Certificados digitales y seguridad

El Certificado Digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de Internet. Además:

El certificado digital permite la firma electrónica de documentos El receptor de un documento firmado puede tener la seguridad de que éste es el original y no ha sido manipulado y el autor de la firma electrónica no podrá negar la autoría de esta firma.

El certificado digital permitecifrar las comunicaciones. Solamente el destinatario de la información podrá acceder al contenido de la misma.

En definitiva, la principal ventaja es que disponer de un certificado le ahorrará tiempo y dinero al realizar trámites administrativos en Internet, a cualquier hora y desde cualquier lugar.

Un Certificado Digital consta de una pareja de claves criptográficas, una pública y una privada, creadas con un algoritmo matemático, de forma que aquello que se cifra con una de las claves sólo se puede descifrar con su clave pareja.

El titular del certificado debe mantener bajo su poder la clave privada, ya que si ésta es sustraída, el sustractor podría suplantar la identidad del titular en la red. En este caso el titular debe revocar el certificado lo antes posible, igual que se anula una tarjeta de crédito sustraída.

La clave pública forma parte de lo que se denomina Certificado Digital en sí, que es un documento digital que contiene la clave pública junto con los datos del titular, todo ello firmado electrónicamente por una Autoridad de Certificación, que es una tercera entidad de confianza que asegura que la clave pública se corresponde con los datos del titular.

La Firma Electrónica sólo puede realizarse con la clave privada. Puedes encontrar más información sobre el proceso de firma digital en la sección “¿Qué es una firma digital?”

La Autoridad de Certificación se encarga de emitir los certificados para los titulares tras comprobar su identidad.

El formato de los Certificados Digitales está definido por el estándar internacional ITU-T X.509. De esta forma, los certificados pueden ser leídos o escritos por cualquier aplicación que cumpla con el mencionado estándar.

En la UPV se admiten los Certificados Digitales del DNI electrónico, emitidos por el Cuerpo Nacional de la Policía, y los emitidos por la Autoridad de Certificación de la Generalitat Valenciana (ACCV).

Otra utilidad de los Certificados Digitales es que posibilitan el envío de mensajes cifrados: utilizando la clave pública de un Certificado, es posible cifrar un mensaje

y enviarlo al titular del Certificado, quien será la única persona que podrá descifrar el mensaje con su clave privada.

Algunas de las aplicaciones que podrá darle el usuario a sus certificados son:

- Inicio de sesión en la Intranet: Permite a los miembros de la Comunidad Universitaria iniciar sesión en la Intranet utilizando como identificación el DNI o el carné universitario, sin necesidad introducir la contraseña de red.

- Firma de Mensajes de Correo: Para asegurar la identidad del firmante y la integridad del mensaje. Los destinatarios pueden estar seguros de quién envió el correo, y de que no se ha modificado su contenido.

- Envío de mensajes de correo cifrados: Aquellos usuarios que dispongan de su clave pública, podrán enviarle mensajes de correo cifrados, de forma que sólo usted pueda leerlos.

Referencias:

http://www.upv.es/contenidos/CD/info/711251normalc.html