Dos de las aplicaciones más utilizadas, y que más están impulsando la utilización de Internet e Intranets, son el correo electrónico y las conexiones WWW

Autoridades de Certificación y II

Aplicación al correo electrónico

Para proporcionar seguridad a estas aplicaciones se han definido multitud de estándares, que han ido evolucionando hasta contemplar la utilización de las Autoridades de Certificación (AC). Tal es el caso del estándar S/MIME para correo electrónico y SSL para las aplicaciones TCP/IP, entre las que se encuentra el protocolo HTTP que permite establecer las conexiones WWW.

A continuación se describen de forma general los protocolos para comunicarse con una Autoridad de Certificación, y un modo sencillo y rápido de disponer de correo electrónico y conexiones WWW seguras, utilizando los servicios de una Autoridad de Certificación.

Protocolos

Teniendo en cuenta el proceso de certificación, es necesario disponer de determinados métodos o protocolos que permitan al usuario comunicarse adecuadamente con la AC.

En primer lugar es necesario que el usuario solicite un certificado. En este sentido, la AC es responsable de definir el modo en que el usuario realiza la petición, mientras que la generación de las claves depende exclusivamente del propio usuario, debido a la distinta naturaleza que puede presentar el mismo. Esto es, el usuario puede ser un servidor WWW o alguien que quiere utilizar el correo electrónico.

En cualquier caso, la AC definirá los diferentes formatos de petición que acepta y el modo de enviarlos (el formato más extendido, aunque no el único, es el que define el estándar PKCS#10). Por ejemplo, en el caso de un servidor WWW, lo habitual es enviar la petición mediante correo electrónico a la dirección indicada por la AC. En el caso de un cliente WWW, el propio navegador generará las claves y la petición, utilizando la conexión HTTP para enviar los datos y recibir posteriormente el certificado.

Una vez recibida la petición de certificado, la AC debe comprobar la identidad del usuario propietario de esa clave pública. Si se desea disponer de un buen nivel de seguridad será necesario que el usuario se identifique de algún modo ante el administrador de la AC. Las ACs que emiten certificados de forma automática no ofrecen seguridad sobre la identidad de la clave.

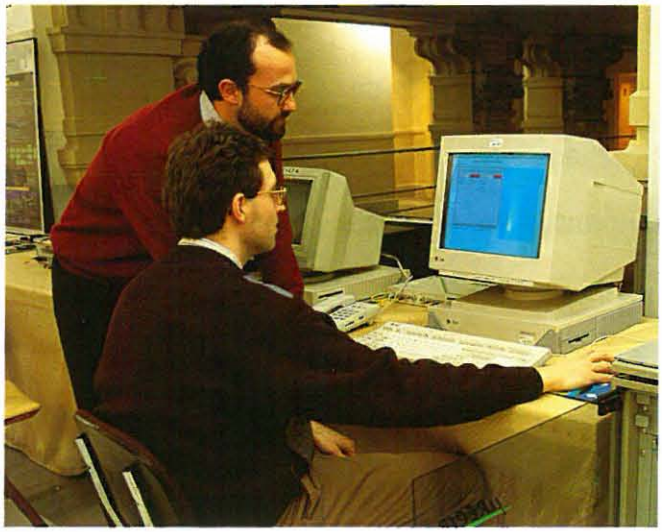
Otro aspecto importante es la obtención por parte de los usuarios de la clave pública de la AC, indispensable para poder comprobar los certificados de las claves públicas de los demás usuarios. Para ello es necesario obtener un certificado autofirmado por la AC conteniendo su clave pública.

Con todo esto, una vez el usuario dispone de su certificado, el sistema puede funcionar con la garantía de que las claves públicas que se utilizan son las verdaderas. Surge entonces un nuevo problema, controlar la validez de los certificados. Es decir, ¿que ocurre si alguien consigue robar la clave privada de un usuario? En este caso, la clave pública no se debería utilizar, puesto que no solo el usuario propietario de la clave puede descifrar el mensaje sino también el que la robó. En cambio, el sistema sólo comprueba que la clave pública está certificada por una AC y es válida. Para evitar estas y otras situaciones se definen las listas de certificados revocados, que incluyen todos los certificados que dejan de ser válidos aunque no haya transcurrido su período de validez (especificado por la AC a la hora de emitirlo). Se hace necesario, por tanto, no sólo comprobar el período de validez, sino consultar las listas de certificados revocados para garantizar una correcta utilización de las claves.

