Introducción a los certificados digitales

Sergio Talens-Oliag

InfoCentre (http://www.infocentre.gva.es/)

stalens@infocentre.gva.es

Introducción

Los certificados digitales son el equivalente digital del DNI, en lo que a la autentificación de individuos se refiere, ya que permiten que un individuo demuestre que es quien dice ser, es decir, que está en posesión de la clave secreta asociada a su certificado.

Para los usuarios proporcionan un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red, el envío de correo encriptado y/o firmado digitalmente, el control de acceso a recursos, etc.

En este artículo explicaremos qué son los certificados digitales, cuales son los formatos estándar, como podemos controlar sus periodos de validez o anularlos si se ven comprometidos, quien los genera y las infraestructuras necesarias para soportarlos.

Certificados Digitales

Un *certificado de clave pública* es un punto de unión entre la clave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la clave pública pertenece a la entidad identificada y que la entidad posee la correspondiente clave privada.

Los *certificados de clave pública* se denominan comúnmente *Certificado Digital*, *ID Digital* o simplemente *certificado*. La entidad identificada se denomina *sujeto del certificado* o *subscriptor* (si es una entidad legal como, por ejemplo, una persona).

Los certificados digitales sólo son útiles si existe alguna *Autoridad Certificadora* (*Certification Authority* o *CA*) que los valide, ya que si uno se certifica a sí mismo no hay ninguna garantía de que su identidad sea la que anuncia, y por lo tanto, no debe ser aceptada por un tercero que no lo conozca.

Es importante ser capaz de verificar que una autoridad certificadora ha emitido un certificado y detectar si un certificado no es válido. Para evitar la falsificación de certificados, la entidad certificadora después de autentificar la identidad de un sujeto, firma el certificado digitalmente.

Los *certificados digitales* proporcionan un mecanismo criptográfico para implementar la autentificación; también proporcionan un mecanismo seguro y escalable para distribuir claves públicas en comunidades grandes.

Certificados X.509

El formato de certificados X.509 es un estándar del ITU-T (*International Telecommunication Union-Telecommunication Standarization Sector*) y el ISO/IEC (*International Standards Organization / International Electrotechnical Commission*) que se publicó por primera vez en 1988. El formato de la versión 1 fue extendido en 1993 para incluir dos nuevos campos que permiten soportar el control de acceso a directorios.

Después de emplear el X.509 v2 para intentar desarrollar un estándar de correo electrónico seguro, el formato fue revisado para permitir la extensión con campos adicionales, dando lugar al X.509 v3, publicado en 1996.

Los elementos del formato de un certificado X.509 v3 son:

- **Versión**. El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
- **Número de serie del certificado**. Este campo 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**. Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
- **Nombre del emisor**. Este campo identifica la CA que ha firmado y emitido el certificado.
- **Periodo de validez**. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
- **Nombre del sujeto**. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
- **Información de clave pública del sujeto**. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
- **Identificador único del emisor**. Este es un campo opcional que permite reutilizar nombres de emisor.
- **Identificador único del sujeto**. Este es un campo opcional que permite reutilizar nombres de sujeto.
- **Extensiones**.

Las extensiones del X.509 v3 proporcionan una manera de asociar información adicional a sujetos, claves públicas, etc. Un campo de extensión tiene tres partes:

1. **Tipo de extensión**. Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión.
2. **Valor de la extensión**. Este subcampo contiene el valor actual del campo.
3. **Indicador de importancia**. Es un *flag* que indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo. El indicador proporciona una manera de implementar aplicaciones que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones.

El ITU y el ISO/IEC han desarrollado y publicado un conjunto de extensiones estándar en un apéndice al X.509 v3:

- **Limitaciones básicas**. Este campo indica si el sujeto del certificado es una CA y el máximo nivel de profundidad de un camino de certificación a través de esa CA.
- **Política de certificación**. Este campo contiene las condiciones bajo las que la CA emitió el certificado y el propósito del certificado.
- **Uso de la clave**. Este campo restringe el propósito de la clave pública certificada, indicando, por ejemplo, que la clave sólo se debe usar para firmar, para la encriptación de claves, para la encriptación de datos, etc. Este

campo suele marcarse como importante, ya que la clave sólo está certificada para un propósito y usarla para otro no estaría validado en el certificado.

El formato de certificados X.509 se especifica en un sistema de notación denominado *sintaxis abstracta uno* (*Abstract Sintax One* o ASN-1). Para la transmisión de los datos se aplica el DER (*Distinguished Encoding Rules* o *reglas de codificación distinguible*), que transforma el certificado en formato ASN-1 en una secuencia de octetos apropiada para la transmisión en redes reales.

Listas de Anulación de Certificados (CRLs)

Los certificados tienen un periodo de validez que va de unos meses a unos pocos años. Durante el tiempo que el certificado es válido la entidad certificadora que lo generó mantiene información sobre el estado de ese certificado.

La información más importante que guarda es el *estado de anulación*, que indica que el periodo de validez del certificado ha terminado antes de tiempo y el sistema que lo emplee no debe confiar en él. Las razones de anulación de un certificado son varias: la clave privada del sujeto se ha visto comprometida, la clave privada de la CA se ha visto comprometida o se ha producido un cambio en la afiliación del sujeto (por ejemplo cuando un empleado abandona una empresa).

Las *listas de anulación de certificados* (*Certification Revocation Lists* o CRL) son un mecanismo mediante el cual la CA publica y distribuye información a cerca de los certificados anulados a las aplicaciones que los emplean. Una CRL es una estructura de datos firmada por la CA que contiene su fecha y hora de publicación, el nombre de la entidad certificadora y los números de serie de los certificados anulados que aun 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 él.

Existen varios métodos para la actualización de CRLs:

1. **Muestreo de CRLs**. Las aplicaciones acceden a la CA o a almacenes de archivos y copian el último CRL a intervalos regulares. La pega de este esquema es que durante el periodo entre actualizaciones del CRL podemos aceptar un certificado ya anulado, por lo que el periodo debe ser corto.
2. **Anuncio de CRLs**. La entidad certificadora anuncia que ha habido un cambio en el CRL a las aplicaciones. El problema de este enfoque es el anuncio puede ser muy costoso y no sabemos que aplicaciones deben ser informadas.
3. **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.

Listas de Anulación de Certificados X.509

El formato de listas de anulación de certificados X.509 es un estándar del ITU-T y la ISO/IEC que se publicó por primera vez en 1988 como versión 1. El formato fue modificado para incluir campos de extensión, dando origen al al formato X.509 v2 CRL.

Los campos básicos de un formato X.509 CRL (válidos para las versiones 1 y 2) son:

- **Versión**. Debe especificar la versión 2 si hay algún campo de extensión.

- **Firma**. El campo contiene identificador del algoritmo empleado para firmar la CRL.
- **Nombre del generador**. Este campo contiene el nombre de la entidad que ha generado y firmado la CRL.
- **Esta actualización**. Fecha y hora de la generación de la CRL.
- **Próxima actualización**. Indica la fecha y hora de la próxima actualización. El siguiente CRL puede ser generado antes de la fecha indicada pero no después de ella.
- **Certificado del usuario**. Contiene el número de serie de un certificado anulado.
- **Fecha de anulación**. Indica la fecha efectiva de la anulación.

Existe también un conjunto de campos de entrada de extensión en las CRLs X.509 v2, como el **código de razón**, que identifica la causa de la anulación: sin especificar, compromiso de clave, compromiso de la CA, cambio de afiliación, superado (el certificado ha sido reemplazado), cese de operación (el certificado ya no sirve para su propósito original), certificado en espera (el certificado está suspendido temporalmente) y elimina de la CRL (un certificado que aparecía en una CRL previa debe ser eliminado).

Adicionalmente también se ha añadido un conjunto de extensiones para las X.509v2 CRL con los mismos subcampos que en los certificados X.509v3. Estas extensiones permiten que una comunidad o entidad se defina sus propios campos de extensión privados.

Autoridades Certificadoras

Una *autoridad certificadora* es una organización fiable que acepta solicitudes de certificados de entidades, las valida, genera certificados y mantiene la información de su estado.

Una CA debe proporcionar una *Declaración de Prácticas de Certificación* (*Certification Practice Statement* o *CPS*) que indique claramente sus políticas y prácticas relativas a la seguridad y mantenimiento de los certificados, la responsabilidades de la CA respecto a los sistemas que emplean sus certificados y las obligaciones de los subscriptores respecto de la misma.

Las labores de un CA son:

- **Admisión de solicitudes**. Un usuario rellena un formulario y lo envía a la CA solicitando un certificado. La generación de las claves pública y privada son responsabilidad del usuario o de un sistema asociado a la CA.
- **Autentificación del sujeto**. Antes de firmar la información proporcionada por el sujeto la CA debe verificar su identidad. Dependiendo del nivel de seguridad deseado y el tipo de certificado se deberán tomar las medidas oportunas para la validación.
- **Generación de certificados**. Después de recibir una solicitud y validar los datos la CA genera el certificado correspondiente y lo firma con su clave privada. Posteriormente lo manda al subscriptor y, opcionalmente, lo envía a un almacén de certificados para su distribución.
- **Distribución de certificados**. La entidad certificadora puede proporcionar un servicio de distribución de certificados para que las aplicaciones tengan acceso y puedan obtener los certificados de sus subscriptores. Los métodos de distribución pueden ser: correo electrónico, servicios de directorio como el X.500 o el LDAP, etc.
- **Anulación de certificados**. Al igual que sucede con las solicitudes de certificados, la CA debe validar el origen y autenticidad de una solicitud de anulación. La CA debe mantener información sobre una anulación durante todo el tiempo de validez del certificado original.
- **Almacenes de datos**. Hoy en día existe una noción formal de *almacén* donde se guardan los certificados y la información de las anulaciones. La designación oficial de una base de datos como almacén tiene por objeto señalar que el trabajo con los certificados es fiable y de confianza.

Infraestructuras de Clave Pública

La difusión de las técnicas de clave pública requiere una *infraestructura* que defina un conjunto de estándares, autoridades de certificación, estructuras entre múltiples CAs, métodos para descubrir y validar rutas de certificación, protocolos operacionales, protocolos de gestión, herramientas que pueden operar entre sí y un marco legislativo.

Los protocolos operacionales se dirigen al problema del envío de certificados y CRLs a los sistemas que emplean certificados. Los protocolos de gestión tratan de los requisitos para la interacción de dos componentes de la infraestructura: registro, inicialización, certificación, anulación y recuperación de claves.

Una estructura entre múltiples CAs proporciona una o más rutas de certificación entre un subscriptor y una aplicación. Una *ruta de certificación* (o cadena de certificación) es una secuencia de uno o más puntos conectados entre el subscriptor y una CA raíz. Una *CA raíz* es una autoridad en la que confía la aplicación, ya que tiene almacenada de forma segura su clave pública.

Un sistema que emplea certificados necesita obtener una ruta de certificación entre un subscriptor y un CA raíz antes de evaluar el nivel de confianza en el certificado del subscriptor. El problema de determinar una ruta de certificación entre dos subscriptores arbitrarios en una estructura de interconexiones entre diferentes CAs se denomina *descubrimiento de rutas de certificación*. El problema de verificar la asociación entre el nombre del subscriptor y su clave pública en una ruta de certificación se denomina *validación de la ruta de certificación*.