Alumnos: Aguilar Chávez Luis Daniel

Ortega Rivera Javier

Grupo: 6s2

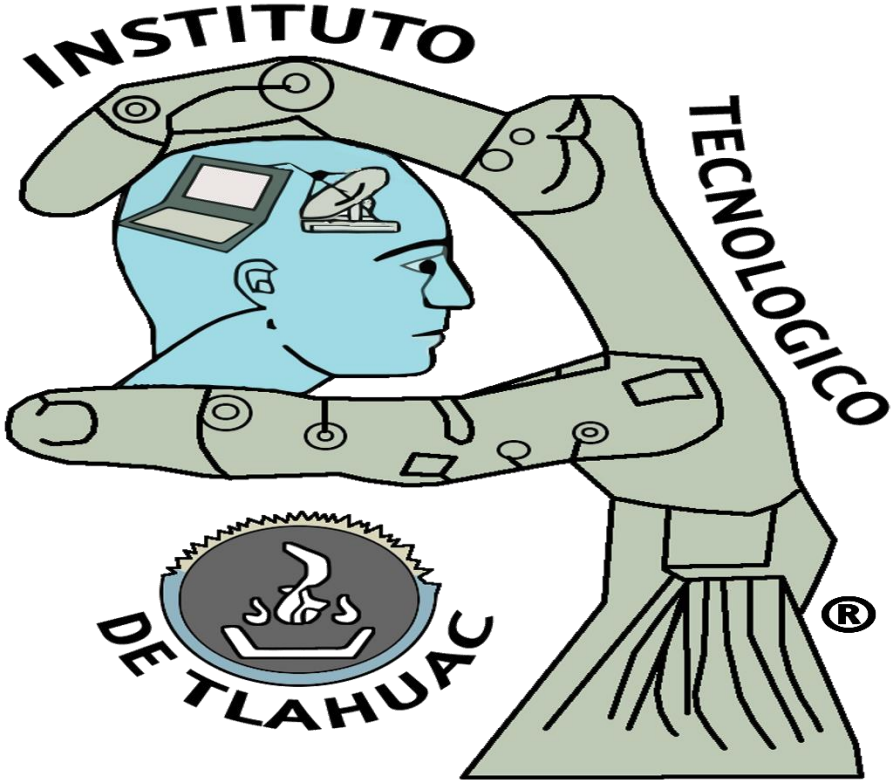
Asignatura: Administración de Servicios Web.

Maestro: Domínguez Hernández Roberto

Ciclo Escolar: 2016-2020

Fecha: 01 De Mayo Del 2020

Trabajo: Investigar Las Técnicas De Implementación De Firma Electrónica y Certificados Digitales



¿Qué es la firma electrónica?

Firma electrónica simple El término firma electrónica (o firma electrónica simple) implica el uso de cualquier medio electrónico para firmar un documento.

Es este sentido, el simple escaneo de una firma autógrafa y su inserción como imagen en un documento digital puede considerarse como firma electrónica. Sin embargo, este tipo de firma electrónica no garantiza los servicios de no repudio, por ejemplo. Otro ejemplo es el uso de un lápiz electrónico para recabar la firma autógrafa (común para expedir credenciales) o mediante la selección de algo en una pantalla táctil por parte del firmante. De igual forma, este tipo de firma no provee los servicios de integridad y no-repudio.

Firma electrónica avanzada

Firma digital La firma digital o firma electrónica avanzada (FEA) establece que se entiende como tal, aquella firma, que a través de un certificado digital emitido por una entidad de certificación acreditada, incorpore una serie de datos electrónicos que identifican y autentifican al firmante a través de la asignación de una llave pública y otra privada en base a los parámetros de la criptografía asimétrica (o también conocida como de llave pública). Mediante este proceso, se garantiza que en el caso de sufrir variaciones en la firma y/o gestión de documentación electrónica, la responsabilidad es del usuario, ya que al tener esta firma bajo su control exclusivo, el usuario es por tanto el responsable último de todos los procesos asociados a la misma. La firma digital es un concepto que nace con la criptografía de llave pública [Menezes et al., 1996] propuesta por W. Diffie y M.

