Certificados digitales

Johnny Herrera Acebey, Daniel Fernández Terrazas

Departamento de Ciencias Exactas e Ingeniería, Universidad Católica Boliviana
Av. General Galindo s/n, Cochabamba, Bolivia

e-mail: herrera@ucbcba.edu.bo, djft@ucbcba.edu.bo

1. Introducción

Los sistemas que ofrecen servicios mediante Internet requieren de confianza, privacidad y seguridad entre ellos y sus clientes. El problema de la identificación de personas o sistemas que usan medios de comunicación no fiables se puede resolver usando certificados digitales. En este artículo se presenta un estudio de los certificados digitales.

2. Definición de certificado digital

Los sistemas de control de acceso basados en criptografía utilizan un concentrado de información denominado, por Kohnfelder, certificado digital [12], que se usa para demostrar la identidad y los atributos de su poseedor antes de permitirle el acceso a un sistema en Internet.

El objetivo principal de un certificado digital es restringir el acceso a un sistema basado en un proceso de autorización para evitar la suplantación de un usuario. Un certificado digital permite también detectar si una transacción ha sido alterada durante la transmisión, consiguiendo de este modo garantizar la integridad de un mensaje [13].

3. Tipos de certificados

3.1. Certificados de identidad

Dos entidades que poseen claves privadas y que desean intercambiar datos con confianza mediante un medio no fiable pueden asociar esas claves con una clave pública e integrarla en un certificado digital de identidad. Los certificados de identidad son estructuras de datos que tienen un contenido datos usado para reconocer a un sujeto (persona, objeto o máquina) y tienen la propiedad de conectar una entidad con su clave pública[6].

Los certificados de clave pública son emitidos por autoridades de certificación (AC) y representan una evidencia que asegura el vínculo (pertenencia) de la clave pública con los datos de identidad declarados en el mismo, evidencia que puede ser demostrada (probada) mediante un proceso de verificación técnica que consiste en la presentación de una clave privada o una afirmación hecha por el sujeto. Las autoridades de certificación son organizaciones seguras que administran las firmas digitales de clave pública y proporcionan servicios de consulta. Estos servicios permiten la verificación de firmas para asegurar que una entidad sea considerada legítima o no niegue su identidad (X.509).

Los certificados de identidad de clave pública son utilizados en un proceso de control de acceso para legitimar a su propietario (autentificación). La distribución de las claves públicas y los certificados requieren de una infraestructura denominada de clave pública (Public Key Infraestructure, PKI). La ITU mediante el estándar X.509 define y describe esta forma de administración de claves.

3.2. Certificados de atributo

El proceso de control de acceso puede usar la información contenida en estructuras de datos, denominados certificados de atributo, no sólo para comprobar la identidad de un sujeto sino también sus roles. Los certificados de atributo tienen una estructura de datos similar a la de un certificado de identidad [2]. La diferencia está en que los certificados de atributo no contienen una clave pública, en lugar de ella incluyen atributos que especifican información de control de acceso asociado con el poseedor del certificado. En el proceso de autorización las decisiones no sólo se basan en la verificación de identidad sino también en la verificación de roles, reglas y control de acceso basado en el rango. Los certificados de atributo permiten asociar información de identidad con información de autorización que no es de identidad [6].

Esta forma de control de acceso permite restringir de acuerdo al perfil de los usuarios y así agregar a los sistemas mayor grado de fiabilidad. La información de control de acceso puede utilizarse en un proceso de autorización para validar dinámicamente un certificado y prescindir de la revocación de certificados manejando cortos períodos de vida de un certificado.

Las autoridades de atributos son entidades responsables de emitir certificados de atributo al igual que las autoridades de certificación de certificados de clave pública.

3.3. Otros tipos de certificados

Los sistemas basados en la identidad son una opción pero no una solución al problema de dar confianza, existen otras propiedades además de la identidad (edad, dirección, nacionalidad, estado civil y otros) que son relevantes para establecer confianza entre las partes involucradas. Estos son los sistemas de credencial digital [9]. Stefan Brands introduce el concepto de credenciales digitales como certificados de atributo de privacidad-mejorada [12]. Considerando que las infraestructuras de certificados de clave

pública ignoran la privacidad de la identidad de las personas, Zero-Knowledge Systems en noviembre de 2000 publicó su visión de las credenciales privadas. También existen otros modelos conceptuales que son SPKI (Simple Public Key Infraestructure) y PGP (Pretty God Privacy). Una comparación de sistemas de certificación se presenta en el trabajo de E. Gerck, quien afirma que los métodos de certificación absoluta son lógicamente imposibles, porque un certificado no puede certificarse así mismo [3].

