

PKI – Un modelo de Seguridades para e-commerce.

AUTOR:

Ing. Juan Fernando Galárraga Hurtado, MsC ¹

RESUMEN:

El número de usuarios de Internet ha experimentado en los últimos años un increíble aumento debido en parte a la mejora de los servicios y al abaratamiento de los costos. Este hecho ha sido aprovechado por el mundo empresarial, que está utilizando cada vez más Internet como medio de difusión para dar a conocer sus productos y ofrecer sus servicios. Sin embargo, este fenómeno ha puesto al descubierto una de las mayores deficiencias de Internet: su seguridad.

Los protocolos sobre los que se ha construido el Internet no ofrecen ningún tipo de seguridad; un paquete viaja por varias redes hasta alcanzar su destino y es fácil leerlo, o incluso modificarlo, lo cual es un problema cuando la información que se transmite es especialmente sensible: datos personales, número de tarjeta de crédito, etc. Reconociendo este problema, la sociedad de la información debe dotar a sus miembros de los mecanismos básicos de seguridad: autenticación, integridad y confidencialidad en las comunicaciones sobre Internet.

Esta Ponencia describe los conceptos de Infraestructura de Clave Pública, las aplicaciones PKI y su impacto en la sociedad las mismas que proporcionan una base para el desarrollo del comercio electrónico en un entorno seguro.

INTRODUCCIÓN

La criptografía protege a los usuarios de Internet ya que proporciona funciones de cifrado de datos y de autenticación de otros servicios. Esta ciencia permite al receptor de un mensaje electrónico comprobar la identidad del emisor, asegura que un mensaje sólo puede leerlo la persona a la que va dirigido y asegura al destinatario que un mensaje no ha sufrido ninguna alteración durante su envío.

La criptografía es esencial para realizar intercambios de información seguros en intranets, extranets e Internet. Desde un punto de vista empresarial, las funciones de seguridad que permite la criptografía son autenticación, que asegura al destinatario de un mensaje que el remitente es quien dice ser; confidencialidad, que asegura que un mensaje sólo puede ser leído por el destinatario previsto e integridad, que asegura que durante la transmisión no se ha alterado el destinatario de un mensaje. Desde un punto de vista técnico, la criptografía es la ciencia que se encarga de la protección de datos mediante la transformación matemática de los mismos a un formato ilegible.

Las Infraestructuras que usan Criptografía simétrica se han ensayado y han fracasado debido a problemas de manejo, escalabilidad y ciclo de vida que presentan. En cambio, en la criptografía asimétrica, cada entidad sólo ha de poseer un par de claves (pública y privada) independientemente del número de sistemas con los que se comunique. El único requisito que se ha de cumplir es la integridad de la clave,

¹ ESPE – Departamento de Ciencias de la Computación.
Mail: fgalarraga@espe.edu.ec
Teléfono: 098134524

para así evitar que un posible atacante sustituya una clave pública y suplante a su usuario legítimo (ataque man-in-the-middle).

Para evitar lo descrito anteriormente, se recurre a lo que se denominan los certificados de clave pública, que son emitidos por terceras partes de confianza llamadas Autoridades Certificadoras (CAs, Certification Authorities) y que garantizan que una determinada clave pública pertenece a su verdadero propietario.

En consecuencia, Una PKI permite a una organización desplegar servicios de seguridad que se basan en el cifrado simétrico y asimétrico. Esta característica permite crear entidades de confianza que se requieren para los procesos de identificación y autenticación en una organización o en un sector de mercado vertical (por ejemplo: los abogados utilizan certificados digitales expedidos por la asociación de abogados).

Las Autoridades Certificadoras garantizan los servicios de confidencialidad e integridad de los datos, el no repudio de origen y destino, así como la autenticación e identidad univoca del signatario. Como PKI se interesa principalmente en la creación de identidades de confianza, que se utilizan como la base de otros servicios de seguridad por niveles jerárquicos, muchas empresas quieren mantener el control directo de todos los aspectos de la expedición de las identidades. Es por esta razón que en un modelo de confianza se requiere definir, en algunos casos, un segmento de mercado vertical que pueda desarrollar su propia infraestructura para uso de los miembros de una asociación, en otros casos, se puede esperar que cada empresa opere su propia Infraestructura de Claves Públicas.

En el terreno de las seguridades informáticas, las nuevas tecnologías basadas en infraestructuras de clave pública (PKI) son las únicas alternativas que permiten cubrir las carencias de seguridad del Internet, las mismas que afectan a la protección de la información que fluye a través de la red de redes.