Hellman en 1976 [Diffie and Hellman, 1976]. Este concepto permite la provisión de los servicios de seguridad informática de autenticación y principalmente, no repudio, los cuales no podían garantizarse con la criptografía simétrica existente en ese tiempo. Para implementar este concepto se hace uso de la teoría de números del álgebra abstracta, en lo que respecta a la teoría de grupos y campos finitos [Lidl and Niederreiter, 1986].

¿Para qué se usa la firma digital?

Una firma digital es una firma electrónica que se puede usar para autenticar la identidad de quien envía un mensaje o quien firma un documento electrónico, así como asegurar que el contenido original del mensaje o del documento electrónico que ha sido enviado no ha sido modificado. Las firmas digitales son fácilmente transportables y no pueden imitarse.

La firma digital puede aplicarse a cualquier tipo de información electrónica, ya sea que se encuentre cifrada o en texto claro. En la tabla 1 se muestra una comparación entre la firma digital y la firma autógrafa. En la tabla 2 se muestra una comparación entre la firma digital y otros mecanismos de autenticación [Gupta et al., 2004], de donde se puede observar que la firma digital es un mecanismo eficaz, equiparable al ADN como medio de autenticación. En términos prácticos y desde el punto de vista legal, una firma digital provee una solución viable para contar con documentos electrónicos con validez jurídica. Parecido al método de firma basada en papel y tinta, la firma digital agrega al documento digital la identidad del firmante. Sin embargo, a diferencia de la firma autógrafa, es considerado imposible falsificar una firma digital en la forma en que si se podría falsificar una firma autógrafa. Además, la firma digital asegura que cualquier cambio realizado a los datos firmados no

puede ser indetectable. Con ello, es posible eliminar la necesidad de contar con documentos impresos firmados. Además de los ahorros en consumo de papel, la firma digital permite automatizar los procesos de manipulación de los documentos, tales como su distribución y almacenamiento. La implementación de la firma digital está regulada de acuerdo a las leyes de cada país.

Propiedad	Firma autógrafa	Firma digital
Se puede aplicar a documentos electrónicos y transacciones	No	Si
El proceso de verificación de firma digital puede automatizarse	No	Si
La firma permite detectar alteraciones en el documento	No	Si
Está reconocida por la ley[a]	Si	Si

Tabla 1: Ventajas de la firma electrónica avanzada (firma digital) frente a la firma autógrafa.

Médio de autenticación	Fallas en la autenticación	Tasa de falsos rechazos	Tasa de falsos aceptados	Fácil de usar	Altamente seguro
Firma digital	♦♦♦♦♦	♦♦♦♦♦	♦♦♦♦♦	♦♦♦♦◊	♦♦♦♦♦
Tarjeta inteligente	♦♦♦♦◊	♦♦♦♦◊	♦♦♦♦◊	♦♦♦♦♦	♦♦◊◊◊
Passwords	♦♦♦♦♦	♦♦♦♦♦	♦♦♦♦♦	♦♦♦♦♦	♦◊◊◊◊
Firma escrita	♦♦♦◊◊	♦♦♦◊◊	♦♦♦◊◊	♦♦♦♦♦	♦♦♦◊◊
Voz	♦◊◊◊◊	♦♦♦◊◊	♦♦♦◊◊	♦♦♦♦◊	♦♦◊◊◊
Huella dactilar	♦♦♦♦◊	♦♦♦♦◊	♦♦♦♦◊	♦♦♦♦◊	♦♦♦◊◊
Geometría de la mano	♦♦◊◊◊	♦♦◊◊◊	♦♦◊◊◊	♦♦♦♦◊	♦♦♦◊◊
Reconocimiento de rostro	♦♦◊◊◊	♦♦◊◊◊	♦♦◊◊◊	♦♦♦♦◊	♦♦◊◊◊
Patrón de Retina	♦♦♦♦◊	♦♦♦♦◊	♦♦♦♦◊	♦♦♦◊◊	♦♦♦♦◊
Escaneo de Iris	♦♦♦♦◊	♦♦♦♦◊	♦♦♦♦◊	♦♦♦◊◊	♦♦♦♦◊
ADN	♦♦♦♦♦	♦♦♦♦♦	♦♦♦♦♦	♦♦♦◊◊	♦♦♦♦♦

Tabla 2: Comparación de tecnologías de autenticación en base a 5 factores de desempeño. Entre más marcas obscuras existan, mejor la métrica ofrecida por el mecanismo de autenticación.