4. Definición y funciones de las autoridades de certificación

"Una autoridad de certificación (AC) es definida como una autoridad que ha recibido confianza de uno o más usuarios para crear y asignar certificados" [X.509]. Las AC tienen la facultad de certificar la correspondencia entre una entidad y una clave pública. Sin embargo, semánticamente una AC no es capaz de denotarla [3]. La AC se constituye en la tercera parte confiable, frente a las entidades que se comunican (emisor y receptor). Entre las autoridades de certificación más conocidas se tienen a: Verisign, Thawte, GeoTrust, RapidSSL y DigiCertSSL

Todas las Autoridades de Certificación deben mantener una base de datos de nombres distinguidos (ND) para usuarios o AC subordinadas y tomar las medidas para asegurar que ninguna autoridad emita duplicados de ND. Las funciones más importantes que realizan las autoridades de certificación son:

- Registro de usuarios: tienen la responsabilidad de gestionar la información de identidad de los usuarios.
- Emisión de certificados: deben generar los certificados que enlacen a un usuario con una clave pública.
- Administración de certificados: además de registrar deben controlar atributos de los certificados para tomar decisiones de revocación, renovación y suspensión.
- Servicio de consulta: deben ofrecer servicios a los usuarios para facilitar el seguimiento sobre el estado de los certificados.
- Administración de las firmas: deben ofrecer mecanismos para la generación de claves usando algoritmos de cifrado de mensajes.

5. Jerarquía de certificación

La jerarquía de autoridades de certificación se define en el documento RFC 1422. Este estándar establece una estructura jerárquica rígida de AC. En la estructura se definen tres tipos de autoridades de certificación:

a) Internet Policy Registration Authority (IPRA): Esta autoridad es la más alta (raíz) de la jerarquía de certificación PEM. La actuación de esta autoridad es a nivel 1 y sólo se le está permitido emitir certificados para el siguiente nivel

de autoridad (PCA). Todo proceso de certificación comienza en una autoridad IPRA.

b) Policy Certification Authorities (PCA): las autoridades PCA actúan a nivel 2 de la jerarquía. Cada autoridad PCA debe estar certificada por una autoridad IPRA. Una autoridad PCA debe establecer y declarar su política respecto a los usuarios o subautoridades de certificación. Está permitida la existencia de distintas autoridades PCA para responder necesidades específicas de los usuarios.

c) Certification Authorities (CA). las autoridades CA están ubicadas a nivel 3 y pueden funcionar a niveles inferiores. Las autoridades que están a nivel 3 tienen que recibir la certificación de una autoridad del nivel 2.

Una regla de designación de nombres también está definida en RFC 1422, además, ésta establece que una autoridad CA sólo puede emitir certificados para entidades cuyos nombres se subordinan al nombre de la misma autoridad CA. A partir de esta regla se puede hacer un seguimiento de encadenamiento de autoridades de certificación.

6. Revocación de certificados

Después de la emisión de un certificado por parte de una autoridad de certificación, es posible que se haya puesto en peligro la clave privada del titular del certificado o que se haya utilizado información falsa para solicitar el certificado. En estos y otros casos surge la necesidad de dar a las autoridades de certificación la facultad de retirar un certificado ya emitido.

Las listas de revocación de certificados (CRL) son un mecanismo mediante el cual la CA publica y distribuye información acerca de los certificados anulados a las aplicaciones que los emplean. Una CRL es una estructura de datos firmada por la CA que contiene la fecha y hora de su publicación, el nombre de la entidad certificadora y los números de serie de los certificados anulados que aún no han expirado. Cuando una aplicación trabaja con certificados debe obtener la última CRL de la entidad que firma el certificado que está empleando y comprobar que su número de serie no está incluido en dicha lista [13].

Existen varios métodos para la actualización de CRLs:

- Muestreo de CRLs. Las aplicaciones acceden a la CA o a los almacenes de archivos y copian el último CRL en intervalos regulares.
- Anuncio de CRLs. La entidad certificadora anuncia que ha habido un cambio en el CRL a las aplicaciones. El problema de este enfoque es que el anuncio puede ser muy costoso y no se sabe qué aplicaciones deben ser informadas.