El término PKI básicamente describe la gestión de los certificados digitales basada en criptografía de clave pública y terceras partes de confianza, proporcionando a los usuarios de mecanismos de seguridad que garanticen la autenticación, integridad y confidencialidad en las comunicaciones sobre Internet.

En la práctica, una infraestructura de claves públicas hace referencia a un sistema de certificados digitales, entidades emisoras de certificados (CA) y entidades de registro (RA) que comprueban y autentican la validez de cada parte implicada en una transacción electrónica. Los estándares de la infraestructura de claves públicas siguen evolucionando, aunque se estén implementando de forma generalizada como elemento necesario del comercio electrónico.

La tecnología PKI se basa en estándares aceptados por la comunidad internacional por lo que se hace necesario conocer y aplicar las recomendaciones X.509 de la ITU (Unión Internacional de Telecomunicaciones) y los estándares PKCs de RSA Laboratorios, el cuerpo de trabajo más importante se ha logrado en el grupo de trabajo de IETF (Grupo de Trabajo de Ingeniería de Internet) a través del modelo PKIX. Otros grupos de la industria y del gobierno han trabajado para definir perfiles y modelos operacionales que se ajusten más a las especificaciones de PKI según las necesidades de sus organizaciones en cuanto a seguridad y comercio electrónico.

La criptografía de clave pública es la parte fácil, la Infraestructura de Claves Públicas (PKI) es el desafío actual.

CONCLUSIONES

- Una PKI es la combinación de productos de hardware y software, políticas y procedimientos tendientes a proveer una alta seguridad al intercambio de información validada a través de redes públicas o redes corporativas.
- La Infraestructura de Claves Públicas se basa en identificaciones digitales, también conocidas como certificados digitales, los cuales actúan como pasaportes electrónicos vinculando a un usuario de firma digital con su clave pública. Debido a la característica impersonal involucrada en este tipo de tecnología, es que se hace necesario contar con medios que garanticen una efectiva identificación y autenticación de los usuarios participantes con el fin de poder lograr el no repudio de las operaciones realizadas. Por esta razón, en todo momento, se debe garantizar la confidencialidad e integridad de las transacciones que viajan por Internet.
- El trabajo para establecer una PKI requiere de un esfuerzo significativo en la planeación de un modelo de gestión, por lo que surge la necesidad de preguntarnos ¿Cuáles serán las decisiones que los administradores de IT deberán tomar para instituir una PKI corporativa? Es por esta razón, que se requiere determinar un conjunto de políticas para expedir los certificados digitales, procedimientos para establecer la seguridad del ambiente en donde opera y las directivas para la administración del ciclo de vida de los certificados digitales en la organización.

RECOMENDACIONES

- Para trabajos futuros se requiere Investigar y fomentar en la Universidades y Escuelas Politécnicas que pertenecen al Sistema de Educación Superior del Ecuador, el uso de las aplicaciones PKI:
 - ✓ Tarjetas Inteligentes
 - ✓ e-DNI
 - ✓ Notario electrónico
 - ✓ Single sig-on

PALABRAS CLAVE

- ✓ PKI
- ✓ Certificado Digital
- ✓ Criptografía
- ✓ Firma digital
- ✓ Autoridad Certificadora

REFERENCIAS

- COMPUTER SECURITY INSTITUTE/FBI , Computer Crime and Security,
- ENTERPRISE MANAGEMENT ASSOCIATES, Security Strategies, Internet. <http://techupdate.zdnet.com/techupdate/filters/specialreport/0,14622,6022871,00.html>.
- EORIGNAL, Applying PKI to Business Applications, Internet. <http://www.intiss.com/ecaug/pki200005.ppt>.
- Ley de Comercio Electrónico, Firmas digitales y mensajes de datos.
- Reglamento a la Ley de comercio electrónico del Ecuador.

PKI – Un modelo de Seguridades para e-commerce.

AUTOR:

Ing. Juan Fernando Galárraga Hurtado, MsC ²

RESUMEN:

El número de usuarios de Internet ha experimentado en los últimos años un increíble aumento debido en parte a la mejora de los servicios y al abaratamiento de los costos. Este hecho ha sido aprovechado por el mundo empresarial, que está utilizando cada vez más Internet como medio de difusión para dar a conocer sus productos y ofrecer sus servicios. Sin embargo, este fenómeno ha puesto al descubierto una de las mayores deficiencias de Internet: su seguridad.

Los protocolos sobre los que se ha construido el Internet no ofrecen ningún tipo de seguridad; un paquete viaja por varias redes hasta alcanzar su destino y es fácil leerlo, o incluso modificarlo, lo cual es un problema cuando la información que se transmite es especialmente sensible: datos personales, número de tarjeta de crédito, etc. Reconociendo este problema, la sociedad de la información debe dotar a sus miembros de los mecanismos básicos de seguridad: autenticación, integridad y confidencialidad en las comunicaciones sobre Internet.

Esta Ponencia describe los conceptos de Infraestructura de Clave Pública, las aplicaciones PKI y su impacto en la sociedad las mismas que proporcionan una base para el desarrollo del comercio electrónico en un entorno seguro.

INTRODUCCIÓN

La criptografía protege a los usuarios de Internet ya que proporciona funciones de cifrado de datos y de autenticación de otros servicios. Esta ciencia permite al receptor de un mensaje electrónico comprobar la identidad del emisor, asegura que un mensaje sólo puede leerlo la persona a la que va dirigido y asegura al destinatario que un mensaje no ha sufrido ninguna alteración durante su envío.

La criptografía es esencial para realizar intercambios de información seguros en intranets, extranets e Internet. Desde un punto de vista empresarial, las funciones de seguridad que permite la criptografía son autenticación, que asegura al destinatario de un mensaje que el remitente es quien dice ser; confidencialidad, que asegura que un mensaje sólo puede ser leído por el destinatario previsto e integridad, que asegura que durante la transmisión no se ha alterado el destinatario de un mensaje. Desde un punto de vista técnico, la criptografía es la ciencia que se encarga de la protección de datos mediante la transformación matemática de los mismos a un formato ilegible.

Las Infraestructuras que usan Criptografía simétrica se han ensayado y han fracasado debido a problemas de manejo, escalabilidad y ciclo de vida que presentan. En cambio, en la criptografía asimétrica, cada entidad sólo ha de poseer un par de claves (pública y privada) independientemente del número de sistemas con los que

² ESPE – Departamento de Ciencias de la Computación.
Mail: fgalarraga@espe.edu.ec
Teléfono: 098134524

se comuniquen. El único requisito que se ha de cumplir es la integridad de la clave, para así evitar que un posible atacante sustituya una clave pública y suplante a su usuario legítimo (ataque man-in-the-middle).

Para evitar lo descrito anteriormente, se recurre a lo que se denominan los certificados de clave pública, que son emitidos por terceras partes de confianza llamadas Autoridades Certificadoras (CAs, Certification Authorities) y que garantizan que una determinada clave pública pertenece a su verdadero propietario.

En consecuencia, Una PKI permite a una organización desplegar servicios de seguridad que se basan en el cifrado simétrico y asimétrico. Esta característica permite crear entidades de confianza que se requieren para los procesos de identificación y autenticación en una organización o en un sector de mercado vertical (por ejemplo: los abogados utilizan certificados digitales expedidos por la asociación de abogados).

Las Autoridades Certificadoras garantizan los servicios de confidencialidad e integridad de los datos, el no repudio de origen y destino, así como la autenticación e identidad unívoca del signatario. Como PKI se interesa principalmente en la creación de identidades de confianza, que se utilizan como la base de otros servicios de seguridad por niveles jerárquicos, muchas empresas quieren mantener el control directo de todos los aspectos de la expedición de las identidades. Es por esta razón que en un modelo de confianza se requiere definir, en algunos casos, un segmento de mercado vertical que pueda desarrollar su propia infraestructura para uso de los miembros de una asociación, en otros casos, se puede esperar que cada empresa opere su propia Infraestructura de Claves Públicas.

En el terreno de las seguridades informáticas, las nuevas tecnologías basadas en infraestructuras de clave pública (PKI) son las únicas alternativas que permiten cubrir las carencias de seguridad del Internet, las mismas que afectan a la protección de la información que fluye a través de la red de redes.

El término PKI básicamente describe la gestión de los certificados digitales basada en criptografía de clave pública y terceras partes de confianza, proporcionando a los usuarios de mecanismos de seguridad que garanticen la autenticación, integridad y confidencialidad en las comunicaciones sobre Internet.

En la práctica, una infraestructura de claves públicas hace referencia a un sistema de certificados digitales, entidades emisoras de certificados (CA) y entidades de registro (RA) que comprueban y autentican la validez de cada parte implicada en una transacción electrónica. Los estándares de la infraestructura de claves públicas siguen evolucionando, aunque se estén implementando de forma generalizada como elemento necesario del comercio electrónico.