Esquema general de la firma digital

Con la criptografía de llave pública es posible implementar el concepto de firma digital. En lugar de usar tinta y papel para firmar un documento, la firma digital usa "llaves" digitales generadas de acuerdo a la teoría de la criptografía de llave pública. El esquema de operación de firma digital es similar al proceso de cifrado solo que las llaves pública y privada son invertidas, es decir, la llave privada se emplea para generar la firma del mensaje o documento electrónico y la llave pública se utiliza para verificar dicha firma.

El diagrama general de la firma digital se muestra en la figura 2. Para generar la firma digital primero se obtiene un resumen de la información electrónica que se firmará usando un algoritmo hash, el cual aplica una función unidireccional a cada bit del mensaje o documento electrónico y produce como salida una cadena binaria, que puede interpretarse como la huella digital del de los bits de entrada. La función hash es tal que a partir del resumen o huella digital es prácticamente imposible poder deducir el mensaje o documento electrónico que lo produce. Esta última aseveración depende de número de bits que se usen para representar al resumen o huella digital que la función

hash produce. El actual estándar para calcular funciones hash es la familia SHA-2, donde el resumen del mensaje puede ser de entre 200 a 600 bits.

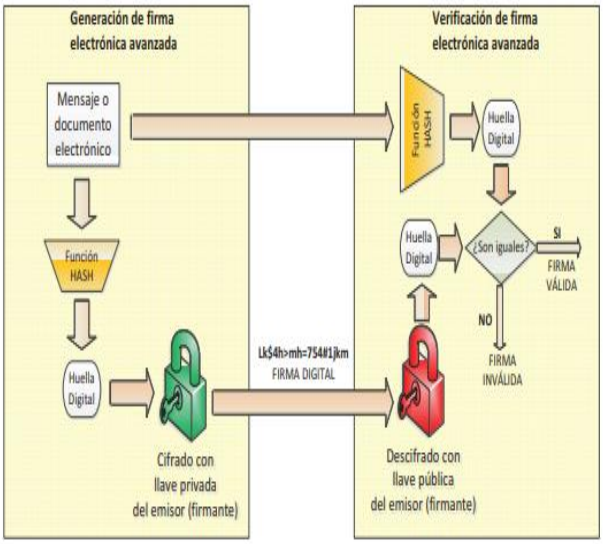


Figura 2: Esquema general de la firma digital.

La cadena binaria correspondiente al resumen del mensaje/documento entonces se cifra con la llave privada del firmante, resultando una nueva cadena binaria que representa la firma digital del mensaje/documento. Entonces el mensaje/documento junto con la firma se distribuye o almacena. Después, para realizar el proceso de verificación, se descifra la cadena binaria correspondiente a la firma digital usando la llave pública del firmante. Este valor descifrado debe corresponder al valor hash original del archivo firmado. Entonces, solo resta calcular nuevamente el valor hash del mensaje/documento y compararlo con el valor resultante del descifrado. Si los valores coinciden, la firma digital es considerada auténtica, de lo contrario, la firma es rechazada, por lo que quién verifica la firma considera como inválido el mensaje/documento, ya que éste o ha sufrido modificaciones y no corresponde al mensaje/documento originalmente firmado, o se esta intentando verificar la firma con la llave pública de un usuario distinto al que firmó el mensaje/documento.

Seguridad de los esquemas de firma digital

En el esquema de firma digital, el firmante posee dos llaves, una pública y una privada, además se requiere de dos procesos uno de cifrado y otro de descifrado así como de la aplicación de una función hash. Existen diversos criptosistemas que se han propuesto para llevar a cabo el proceso de generación y verificación de firma digital, en los que se definen los algoritmos para generar las llaves pública y privada y los algoritmos de cifrado/descifrado.

