¿Qué es la firma digital?

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos posean la misma característica que la firma hológrafa (de puño y letra) exclusiva de los documentos en papel.
Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.
La firma digital no implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.

Principales ventajas de la firma digital

- Brinda seguridad en el intercambio de información crítica.
- Reemplaza a la documentación en papel por su equivalente en formato digital.
- Reduce costos generales y mejora la calidad de servicio.
- Mayor velocidad de procesamiento.
- Las empresas podrán extender sus plataformas de comercio electrónico con mayor seguridad, garantizando el mismo marco jurídico que proporciona la firma hológrafa.
- Es un pilar fundamental donde apoyar el desarrollo del gobierno electrónico (e-government).

Características de la firma digital

Cada titular de una firma digital posee un par de claves asociadas, una privada y otra pública, generada mediante un proceso matemático.

	CLAVE PRIVADA es utilizada por su titular para firmar digitalmente un documento o mensaje, es secreta y mantenida por ese titular bajo su exclusiva responsabilidad
	La CLAVE PUBLICA es utilizada por el receptor de un documento o mensaje firmado para verificar la integridad y la autenticidad, asegurando el “no repudio”.

Ambas claves se encuentran asociadas entre sí por las características especiales del proceso matemático.

¿Cómo funciona?

La firma digital funciona utilizando complejos procedimientos matemáticos que relacionan el documento firmado con información propia del firmante, y permiten que terceras partes puedan reconocer la identidad del firmante y asegurarse de que los contenidos no han sido modificados.
El firmante genera, mediante una función matemática, una huella digital del mensaje, la cual se cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital, que se enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento una marca que es única para dicho documento y que sólo él es capaz de producir.
Para realizar la verificación del mensaje, en primer término el receptor generará la huella digital del mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que no hubo alteración y que el firmante es quien dice serlo.
El sistema opera de tal modo que la información cifrada con una de las claves sólo puede ser descifrada con la otra. De este modo si un usuario cifra determinada información con su clave privada, cualquier persona que conozca su clave pública podrá descifrar la misma.
En consecuencia, si es posible descifrar un mensaje utilizando la clave pública de una persona, entonces puede afirmarse que el mensaje lo generó esa persona utilizando su clave privada (probando su autoría).

¿Qué son los certificados digitales?

Los certificados digitales son pequeños documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado. Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona.

En algunos casos, puede ser necesario crear una cadena de certificados, cada uno certificando el previo, para que las partes involucradas confíen en la identidad en cuestión.

¿Qué contiene un certificado digital?

En su forma más simple, el certificado contiene una clave pública y un nombre. Habitualmente, también contiene una fecha de expiración, el nombre de la Autoridad Certificante que la emitió, un número de serie y alguna otra información. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del mismo.
Su formato está definido por el estándar internacional ITU-T X.509. De esta forma, puede ser leído o escrito por cualquier aplicación que cumpla con el mencionado estándar.

¿Qué tipos de certificados digitales existen?

	Certificados Clase 3. Tiene la ventaja de no necesitar ningún hardware especial, sin costos, posibilitando su uso masivo. Solo requiere instalar el certificado en la PC que utilizará para firmar digitalmente documentos. El sistema solicitará el ingreso de la clave privada para firmar documentos.
	Certificados Clase 4. Brinda una mayor seguridad ya que los datos privados del titular son almacenados en un dispositivo criptográfico especial. Para firmar digitalmente el sistema solicitará que conecte el dispositivo criptográfico e ingrese la clave privada.

¿Qué valor legal tiene la firma digital?

Según la legislación argentina, si un *documento firmado digitalmente* es verificado correctamente, se presume *salvo prueba en contrario* que proviene del suscriptor del certificado asociado y que no fue modificado.
Por otra parte, para reconocer que un documento ha sido firmado digitalmente se requiere que el certificado digital del firmante haya sido emitido por un ***Certificador Licenciado*** (o sea que cuente con la aprobación del *Ente Licenciante*).
El certificado digital permite identificar quién es el propietario de la clave privada.
El marco normativo de la República Argentina en materia de Firma Digital está constituido por la Ley Nº 25.506, el Decreto Nº 2628/02 y su modif.. y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

¿Qué es una Infraestructura de Firma Digital?

En nuestro país se denomina "Infraestructura de Firma Digital" al conjunto de leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes (por ej. Internet).
Realmente esta definición es conocida mundialmente con las siglas PKI que significan Public Key Infraestructure o Infraestructura de Clave Pública.

Esta Infraestructura de Firma Digital de alcance federal está integrada por:

Autoridad de Aplicación:	Según el Decreto N° 409/2005, la Subsecretaría de la Gestión Pública actuará como autoridad de aplicación del régimen normativo que establece la infraestructura de firma digital establecida en la Ley Nº 25.506 y en las funciones de entidad licenciante de certificadores, supervisando su accionar.
Comisión Asesora para la Infraestructura de Firma Digital:	Funciona en el ámbito de la Subsecretaría de la Gestión Pública, emitiendo recomendaciones sobre los aspectos técnicos referidos al funcionamiento de la Infraestructura de Firma Digital. A través del Decreto N° 160/2004, el Poder Ejecutivo Nacional ha designado a los integrantes de la Comisión Asesora para la Infraestructura Nacional de Firma Digital, en cumplimiento de lo dispuesto en la Ley Nº 25.506.
Ente Licenciante:	Es el órgano técnico-administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad..
Certificadores licenciados:	Son aquellas personas de existencia ideal, registro público de contratos u organismo público que obtengan una licencia emitida por el ente licenciante para actuar como proveedores de servicios de certificación en los términos de la Ley Nº 25.506 y su normativa complementaria.
Autoridades de Registro:	Son entidades que tienen a su cargo las funciones de validación de la identidad y otros datos de los suscriptores de certificados. Dichas funciones son delegadas por el certificador licenciado.
Sistema de Auditoría:	Será establecido por la autoridad de aplicación, a fin de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados.