firmar y cifrar, y qué claves se requieren para cada paso en el proceso.

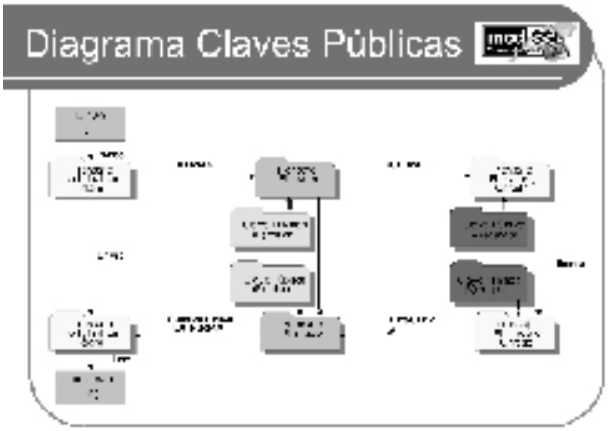

Figura 1. Diagrama de claves públicas

Ejemplos de implementaciones de llaves asimétricas son Open SSL y Gnu PG (PGP) que funcionan como un algoritmo del tipo de clave pública asimétrica.
Características principales de la criptografía asimétrica:

- No utiliza la misma clave para cifrar y descifrar documentos.
- El cifrado asimétrico es más lento pero seguro.
- No tiene el problema de que la clave pueda ser interceptada pues el transmisor nunca envía al receptor la clave secreta o privada
- Las claves son escalables para grandes poblaciones pues las claves públicas que se deben distribuir son iguales al número de claves públicas de los participantes.
- Las claves no requieren una administración compleja.
- La criptografía asimétrica cumple con el requerimiento de aceptación o no repudio, además de los certificados digitales
- No exige una relación entre emisor y receptor para hacer intercambio de claves públicas
- Tiene la desventaja de que expande el texto cifrado cada vez que se cifra.

I. Criptografía asimétrica + Criptografía simétrica
Esta es la solución, usar lo mejor de cada tecnología. Hoy la mayoría de servicios como el correo electrónico seguro, las VPN que interconectan oficinas remotas, las sesiones seguras entre cliente y servidor web, etc.

Los criterios deseables:

1. Una solución segura.
2. Un cifrado rápido.
3. Un texto cifrado muy compacto.
4. Una solución escalable a grandes poblaciones.
5. No permite la interceptación de claves.
6. No requiere relación entre emisor y transmisor.
7. Soporta firmas digitales.
8. Soporta el no repudio = “aceptación”.

Pasos del proceso como ocurren en los servicios que se utilizan hoy:

Transmisor:

1. El texto en claro de gran volumen se cifra con criptografía simétrica mediante una clave simétrica aleatoria, generalmente de 128/256 bits
2. Se consigue la clave pública del receptor en un directorio, generalmente, la clave pública tiene 1024bits.
3. Se cifra la clave simétrica con la clave pública del receptor: “Operación de clave empaquetada”.
4. Se crea un sobre digital que contiene la clave simétrica cifrada + el texto cifrado con la clave simétrica
5. Se envía el sobre digital

Receptor:

6. El receptor abre el sobre: encuentra el texto cifrado y la clave empaquetada.
7. El receptor con su clave privada descifra la clave empaquetada.
8. Ahora, el receptor descifra el archivo cifrado y lo convierte a texto en claro con la clave simétrica.

Problemas:

¿Qué pasaría si un pirata consigue mi clave pública y se hace pasar por un transmisor conocido que me envía información falsa?
Respuesta. Se debe firmar el hash de tipo sha1 (160 bits) del texto con la clave privada del transmisor, esto garantizaría el requerimiento número 7: soporte de firmas digitales
¿Qué pasaría si el pirata cambia en el directorio público la llave pública del transmisor?
Respuesta. Se deben utilizar los certificados digitales X.509, esto garantizaría el requerimiento número 8: soporte al no repudio

Entonces, definamos qué es un certificado digital y por qué se necesitan entidades de confianza para que las criptografías simétricas y asimétricas sean aceptadas por las leyes locales de cada país, cuando se hagan transacciones de comercio electrónico.

PKI

Wikipedia define PKI como "Una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas".

El objetivo fundamental de PKI es establecer identidades digitales, es decir asociar a una entidad (personas, organizaciones) o cosas (router, firewall) una unicidad con su par de llaves pública/privada.

La posesión de una pareja de claves pública/privada no es suficiente para establecer la identidad confiable de una persona o cosa, se requieren "relaciones de confianza" como en el mundo análogo respecto de los notarios, los notarios son al mundo análogo como las CA o entidades certificadoras son al mundo digital.

Importante:

- La CA es la entidad certificadora.
- La CA tiene su propia clave privada y su clave pública diferentes a los usuarios, que tienen sus propias claves privadas y públicas.
- La CA firma el requerimiento de un usuario con su clave privada para crear la clave pública que le solicitaron (se la vende al usuario, ese es el negocio de las CA).

PKI logra establecer identidades digitales así: la CA hace un hash de la clave pública y la firma con su clave privada (de la CA), ahora empaqueta en un solo archivo los datos de la persona o cosa, la clave pública de la persona o cosa, el hash firmado con la clave privada de la CA y la clave pública de la CA.

¿Qué es un certificado digital?

Es un mecanismo que se basa en la criptografía de claves públicas o asimétricas para permitir comunicaciones seguras entre origen y/o el destino utilizando medios de comunicaciones inseguros como Internet, además permiten que la comunicación esté certificada por un tercero de confianza denominado CA "Certificate Authority" que garantiza la confidencialidad y el no repudio de la comunicación. Ver Figura 2.

Importante:

- Técnicamente, un "Certificado digital" es el hash de la clave pública firmada con la clave privada de la CA, mas la información de la persona o cosa, mas la clave publica de la CA, mas la clave pública de la CA

Raíz, esto es crítico pues permite verificar la jerarquía de confianza leyendo un solo archivo digital.

- En Colombia, la única entidad certificadora a la fecha es Certicámara, esto se debe por la poca demanda de certificados digitales.
- Por ley, en Colombia, sólo son válidas las firmas digitales hechas con los certificados digitales expedidos por Certicámara.
- Si una investigación forense se firma con un certificado digital expedido por una CA que no está en Colombia, esta investigación no tendrá fuerza ante un juez.

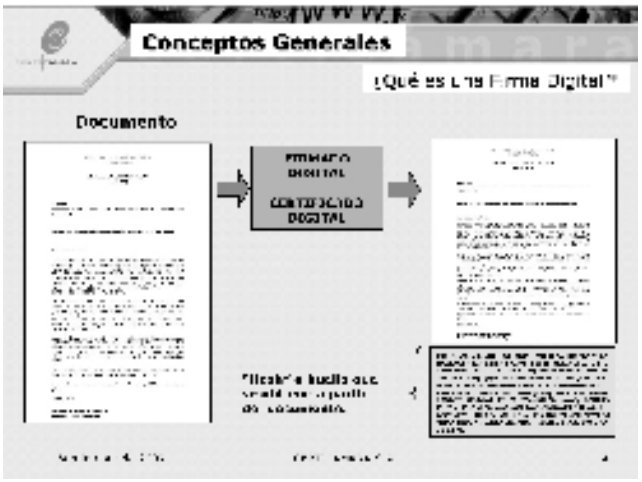

Figura 2. Representación de una firma digital

¿Para que sirve un certificado digital?

Garantizan la confidencialidad, autenticidad, integridad y no repudio en el envío de mensajes seguros al transmitirlos por medios inseguros, permiten firmar y cifrar (esto se hereda de la criptografía asimétrica), se entiende por gestión de certificados la emisión, renovación y revocación de certificados digitales. Una lista parcial de soluciones o aplicaciones de tipo PKI sería:

Aplicaciones de PKI

Soluciones internas:

- Gestión de certificado de servidor (web, correo, y otros)
- Gestión de certificados de usuario para empleados que permitan la autenticación contra un determinado servicio
- Gestión de certificados de atributos para empleados que permitan la autenticación y autorización contra una determinada aplicación/datos

Soluciones externas:

- Certificados de usuario para los empleados que permitan firmar correos entre entidades/empresas de confianza.
- Certificados de usuario para los empleados que permitan cifrar correos entre entidades/empresas de confianza.
- Proveer certificados de servidor a terceros (Prestador de Servicios de Certificación).

En resumen, las organizaciones requieren de una infraestructura de claves públicas por los siguientes requerimientos:

- Generación segura de buenas claves.
- Validación de identidad.
- Manejo del ciclo de vida de los certificados. Expedición, renovación y terminación de certificados.
- Validación de los certificados.
- Distribución de certificados.
- Suministro de la información asociada a un certificado digital.
- Almacenamiento seguro.
- Recuperación segura de claves.
- Generación de firmas y registro de tiempos.
- Administración de relaciones de confianza.
- Integración con las aplicaciones de la organización.
- Integración con el sistema de seguridad de la organización.

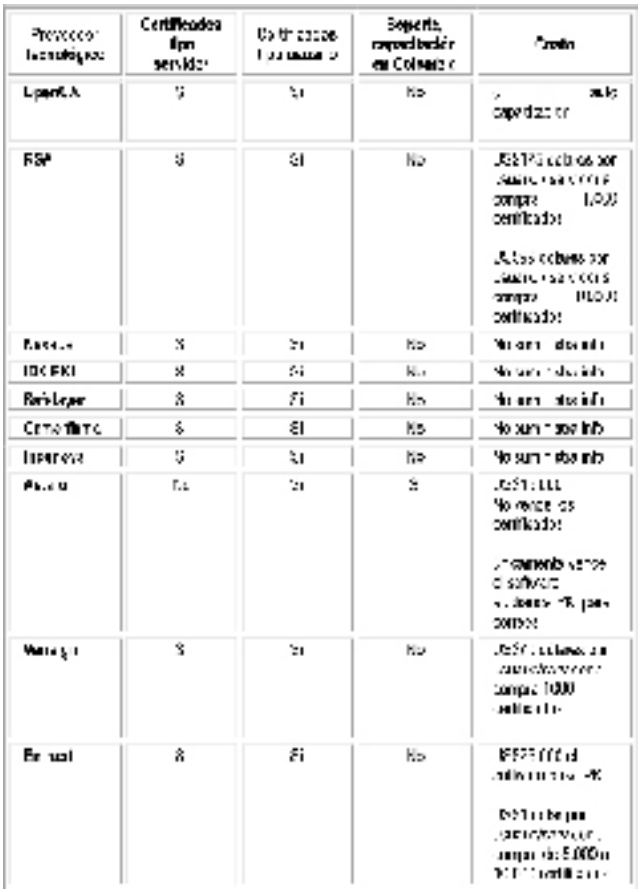

Tabla 1. Soluciones PKI

Diferentes soluciones PKI

Análisis de alternativas:

- Todos los proveedores consultados, en general cumplen con los dos tipos de certificados digitales requeridos, excepto el fabricante de UTM (administración centralizada de amenazas) Astaro, que es una solución europea especializada en PKI únicamente para la gestión de correos seguros respecto del negocio de las PKI. Su verdadero negocio son los cortafuegos de tipo UTM.

- Para el caso de Colombia y Sur América no existe soporte local excepto Astaro, que sí cuenta con un distribuidor local.

- En todas las soluciones se requiere un alto grado de conocimiento de PKI, es decir no es transparente para el usuario final, excepto Astaro que en forma transparente cifra y descifra los correos seguros. Astaro fue la única opción que incluía appliance y lo hacía transparentemente para el usuario final pero no tenía la opción de certificados de tipo servidor; es decir, no cumple con la totalidad de los requerimientos de la solución
- No hay precios homogéneos por solución, pues unos proveedores lo hacen por número de usuarios, otros por servidor y otros hacen combinaciones haciendo más compleja la tarea de comparar precios
- Se encuentran muy pocos proveedores locales expertos de servicios profesionales de OpenCA.

Selección de la alternativa propuesta por este documento:

Se selecciona la alternativa OpenCA por las siguientes razones:

- Posee un API que puede ser utilizado desde los lenguajes de desarrollo de software para que el programador pueda mejorar sus propias interfaces de gestión, el resto de proveedores evaluados no muestran la existencia de un API, para que el implementador mejore las características de cada opción
- En general, las opciones evaluadas no poseen soporte local lo que generaría dependencia tecnológica de estos proveedores que, en la mayoría de los casos, están en otros continentes, en cambio OpenCA por ser de tipo OpenSource permite que localmente se mejore la documentación y se hagan cambios específicos para la región, esto la hace una opción altamente deseable, según los requerimientos anteriormente enunciados
- Por ser OpenCA de licencia OpenSource no tiene costo de adquisición, sí hay costos de implementación y capacitación interna para aprender a manejar la herramienta.
- Con OpenCA la curva de aprendizaje es

más larga que la de los productos ya establecidos en otros países que ya tienen documentación y soporte probado en sus países de origen

- Definitivamente los precios de los certificados individuales y la poca integración con las aplicaciones es lo que ha hecho difícil la implementación de PKI pues, finalmente, es el usuario quien paga estos costos.
- Es una oportunidad única para aportar soluciones a la región en el tema específico de PKI con OpenCA.

Costos de la solución
Ver tabla 2.

Ítem	Costo en dólares americanos	Comentarios
Servidor PKI	3.700	No se cuenta con un servidor para [illegible], tampoco se cuenta con la versión de Linux SUSE 10 Enterprise Server con drivers para la SAN
Firewall UTM para proteger el servidor PKI y los PC(s) de la zona protegida PKI	300	Se cuenta con un Astaro 120 de propiedad de Globaltek para realizarlo. Sólo se debe seguir actualizando el mantenimiento anual Globaltek es distribuidor autorizado de este sistema de control
Para garantizar que únicamente los seriales de los tokens OTP/USB autorizados se autentiquen contra el servidor LDAP, se utilizará un software denominado "Sarend" de www.sarend.com que valide los seriales respectivos contra la base de datos de usuarios autorizados en el directorio de usuarios.	1.200	Globaltek es distribuidor autorizado de este sistema de control para dispositivos [illegible]
Administrador del servicio PKI como empresa independiente por un año [illegible] Instalación, mantenimiento y mejoras localizadas a la región del software OpenCA para una gestión gráfica más fácil.	36.000	US$3000 mensuales x 12 = US$36.000
UPS independiente del sistema central con capacidad de 4 KVA	2.000	
24 OTP/Smart cards para contener los certificados de cada individuo + 6 unidades de respaldo. Software para gestionar los tokens/Smart card.	1.200 1.200	Cada unidad cuesta US$40 x 30 unidades = 1.200 El software de gestión es crítico para llevar el ciclo de vida de los tokens
1 portátil para consola para administrar la solución PKI	3.000	Portátil Dell Inspiron E1505

Tabla 2. Relación de costos de la solución

Legislación sobre comercio electrónico, en Colombia

J. Resumen de leyes colombianas

Este es un resumen de las leyes expedidas, en Colombia, relacionadas con la regulación sobre las PKI:

Ley 527, de agosto de 1999, define y reglamenta el acceso y uso de mensajes de datos (MD), del comercio electrónico, firmas digitales y entidades de certificación (EC)

Decreto 1747 de 2000, reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. Las entidades de certificación requieren de permiso expreso de la Superintendencia de Industria y Comercio de Colombia para actuar como tal. El decreto 1747 decreta dos tipos de entidades de certificación:

- Entidad de certificación cerrada. Para el intercambio de mensajes de datos entre la entidad y el suscriptor, no tiene remuneración directa
- Entidad de certificación abierta. Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor, la entidad certificadora recibe remuneración por los servicios prestados

La Circular 011 de 2003, de Supervalores, que exige el uso de firmas digitales certificadas para el envío de reportes por los vigilados de esa entidad.

La Circular 643 de 2004, posibilita y fija las condiciones para la remisión de documentos de origen notarial, desde las notarías colombianas a las cámaras de comercio, utilizando firmas digitales.

La Circular 011 de 2004, de Supersalud, que exige el uso de firmas digitales certificadas para el envío de reportes de información financiera y general por parte de las IPS (Instituciones Prestadoras de Servicios privadas).

La Circular 012 de 2004, de Supersalud, que exige el uso de firmas digitales certificadas para el envío de reportes de información financiera y general por parte de las ESE (Empresas Sociales del Estado).

La Circular 013 de 2004, de Supersalud, que exige el uso de firmas digitales certificadas para el envío de reportes de información sobre el IVA (Impuesto de Valor Agregado) cedido al sector salud por parte de las gobernaciones, secretarias de hacienda, secretarias de salud y productores de licores entre otros.

La ley 794 de 2003, que se requirió para convalidar expresamente el uso de medios electrónicos y firmas digitales certificadas en el procedimiento civil. (En espera reglamentación)

La circular 27 del 26 de julio de 2004 de la Superintendencia Bancaria (hoy superfinanciera) que da paso a pruebas de comunicación, entre sus empresas vigiladas y la superintendencia, utilizando firmas digitales.

La circular externa 50 de 2003 del Ministerio de Industria y Comercio, establece la posibilidad del registro de importación a través de Internet. Este trámite puede hacerse de forma remota firmado digitalmente y de ese modo reducir el trámite que se piensa racionalizar por este medio.

Certificación digital Ley 962. Ley Antitrámite como: Medios tecnológicos en la Administración Pública, Derecho de Turno, Factura electrónica, Racionalización de la conservación de los libros del comerciante, Solicitud oficiosa por parte de las entidades públicas

Circular de Supersociedades. Dirigida a todas las sociedades mercantiles vigiladas y controladas por la superintendencia para el envío de información financiera y contable a través del sistema SIREM, el Sistema de Información y Riesgo Empresarial un sistema vía web que permite entregar todos los reportes e informes por esta vía, con el uso de certificados digitales.

El Sistema Integrado de Información Financiera SIIF - NACIÓN, en su labor misional de centralizar e integrar la operación financiera en línea de la mayor parte de las entidades que conforman el Presupuesto General de la Nación, con el fin de garantizar un sistema robusto de autenticación y gozar de garantías de autenticidad, no repudiación e integridad, ha incorporado a sus transacciones y reportes el uso de la Firma Digital, que ofrece un esquema de seguridad tecnológica y jurídica a las transacciones realizadas por las diferentes entidades dentro del sistema SIIF NACIÓN. En la actualidad, mas de 145 entidades del Estado firman las transacciones del presupuesto general de la nación.

Resoluciones DIAN. Las resoluciones que, hoy día, hacen posible la utilización de firmas digitales y/o electrónicas respaldadas con certificación digital, en la presentación de información tributaria por parte de diversos contribuyentes, permiten el uso de firma electrónica con certificación digital para ciertos grupos de usuarios delimitados por las siguientes resoluciones:

- Resolución No 10141 (28 Oct. 2005) Art. 10. Entidades vigiladas por la Superintendencia Bancaria
- Resolución No 10142 (28 Oct. 2005) Art. 6. Artículo 624 del Estatuto Tributario, que debe ser presentada por las cámaras de comercio
- Resolución No 10143 (28 Oct. 2005) Art. 5. Bolsas de valores y comisionistas de bolsa.
- Resolución No 10144 (28 Oct. 2005) Art. 4. Registraduría Nacional del Estado Civil.
- Resolución No 10145 (28 Oct. 2005) Art. 5. Notarios
- Resolución No 10146 (28 Oct. 2005) Art. 4. Personas o entidades que elaboren fac-

turas o documentos equivalentes.

- Resolución No 10147 (28 Oct. 2005) Art. 19. Grupo de personas naturales, personas jurídicas y demás entidades
- Resolución No 10148 (28 Oct. 2005) Art. 6. Grupos económicos y/o empresariales
- Resolución No 10149 (28 Oct. 2005) Art. 3. Suministrar mensualmente las entidades públicas o privadas que celebren convenios de cooperación y asistencia técnica para el apoyo y ejecución de sus programas o proyectos, con organismos internacionales

Próximamente, se establecerán las comunicaciones oficiales pertinentes para el registro sanitario, en línea del INVIMA, la presentación de reportes e informes de los vigilados de la Superintendencia Solidaria, SEC – Sistema Estadístico Cambiario del Banco de la República.

Consejo Superior de la Judicatura Acuerdo No. PSAA06-3334 de 2006 (marzo 2). "Por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia".

LA SALA ADMINISTRATIVA DEL CONSEJO SUPERIOR DE LA JUDICATURA

K. ¿Qué es Certicámara?[1]

Certicámara S.A, es una empresa filial de las Cámaras de Comercio y Confecámaras, fue creada en el año de 2001 y es la única entidad de certificación digital abierta en el país, autorizada y vigilada por la Superintendencia de Industria y Comercio. Certicámara es el tercero de confianza que garantiza la seguridad jurídica y tecnológica a las transacciones, comunicaciones, aplicaciones y en general a todo proceso de administración de la información digital.

Certicámara cumple con los más altos estándares internacionales exigidos por el American Institute of Certified Public Accountants (AICPA) y el Canadian Institute of Chartered Accountants (CISA), es auditada por la firma internacional Deloitte y obtuvo el sello WEB TRUST, que la califica como una entidad de certificación digital de clase mundial, así como el reconocimiento de Microsoft a sus productos y servicios a nivel mundial.

Productos y Servicios prestados por Certicámara

Certicámara, cuenta con un portafolio integrado de productos y servicios que permiten satisfacer las diferentes necesidades de seguridad jurídica y tecnológica que surgen a partir de los procesos de administración de la información digital:

Certificados digitales de firma:

- Certificado para representante legal
- Certificado de pertenencia empresa
- Certificado de funcionario público
- Certificado de profesional titulado
- Certificado de persona natural
- Certificado de firma de componentes de software (firma de código)

Certificados para seguridad en redes

- Certificado de servidor seguro (Certificado SSL) para el aseguramiento de sitios y aplicaciones Web
- Certificado de VPN para el aseguramiento de redes privadas virtuales
- Certificado de servidor seguro con firma automatizada, para el aseguramiento de aplicaciones que requieren la autenticación e integridad de mensajes de datos

Soluciones de certificación

Sistema Administrador de Firmas Digitales

[1]Nota: El autor en forma expresa agradece a Marcela Bello, directora comercial de Certicámara por los excelentes aportes realizados para este artículo sobre PKI (marcela.bello@certicamara.com).

(SAFD). Es un aplicativo que permite la gestión, recepción, verificación, clasificación, archivo y consulta de grandes volúmenes de documentos firmados digitalmente.

Estampado cronológico

El estampado cronológico es un servicio mediante el cual se puede garantizar la existencia de un documento (o mensaje de datos en general) en un determinado instante de tiempo. Mediante la emisión de una estampa de tiempo es posible garantizar el instante de creación, modificación, recepción, etc., de un determinado mensaje de datos impidiendo su posterior alteración, haciendo uso de la hora legal colombiana suministrada por la Superintendencia de Industria y Comercio.

Las soluciones de Certificación Digital ofrecidas por Certicámara brindan garantías de seguridad jurídica y técnica basadas en la aplicación de la tecnología PKI, dentro del marco legal y técnico para el uso de firmas y certificados digitales en el envío, recepción, archivo y procesamiento de mensajes de datos a partir de la Ley 527 de 1999, conocida como Ley de Comercio Electrónico y su decreto reglamentario 1747 de 2000, así como la Circular Única número 10, de la Superintendencia de Industria y Comercio.

En la actualidad, entidades financieras, estatales y privadas han implementado soluciones de certificación digital y habilitando el uso de firmas digitales al interior de sus sistemas y procedimientos, incorporando estrategias de seguridad jurídica y tecnológica en la administración de la información digital.

Estos son algunas organizaciones que ya cuentan con certificados públicos emitidos por la entidad certificadora colombiana:

Superintendencia Financiera, Superintendencia de Sociedades, Superintendencia Nacional de Salud, Ministerio de Hacienda y Crédito Público - SIIF Nación, Programa de las Naciones Unidas PNUD, Instituto Nacional de Vías – INVIAS, Procuraduría General de la Nación – Sistema SIRI, Aeronáutica Civil, Ministerio de Comercio, Industria y Turismo – Ventanilla Única de Comercio Exterior (VUCE), Instituto Nacional de Vigilancia de Medicamentos y Alimentos - INVIMA - Registro Sanitario en Línea, Wackenhut, Corporación Financiera Colombiana - Corficolombiana , Cámaras de Comercio y Confecámaras – Registro Único Empresarial (RUE), ACH Colombia S.A. – Botón Único de Pagos (PSE) y Giros y Finanzas S.A.

En la actualidad, Certicámara cuenta con un volumen importante de suscriptores, entre los cuales figuran: representantes legales, suplentes de representante legal, revisores fiscales, contadores, coordinadores de recaudo, oficiales de cumplimiento, directores jurídicos, coordinadores logísticos y tesoreros, entre otros. La mayoría de portales web colombianos han incorporado Certificados Digitales de Servidor Seguro para brindar a sus usuarios seguridad en sus transacciones. Igualmente, todos los comercios y entidades financieras que hacen parte de la red del Proveedor de Servicios Electrónicos (PSE) de ACH Colombia, incorporan certificados digitales de Certicámara al sistema de pagos electrónicos seguros.

Conclusiones

En general, las soluciones PKI siguen siendo costosas por la poca demanda de certificados digitales, se espera que al aumentar la demanda de certificados digitales, por fuerza natural aumente la oferta, es decir aumente el número de proveedores CA locales

Una forma de disminuirlos es combinar las PKI públicas con las PKI cerradas donde las empresas sólo compren un certificado a la CA raíz y en forma cerrada ese certificado garantice que los certificados que emita la entidad cerrada sean

válidos cuando los clientes lo usen contra la entidad cerrada para sus transacciones comerciales. Un ejemplo, sería un banco o entidad financiera que actúa como entidad cerrada y genera los certificados digitales a sus clientes con el objeto de que estos interactúen con el banco en forma segura pero avalada por la CA raíz local.

Es de mal gusto ver un mensaje en el explorador del usuario final indicando que el certificado digital no es confiable al no estar avalado por una CA raíz en la memoria cache del explorador, pues indica que debemos desconfiar de la transacción.

En general, se puede concluir que se requieren conocer muchas temáticas variadas como Openssl, Openldap, Apache, Linux, Tokens, Smart Cards y lenguajes de programación que deben ser integrados para que la solución sea funcional y segura. Esto hace que las PKI no sean fáciles de integrar a las aplicaciones

Falta aún que las aplicaciones hagan uso de los API, que permiten PKI entre aplicaciones.

Se han desarrollado programas en PHP sobre Apache y Linux para manejar un directorio de usuarios basados en OpenLDAP (single Sign On) y para este proyecto se ha preferido mejorar OpenCA o integrarse a su API, para generar las consultas y reportes que pasen datos al sistema de gestión de seguridad de la información.

Se disminuyen costos de adquisición de las herramientas licenciadas.