- Verificación en línea. Una aplicación hace una consulta en línea a la CA para determinar el estado de revocación de un certificado. Es el mejor método para las aplicaciones, pero es muy costoso para la CA.

7. Tipos de certificados de clave pública

Existen cuatro tipos de certificados de clave pública: certificados de autoridad, certificados de servidor, certificados de usuario (personales) y certificados de productores de software:

a) Certificados de autoridad. Las entidades emisoras de certificados raíz tienen la capacidad de asignar certificados a certificados de autoridad. Corresponden a entidades que certifican. Los certificados raíz son los únicos auto-firmados y son los que inician una cadena de certificación de acuerdo a la jerarquía definida en el estándar X.509.

b) Certificado de servidor. Certifica que un servidor es de la empresa que dice ser y que el identificador del servidor es correcto. Los certificados de servidor identifican a servidores que participan en comunicaciones seguras con otros equipos mediante la utilización de protocolos de comunicaciones. Estos certificados permiten al servidor probar su identidad ante los clientes.

c) Certificados personales. Los certificados personales aseguran que una dirección de correo y clave pública corresponden a una persona. Estos certificados identifican a personas y se pueden utilizar para autenticar usuarios con un servidor.

d) Certificados de productores de software. Se utilizan para "firmar" el software y asegurar que no ha sido modificado. Esto no implica que se pueda ejecutar con seguridad, pero informa al usuario que el fabricante de software participa en la infraestructura de compañías y entidades emisoras de certificados de confianza. Estos certificados se utilizan para firmar el software que se distribuye por Internet.

8. Componentes de un certificado de clave pública

Los componentes de un certificado X.509 son: el descriptor del certificado, la firma digital y un valor de firma. Los elementos del descriptor son [13]:

- **Versión.** Contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
- **Número de serie.** Es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
- **Identificador del algoritmo de firmado.** Identifica el algoritmo empleado para firmar el certificado.

- **Nombre del emisor.** Identifica la CA que ha firmado y emitido el certificado.
- **Periodo de validez.** Indica el periodo de tiempo durante el cual el certificado es válido. Nombre del sujeto. Identifica el nombre del usuario para el que se emite el certificado.
- **Nombre del sujeto.** Indica el nombre del usuario para el cual se emite el certificado.
- **Información de clave pública del sujeto.** Información de la clave pública del usuario para el que se emite el certificado (nombre, algoritmo, etc.).
- **Identificador único del emisor.** Es un campo opcional que permite reutilizar nombres de emisor.
- **Identificador único del sujeto.** Es un campo opcional que permite reutilizar nombres de sujeto.
- **Extensiones.** Otros campos específicos de cada protocolo que están sujetos a sus propias regulaciones.

9. Nombrado de entidades en certificados de clave pública

El nombrado de entidades en los certificados de X.509 se hace en función de nombres distinguidos (ND). Un ND es un conjunto de atributos con valores asociados. El RFC PKIX presenta una serie de atributos obligatorios en los ND [1].

10. Propiedades de los certificados de clave pública

Las características más importantes de los certificados digitales son:

- **Autentificación.** Para el receptor de un documento, la autentificación implica asegurar que los datos recibidos han sido enviados por quien declara ser poseedor de la identidad contenida en la firma digital.
- **Confidencialidad**. La confidencialidad implica asegurar que la información enviada no podrá ser interceptada por terceros.
- **Integridad**. La integridad de los documentos implica tanto para el remitente como para el destinatario asegurar que la información enviada no será modificada por terceros.
- **Privacidad**. La privacidad de los mensajes implica que los datos sólo podrán ser leídos por el destinatario por contener elementos cifrados.
- **No repudio**. El no repudio implica para el receptor de un mensaje asegurar que el emisor no negará haber enviado la información recibida.

10.1. Autentificación

La autentificación de claves asimétricas permite que un mensaje cifrado con una clave privada sólo pueda haber sido enviado por el propietario de la misma.

10.2. Confidencialidad

Para lograr la confidencialidad, el remitente (emisor) de un mensaje debe cifrarlo con la clave pública del destinatario (receptor), que puede obtenerse de su Certificado Digital. De esta forma el emisor se asegura que el mensaje sólo podrá ser descifrado con la clave privada del receptor, es decir, sólo podrá ser leído por el destinatario.

