Firmas digitales

¿Qué es la firma digital?

Según especifica Wikipedia, una firma digital es un esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. Una firma digital da al destinatario seguridad en que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión.
Consiste en un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.
La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital. El software de firma digital debe además efectuar varias validaciones, entre las cuales podemos mencionar:

* Vigencia del certificado digital del firmante,

* Revocación del certificado digital del firmante,

* Inclusión de sello de tiempo.

La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente. Funciona en una sola dirección, es decir, no es posible, a partir del valor resumen, calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica indiscutible al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. Este tipo de operaciones no están pensadas para que las lleve a cabo el usuario, sino que se utiliza software que automatiza tanto la función de calcular el valor hash como su verificación posterior.

Firma digital avanzada:

Una firma digital básica pierde la certeza de su validez cuando expira el certificado. Una firma digital avanzada sigue siendo valida sin lugar a dudas durante plazos largos que van más allá de la expiración del certificado.

Existen documentos tales como contratos o testamentos para los cuales no es apropiado usar firma digitales básicas ya que estos documentos se mantendrán vigentes por mucho tiempo después de que expiren los certificados digitales de los signatarios. En estos casos lo apropiado es usar firma digital avanzada.

Una firma digital no es valida si fue realizada usando un certificado vencido o revocado. Por otro lado una firma digital básica no contiene información certera acerca de la fecha y hora en que se realizó. Dado lo anterior no es posible saber si las firmas digitales hechas con un certificado fueron hechas antes o después que expirara. Por lo tanto al vencer un certificado se pierde la certeza de la validez de las firmas hechas con este.

La firma digital avanzada contiene información que permite determinar con certeza su validez incluso después que el certificado digital ha vencido. Para lograr esto la firma digital incluye una estampa de tiempo e información de validación que permiten determinar la existencia y validez de la firma digital en un momento del tiempo anterior al vencimiento o revocación del certificado.

La estampa de tiempo que incluye la firma digital avanzada permite determinar que la firma digital existía antes de la fecha y hora dada por la estampa. Lo que permite determinar que el certificado estaba vigente y no había sido revocado antes del momento indicado por la estampa. Esta estampa es generada por una autoridad de estampado de tiempo confiable, es decir podemos estar seguros que esa autoridad siempre suministrará la fecha y hora correctas. En Costa Rica las autoridades de estampado de tiempo son autorizadas por la Dirección de Certificados Digitales del MICITT. Actualmente la única autoridad de estampado de tiempo autorizada es la del SINPE.

Además la firma digital avanzada contiene información de validación que permite establecer la validez del certificado usado, incluso si no se tiene acceso a las fuentes originales de información de validación. Esta información consiste de las listas de revocación de certificados, las respuestas de servicio OCSP y las cadenas de certificados necesarias para validar el certificado usado para firmar y la cadena de certificados desde este hasta la raíz de la jerarquía.

Firma digital vs Firma electrónica

Antes de profundizar en la firma digital y comprender cada uno de los elementos que la hacen posible, debemos distinguir dos términos que solemos utilizar indistintamente: firma electrónica y firma digital. Aunque pueda parecer que representan el mismo concepto, no es así.

- Firma digital: es un conjunto de métodos criptográficos y técnicos. Es un concepto fundamentalmente técnico.
- Firma electrónica: es un término mucho más amplio y hace referencia a cuestiones legales, organizativas, técnicas, etc.

Ahora conociendo ambos términos, se puede concluir que:

- La firma digital es uno de los elementos que componen la firma electrónica. Firma digital es un concepto que está «dentro» del concepto de firma electrónica.

Referencias:

http://www.firma-digital.cr