

## **RESUMEN 500 PALABRAS TRABAJO 12: ESTÁNDARES EN CERTIFICADOS ELECTRÓNICOS PARA INTERNET.**

Oriol Gras - UPC  
Diego Pacheco - UPV  
José Vicente Castelló – UPV

Cuando hablamos de certificados electrónicos estamos hablando de seguridad en Internet. A su vez, si hablamos de seguridad en Internet tenemos que hacerlo de los pilares o servicios básicos que se deben garantizar. Estos servicios básicos son: la confidencialidad, la integridad, el no repudio y la autenticación. La confidencialidad se resuelve con el cifrado, mientras que la integridad y el repudio quedan solventados con la firma digital. Sin embargo, cuando analizamos la autenticación vemos que no queda resuelta ni por la firma digital, ni por el cifrado. La autenticación necesita de algo más, los certificados. Pero, ¿qué es un certificado? Un certificado digital es un documento digital mediante el cual un tercero confiable (Autoridad de Certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública. Así, aparece una tercera parte en la que nosotros confiamos y que juega el papel de notario virtual. Esta tercera parte nos asegura que la clave pública contenida en ese documento digital pertenece a la persona o entidad que figura también en ese certificado.

La infraestructura de clave pública permite que los usuarios puedan acceder a los certificados, mediante unos protocolos específicos. Es decir, se trata del conjunto de componentes que aseguran que un certificado realmente identifica a un usuario y su clave pública. De forma general, las PKI (infraestructuras de clave pública) se pueden dividir en dos tipos: centralizadas y distribuidas. Las PKI centralizadas están compuestas de forma elemental por los siguientes elementos:

- Certificados.
- Autoridades de certificación (CA).
- Repositorio de certificados.
- CRL (Lista de revocación de certificados).

Los certificados que relacionan la clave pública del usuario, con información que lo identifica. Además esta información viene firmada por una tercera parte de confianza. Los certificados tienen un período de validez que viene especificado, y es visible para los usuarios. Las autoridades de certificación son entidades en la que los usuarios confían. La clave con la que firman está fuertemente protegida, y además tiene los medios para verificar la identidad de los participantes de la comunicación. El repositorio es el lugar donde se almacenan los certificados, y el acceso a estos se da por medio del protocolo LDAP. Las CRL ó listas de revocación de certificados son registros en los que las autoridades certificadoras (CAs) indican cuales certificados han dejado de ser válidos, con la razón de dicha invalidez. Causas posibles de esto puede ser violación en la seguridad del certificado, que el titular del certificado desaparezca (en el caso de una empresa) ,o fallezca (si se trata de una persona natural), etc. Para acceder a dicha información se usa el mismo algoritmo LDAP, y la ubicación de estas listas se da de forma distribuida.

La arquitectura de las CA es jerarquizada, es decir, todos los CA están conectados por un nodo central que se considera una autoridad por todos los miembros de Internet. Esta autoridad está representada por el IPRA (Internet Policy Registration Authority), y los nodos que se conectan hacia abajo tienen menor prioridad. La validez de este nodo para los usuarios tiene una forma física con los certificados raíz, que vienen instalados en nuestros navegadores.

De la misma manera que en el modo distribuido, existen diferentes soluciones dentro de lo que se llama PKI distribuida. Diferentes, esto quiere decir que el hecho de conocer una no significa que se conozcan todas. En uno de estos esquemas, los usuarios pueden firmar los certificados de los usuarios en quienes confían, y si yo como usuario veo que al menos un número significativo de personas en quienes confío parcialmente firman los certificados de alguien que no conozco, entonces yo puedo confiar en esa persona, así yo no la conozca. Por otro lado, si alguien en quien confío plenamente firma los certificados de alguien que no conozco, entonces por extensión yo confío en esa persona. Un ejemplo de PKI distribuida es CAcert. Este esquema en particular aún no ha sido aceptado para agregar sus certificados en los registros de los navegadores actuales.

La estandarización en temas de certificación electrónica es una tarea tan ardua y laboriosa como importante para la consecución de una Internet más segura y más compatible para todos los usuarios. En este caso un buen certificado electrónico debe ser similar al servicio proporcionado por un notario frente a seguridad y fiabilidad en los trámites y documentos. Existen unos procedimientos claros y concisos para operaciones realizadas en cualquier notaria y de igual manera ocurre cuando se utiliza un certificado electrónico y para poder conseguir esto los estándares son una herramienta fundamental. En un estándar de certificación electrónica están estipulados todos los campos y condiciones que debe cumplir. El estándar X.509 de la ITU-T es el más utilizado a nivel internacional pero existen otros igualmente válidos y para ello deben ser aprobados por alguna de las distintas organizaciones de estandarización. Así esto sería similar a cuando se utilizan en derecho internacional documentos notariales de otros países porque aunque el estándar no sea el mismo son válidos porque cumplen un determinado criterio y validez establecido por adelantado y avalado por algún ente público u organismo autorizado.

Al pensar en certificados electrónicos podemos pensar que éstos solo se emplean en contadas ocasiones o en situaciones donde se requiera mucha seguridad. No obstante, esto no es así. Los certificados se utilizan en gran cantidad de ocasiones y escenarios. Los ámbitos más comunes y que conforman nuestro día a día son: en el comercio electrónico, para hacer trámites con la administración, en la banca electrónica y en ciertas ocasiones en los e-mails. Destacar que en España tenemos a CERES (Certificación española) como la entidad que facilita y se encarga de hacer posible ciertos trámites entre la administración y las personas a través de Internet. Algunos de los proyectos más conocidos de CERES son: la declaración de la renta a través de la red, el DNIe, trámites varios con los ayuntamientos...

Sin embargo, para que estas aplicaciones sean posibles, detrás de ellas se esconden algunos protocolos que interactúan con los certificados. Los más conocidos son: SSL/TLS, S-HTTP, SET y S-MIME. Hay que destacar entre los protocolos mencionados el SSL. Este protocolo es hoy en día el más utilizado. Combina la criptografía de clave asimétrica con la criptografía de clave simétrica. De esta manera, aprovecha la velocidad de cifrado de clave simétrica y se sirve de la criptografía de clave asimétrica para la transmisión de la clave secreta.