Utilización de las ACs para implementar correo electrónico y conexiones WWW seguros

Actualmente, ya están disponibles los correspondientes paquetes software que implementan los

• Alberto Peinado Domínguez
Ingeniero de Telecomunicación



estándares S/MIME y SSL. El modo más cómodo para disponer de correo y web seguro es utilizar Netscape Communicator 4.04 o Microsoft Internet Explorer 4.0. Estos dos paquetes permiten trabajar de forma complementaria con un navegador (Navigator o Internet Explorer), que implementa SSL, y un cliente de correo (Netscape Messenger oMicrosoft Outlook Express) que implementa S/MIME.

Para trabajar con correo y web seguros utilizando alguno de estos softwares se necesita además utilizar los servicios de cualquier AC. Afortunadamente, podemos elegir entre un gran número de ellas. Elegida la AC, y conectados a la dirección http correspondiente, los pasos a seguir son los siguientes.

1. Obtener la clave pública de la AC. Esta operación sólo hay que realizarla una vez, con anterioridad a la primera comunicación segura que vayamos a efectuar. La clave pública de la AC es necesaria para comprobar la validez de los certificados emitidos por ella. Dependiendo de la AC elegida, esta instalación se puede realizar al principio o al final de todo el proceso. En cualquier caso, es completamente automática. Solo hay que seleccionar un enlace en la página web y el navegador lo almacena internamente. Para comprobar si el navegador lo ha instalado:

Netscape Navigator. Seleccionar Menu Seguridad –Certificados – Firmantes

Microsoft Internet Explorer. Seleccionar Menu Ver –Opciones de Internet –Contenidos –Sitios

En ambos casos aparece una lista con las ACs de las cuales tenemos la clave pública.

2. Solicitar el certificado personal. El usuario debe conectarse a la página de la AC diseñada al efecto. En ella encontrará un formulario que debe rellenar con sus datos personales. A continuación, cuando pulse el botón "enviar formulario" el navegador (Navigator o Internet Explorer), se encargará de generar las claves automáticamente y enviar la petición de certificado. Cuando la AC recibe dicha petición envía un acuse de recibo, incluyendo algunas instrucciones sobre el proceso a seguir.

3. Instalar el certificado personal. Tras comprobar la identidad del propietario de la clave, la AC emite el certificado notificándolo al usuario (normalmente, por correo electrónico). En esta notificación se suele incluir la dirección web donde conectarse para obtener el certificado solicitado, de modo que el navegador lo instale automáticamente. Como se puede ver, el proceso es prácticamente transparente al usuario, que únicamente ha de rellenar un pequeño formulario con sus datos personales, y todo ello utilizando las facilidades que ofrece el entorno WWW.

Surge un nuevo problema, controlar la validez de los certificados

Con el certificado instalado en el navegador, ya podemos usar el cliente de correo asociado (Netscape Messenger o Microsoft Outlook Express) para enviar y recibir correo cifrado y/o firmado, y conectarnos a un servidor web seguro, puesto que los certificados obtenidos son compartidos por el navegador y el cliente de correo.

Si solamente disponemos del certificado de nuestra clave pública, lo único que podemos hacer, en principio, es firmar con nuestra clave privada los mensajes que vamos a enviar. Cuando se envía un mensaje firmado usando S/MIME, también se envía el certificado de nuestra clave pública, para que el receptor pueda comprobar la firma. Para poder cifrar mensajes es necesario disponer de la clave pública del usuario destinatario. A medida que vayamos recibiendo mensajes firmados de otros usuarios, iremos obteniendo sus claves públicas. En cualquier caso, siempre se puede establecer una comunicación no segura con un futuro destinatario y solicitar su clave pública certificada, o utilizar la base de datos que pueda ofrecer la AC con los certificados de sus usuarios.

En cuanto a las conexiones WWW seguras, una vez disponemos de la clave pública de la AC, ya podemos conectarnos con los servidores WWW certificados por dicha AC. El servidor debe realizar un proceso similar al descrito anteriormente (punto 2 y 3) para obtener el certificado de sitio, antes de que cualquier usuario pueda conectarse a él. Una vez certificado el servidor, un usuario puede autenticarlo y enviar y recibir información de forma confidencial, asegurando además la integridad de los datos.

Alberto Peinado Domínguez

•**Ingeniero de Telecomunicación**

--Profesor del Departamento de Ingeniería de Comunicaciones ETS Ingenieros de Telecomunicación de la Universidad de Málaga y vocal de la Asociación Española de Criptología y Seguridad Informática