Apéndice

Laboratorio: Configuración de OpenCA
Prerrequisitos:

- Se debe tener instalado el Suse Linux Enterprise Server 10 con los siguientes componentes:
- Openssl, Openldap, Apache, DNS, Perl. Ver anexos respectivos.
- Para revisar la existencia de los mencionados paquetes se debe digitar:
- # rpm –q openldap2 openssl apache2 named perl
- Además, se deben configurar los dominios virtuales de Apache pues en un mismo servidor existirán los tres servicios: CA, RA-server y public
- El directorio de trabajo será /tmp para copiar y descomprimir los programas
- Cuando se instalen los paquetes, estos se instalaran por defecto en /usr/local/OpenCA
- Descargue de www.openca.org todos los módulos de openca con sus servicios adicionales como openca-ocspd.

Objetivo:

Configurar openCA como servicio de gestión para la empresa ficticia GPS, de Colombia.

Paso 1. Configurar el motor de base de datos
su – postgres
createuser –A –d –W openca
createdb –U openca –W openca

El usuario administrador es openca y la base de datos principal se llamará openca.

Paso 2. Copiar el esquema de base de datos LDAP
cp /tmp/openca-0.9*/contrib/openldap/openca.squema /etc/openldap/schema

Paso 3. Editar slapd.conf y registrar el nuevo esquema ldap
vi /etc/openldap/slapd.conf
Paso 4. Descomprimir los paquetes
cd /tmp
gunzip *

Paso 5. Instalar openca-tools antes de instalar openca
cd /tmp

tar –xvmf openca-tool*
cd openca-tool*
./configure
make
make install

Paso 6. Instalar openca-0.9.x después de instalar openca-tools
cd /tmp
tar –xvmf openca-0.9*
cd openca-0.9*
./configure
make
make install-offline
make install-online

Paso 7. Configurar openca según plantillas de tipo xml
vi /usr/local/openca/etc/config.xml
En este archivo existen secciones para la interface con LDAP, Apache y PosgresQL

Paso 8. Propagar los cambios desde las plantillas de tipo xml para la RA
. /usr/local/openca/etc/configure_etc.sh
Para subir el servicio digite:
. /usr/local/openca/etc/openca_rc start
Para bajar el servicio digite:
. /usr/local/openca/etc/openca_rc stop
No olvide subir los servicios apache, dns, ldap y posgresql

Paso 9. Probar las interfaces web de usuario.
En un explorador digite:
https://localhost/ca, para ver si la CA esta funcionando
https://localhost/ra, para ver si la RA esta funcionando
https://localhost/pub, para ver si la interface pública esta funcionando
https://localhost/ldap, para ver si la interface contra ldap esta funcionando
https://localhost/batch, para evaluar si funciona el procesamiento en lotes.

Paso 10. Instale servicios de openca, como openca-ocspd para informar en línea el estado del certificado
cd /tmp
tar –xvmf openca-ocspd*
cd openca-ocspd*
./configure
make
make install

Paso 11. Instale mas servicios de openca como libpki*:
cd /tmp
tar –xvmf libpki*
cd libpki*
./configure
make
make install

Paso 12. Instale más servicios de openca como libprq*:
cd /tmp
tar –xvmf libprq*
cd libprq*
./configure
make
make install.

Referencias

[1] PKI Infraestructura de claves públicas, Andrew Nash, Osborne McGraw-Hill, Enero 2002, ISBN: 958-41-0283-4
[2] Windows Server™ 2003 PKI and Certificate Security, Brian Komar, Microsoft, Julio 2004.

RFC's y estándares:

[3] PKIX Charter del IETF – http://www.ietf.org/html.charters/pkix-charter.html
[4] PKCS's – http://www.rsasecurity.com/rsalabs/pkcs

Proveedores tecnológicos – Software PKI:

[5] OpenCA – http://www.openca.org
[6] RSA – http://www.rsa.com
[7] Nexus – http://www.nexus-secured.com
[8] IDX-PKI – http://idx-pki.idealx.org/faq.en.html
[9] SafeLayer – http://www.safelayer.com

Proveedores tecnológicos – Tokens criptográficos:

[10] • Rainbow – http://www.rainbow.com
[11] • Aladdin – http://www.ealaddin.com
[12] • Setec – http://www.setec.fi
[13] • nCipher – http://www.ncipher.com