La tecnología PKI se basa en estándares aceptados por la comunidad internacional por lo que se hace necesario conocer y aplicar las recomendaciones X.509 de la ITU (Unión Internacional de Telecomunicaciones) y los estándares PKCs de RSA Laboratorios, el cuerpo de trabajo más importante se ha logrado en el grupo de trabajo de IETF (Grupo de Trabajo de Ingeniería de Internet) a través del modelo PKIX. Otros grupos de la industria y del gobierno han trabajado para definir perfiles y modelos operacionales que se ajusten más a las especificaciones de PKI según las necesidades de sus organizaciones en cuanto a seguridad y comercio electrónico.

La criptografía de clave pública es la parte fácil, la Infraestructura de Claves Públicas (PKI) es el desafío actual.

CONCLUSIONES

- Una PKI es la combinación de productos de hardware y software, políticas y procedimientos tendientes a proveer una alta seguridad al intercambio de información validada a través de redes públicas o redes corporativas.
- La Infraestructura de Claves Públicas se basa en identificaciones digitales, también conocidas como certificados digitales, los cuales actúan como pasaportes electrónicos vinculando a un usuario de firma digital con su clave pública. Debido a la característica impersonal involucrada en este tipo de tecnología, es que se hace necesario contar con medios que garanticen una efectiva identificación y autenticación de los usuarios participantes con el fin de poder lograr el no repudio de las operaciones realizadas. Por esta razón, en todo momento, se debe garantizar la confidencialidad e integridad de las transacciones que viajan por Internet.
- El trabajo para establecer una PKI requiere de un esfuerzo significativo en la planeación de un modelo de gestión, por lo que surge la necesidad de preguntarnos ¿Cuáles serán las decisiones que los administradores de IT deberán tomar para instituir una PKI corporativa? Es por esta razón, que se requiere determinar un conjunto de políticas para expedir los certificados digitales, procedimientos para establecer la seguridad del ambiente en donde opera y las directivas para la administración del ciclo de vida de los certificados digitales en la organización.

RECOMENDACIONES

- Para trabajos futuros se requiere Investigar y fomentar en la Universidades y Escuelas Politécnicas que pertenecen al Sistema de Educación Superior del Ecuador, el uso de las aplicaciones PKI:
 - ✓ Tarjetas Inteligentes
 - ✓ e-DNI
 - ✓ Notario electrónico
 - ✓ Single sig-on

PALABRAS CLAVE

- ✓ PKI
- ✓ Certificado Digital
- ✓ Criptografía
- ✓ Firma digital
- ✓ Autoridad Certificadora

REFERENCIAS

- COMPUTER SECURITY INSTITUTE/FBI , Computer Crime and Security,
- ENTERPRISE MANAGEMENT ASSOCIATES, Security Strategies, Internet. <http://techupdate.zdnet.com/techupdate/filters/specialreport/0,14622,6022871,00.html>.
- EORIGNAL, Applying PKI to Business Applications, Internet. <http://www.intiss.com/ecaug/pki200005.ppt>.
- Ley de Comercio Electrónico, Firmas digitales y mensajes de datos.
- Reglamento a la Ley de comercio electrónico del Ecuador.

**II CONGRESO DE CIENCIA Y TECNOLOGÍA ESPE - 2007
30-31 DE MAYO Y 1 DE JUNIO DE 2007**

BIOGRAFÍA

TEMA

PKI – Un modelo de Seguridades para e-commerce

NOMBRE

Ing. Juan Fernando Galárraga Hurtado, MsC

ESTUDIOS

PREGRADO: Ingeniería en Sistemas e Informática - ESPE

POSTGRADO: Diplomado En Docencia Universitaria – ESPE

Especialista en Comercio Electrónico – EPN

Master en Ciencias de la Computación - EPN

EXPERIENCIA LABORAL / PUBLICACIONES DESTACADAS

DOCENCIA UNIVERSITARIA:
ESPE – USFQ – UDLH

CONFERENCIAS DICTADAS:

BUSINESS INTELLIGENCE, UN NUEVO PARADIGMA DE HACER NEGOCIOS POR INTERNET. III Congreso de Ciencias de la Computación (Manta –2005).

FORMAS DE PAGO PARA E-COMMERCE. III Congreso Nacional de Informática (ESPE 2006).

SEGURIDADES EN COMERCIO ELECTRÓNICO. II Convención de Informática (Quito 2006).