10.3. Integridad

Para garantizar la integridad, el remitente antes de enviar un mensaje aplica un algoritmo hash. De esta forma, al enviar un mensaje, el emisor envía el resultado del hashing cifrado junto con el mensaje original. Cuando el destinatario recibe el mensaje, recalcula el hashing del mensaje y lo compara si es igual al hashing recibido, para comprobar si el mensaje no ha sido modificado.

10.4. No repudio

También como consecuencia directa del concepto de firma digital, la sola existencia del mensaje "firmado" por su clave privada, una vez comprobada su integridad, impide al emisor el repudio del mensaje, ya que el mismo no podría haberse generado por otra vía. El receptor conserva el documento firmado como comprobante de la operación.

11. Generación e instalación de certificados

Los certificados digitales sólo son útiles si existe alguna autoridad de certificación que los valide. Si un certificado es auto-firmado no hay ninguna garantía de que su identidad sea la que anuncia, por tanto, no debe ser aceptada por un tercero que no lo conozca [13]. Entonces, la seguridad comienza cuando las dos entidades confían en la misma CA. Esto permite a ambas partes conocer la clave pública de la otra, al intercambiar certificados firmados por esa autoridad emisora de certificados. Una vez que cada entidad conoce la clave pública de la otra, pueden utilizarla junto a su clave privada (par de claves) para cifrar datos y enviarlos a la otra o para comprobar las firmas contenidas en los documentos.

Una autoridad de certificación debe comprobar la identidad de una entidad solicitante de un certificado antes de emitirlo. Después, la autoridad de certificación firma el certificado con su clave privada, que se utiliza para comprobar el certificado. Las claves públicas de una autoridad de certificación se distribuyen en aplicaciones, por ejemplo, exploradores Web y correo electrónico, aunque también las puede agregar manualmente el usuario.

Proceso de certificación digital:

a) Generación de la clave. La entidad que solicita la certificación (el solicitante, no la entidad emisora) para generar pares de claves públicas/privadas y algoritmos de cifrado. La clave pública puede ser la misma que tiene la autoridad de certificación.

b) Encapsulado de las firmas. El solicitante empaqueta la información de identidad y los atributos necesarios para que la autoridad de certificación emita el certificado.

c) Envío de las claves públicas y la información. El solicitante envía las dos claves y la información a la autoridad de certificación.

d) Comprobación de la información. La autoridad de certificación utiliza la información enviada por el solicitante para tomar la decisión de emitir el certificado.

e) Creación del certificado. La autoridad de certificación crea un documento digital que contiene la información atribuida a la entidad solicitante y lo firma con su clave privada.

f) Envío y publicación del certificado. La autoridad de certificación puede enviar el certificado al solicitante o publicarlo si resulta más apropiado.

g) Instalación del certificado. El procedimiento de instalación de un certificado varía de acuerdo al ambiente del sistema.

A continuación se muestran ejemplos para generar certificados de servidor.

Primer ejemplo

Para generar un certificado digital, en este ejemplo, se debe tener instalado un servidor Web con soporte SSL, por ejemplo: Apache HTTP Server. Antes de generar claves, se debe instalar el paquete de herramientas OpenSSL, que se usa para la creación de certificados digitales e implementación de los protocolos de seguridad SSL y TLS.

La generación de la clave RSA [1]se realiza con el siguiente comando:

 # openssl genrsa -out /etc/httpd/conf/ssl.key/server.key 1024

Para cifrar la clave con una contraseña cuando se inicia el servidor, se debe ejecutar el comando:

 # openssl genrsa -des3 -out /etc/httpd/conf/ssl.key/server.key 1024

[1] Algoritmo de cifrado de Rivest, Shamir y Adleman (RSA)

Para que una autoridad CA firme un certificado, es necesario generar un "Certificate Signing Request".

 # openssl req -new -key /etc/httpd/conf/ssl.key/server.key -out /etc/httpd/conf/ssl.key/server.csr

Después de esta instrucción se pedirá que ingrese información necesaria para llenar el certificado (nombre del país, nombre de provincia, nombre de ciudad, nombre de la organización, nombre de la sección dentro de la organización, nombre del servidor, correo electrónico y dos datos más que son opcionales [challenge password y nombre opcional de la compañía]).

El archivo server.csr se puede enviar a la autoridad CA que firmará la clave.

Se puede autofirmar el certificado de servidor ejecutando la siguiente instrucción:

 # openssl x509 -req -days 365 -in /etc/httpd/conf/ssl.key/server.csr -signkey /etc/httpd/conf/ssl.key/server.key -out /etc/httpd/conf/ssl.crt/server.crt

Segundo ejemplo

En este ejemplo se utiliza la herramienta keytool de Java para generar un certificado digital auto-firmado. Esta herramienta ya viene incluida en las últimas distribuciones de Java. Para ejecutar este ejemplo, se deberá contar con el servidor Web Tomcat.

Inicialmente, se ingresa al directorio "bin", el cual se encuentra dentro del directorio de instalación del JDK de Java y se ejecuta la instrucción:

keytool -genkey -alias tomcat -keyalg RSA –keystore /.keystore

Una vez ejecutada esta instrucción, se requerirá del ingreso de ciertos datos, como ser: la contraseña para el almacén de claves, nombre y apellidos, nombre de la unidad de la organización, nombre de la organización, nombre de la ciudad, nombre de la provincia y el código del país.

Se deberá configurar Tomcat para que pueda trabajar con SSL. Para ello, se deberá modificar el archivo de configuración server.xml, el cual se encuentra en el directorio bin dentro del directorio de instalación de Tomcat. En este archivo se encuentra inhabilitado el conector para SSL:

```
<Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" />
```

Entonces, se deberá habilitar este conector y agregar la siguiente configuración dentro de éste.

keystoreFile="C:\.keystore" keystorePass="mypass"

Donde "C:\.keystore" es el lugar donde se creó el archivo ".keytore" y "mypass" es la contraseña que se especificó al momento de crear el almacén de claves.

Una vez concluido todo esto, se deberá iniciar el servidor Tomcat. Para verificar el éxito de la creación del certificado digital, se podrá ingresar a la dirección:

https://localhost:8443/

12. Aplicaciones de los certificados digitales

Los certificados digitales ofrecen un entorno seguro para comprar, vender, firmar documentos e intercambiar información a través de Internet. Entre las aplicaciones de los certificados digitales, se incluyen las siguientes:

- Correo electrónico
- Redes privadas virtuales
- Acceso a bases de datos confidenciales
- Relaciones entre empresas (proveedores/clientes)
- Transacciones económicas y comerciales
- Banca personal, empresarial y corporativa.
- Intercambio de información sensible o crítica.

Referencias

[1] Altava Soligó, Hugo. *Certificados digitales: Estudio y planificación, Proyecto final de carrera.* Universidad Politécnica de Valencia, septiembre de 2000.

[2] Farrell, S. and R. Housley. *An Internet Attribute Certificate Profile for Authorization.* Internet Draft draft-ietf-pkix-ac509prof-06, January 2001.

[3] Gerck, E. MCG. Overview of Certification Systems: X.509, CA, PGP and SKIP. *http://www.mcg.org.br/cert.htm* (verificado Abril 1997)

[4] How do I use Certificates on the WWW? *http://www.ilabs.interop.net/PKI/certwww.pdf*

[5] Leiva Riffo, Pablo. *http://usuarios.lycos.es/sistemacomputacion/capitulodos3.htm*

[6] Mavridis, Ioannis; Georgiadis, Christos; Pangalos, George; Khair, Marie. *Access Control based on Attribute Certificates for Medical Intranet Applications*. Aristotle University of Thessaloniki, Greece.

[7] Rescorla, E. HTTP Over TLS. Network Working Group,RTFM, Inc. Request for Comments: 2818, May 2000. *http://www.ietf.org/rfc/rfc2818.txt*

[8] Scolnik, Hugo. Universidad de Buenos Aires. *http://www.consecri.com.ar/conferencias.htm*

[9] Seamons, Kent E. Using Digital Credentials to Establish Trust between Strangers. *http://isrl.cs.byu.edu/pres/seamons.CERT1999.pdf*

[10] Smith, Jeremy Alan. *http://members.netscapeonline.co.uk/jeremyalansmith/ssltutorial/*

[11] SSLv3 Protocol Specification. *http://www.netscape.com/eng/ssl3/*

[12] Stefan A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates*. MIT Press, Cambridge, Massachusetts, August 2000.

[13] Talens-Oliag, Sergio. Introducción a los certificados digitales. *http://www.uv.es/~sto/articulos/BEI-2003-11/certificados_digitales.html*

[14] Wagner D. and B. Schneier. Analysis of the SSL 3.0 Protocol. *http://www.counterpane.com/ssl.html*

[15] Warbrick, Jon. University Computing Service. *http://www-uxsup.csx.cam.ac.uk/~jw35/docs/doing_ssl.html*