La seguridad de estos algoritmos se basa en la dificultad para resolver computacionalmente problemas en el dominio del álgebra abstracta. En particular, los problemas en los que los esquemas de firma digital basan su seguridad son el problema de la factorización de números enteros grandes [Rivest et al., 1978] (criptosistema RSA) y el problema del logaritmo discreto, en grupo multiplicativo

[Gal, 2000] (Criptosistema DSA) o en grupo abeliano de curvas elípticas [Johnson et al., 2001] (Criptosistema ECC). En general, cualquier esquema de firma digital resulta ser lento, ya que los algoritmos de cifrado, descifrado y generación de llaves pública y privada realizan diversas operaciones en campos finitos con números de 512, 1024 o 2048 bits, dependiendo del nivel de seguridad que se maneje y del algoritmo usado. Actualmente, existen APIs para la incorporación de estos algoritmos en aplicaciones para distintas tecnologías (Java, .NET, Web, etc.), pero es necesario un claro entendimiento de como operan los esquemas de firma digital a fin de conseguir no solo implementaciones eficientes sino también implementaciones seguras.

Algoritmos criptográficos y recomendaciones de tamaños de llaves

En enero de 2011, el NIST (National Institute of Standards and Technology) emitió el documento SP800- 131A2 donde recomienda algoritmos criptográficos usados para firma electrónica así como las longitudes de llaves recomendadas para uso práctico en los próximos años. En la tabla 3 muestra esta información. Para la generación de la firma digital, el uso de llaves con una longitud equivalente a 80 bits de seguridad es aceptable hasta el año 2010. A partir del año 2011 y hasta el año 2013, el uso de longitudes de llaves con un nivel de seguridad de 80 bits es arriesgado, sobre todo entre más se acerque la fecha límite que es diciembre de 2013.

Después del año 2013, un nivel de seguridad de 80 bits ya no es permitido. La recomendación es utilizar un nivel de seguridad igual o mayor a 112 bits, lo que equivales a usar llaves para DSA y RSA de más de 2048 bits y para ECC, usar llaves de longitud mayor a 224 bits.

Generación de firma digital	Nivel de seguridad de 80 bits : DSA: $((\|p\| \geq 1024)$ and $(\|q\| \geq 160))$ and $((\|p\| < 2048)$ OR $(\|q\| < 224))$ RSA: $1024 \leq \|n\| < 2048$ ECC: $160 \leq \|n\| < 224$	Aceptables hasta el año 2010 En desuso de 2011 a 2013 No permitido depués de 2013
	Nivel de seguridad $\geq$ 112 bits: DSA: $\|p\| \geq 2048$ and $\|q\| \geq 224$ RSA: $\|n\| \geq 2048$ ECC: $\|n\| \geq 224$	Aceptable
Verificación de firma digital	Nivel de seguridad de 80 bits: DSA: $((\|p\| \geq 1024)$ and $(\|q\| \geq 160))$ and $((\|p\| < 2048)$ OR $(\|q\| < 224))$ RSA: $1024 \leq \|n\| < 2048$ ECC: $160 \leq \|n\| < 224$	Aceptables hasta el año 2010 En desuso después de 2010
	Nivel de seguridad $\geq$ 112 bits DSA: $\|p\| \geq 2048$ and $\|q\| \geq 224$ RSA: $\|n\| \geq 2048$ ECC: $\|n\| \geq 224$	Aceptable

Tabla 3: Algoritmos criptográficos y sus respectivos tamaños de llave recomendados por NIST. Para DSA, $|p|$ es el número de bits de la llave pública y privada mientras que $|q|$ indica el número de bits de la firma digital. En el caso de RSA $|n|$ representa el tamaño de la llave pública y para ECC, $|n|$ representa el tamaño de la llave pública y privada.

Certificados digitales

En implementaciones reales de la firma digital, es necesaria la utilización de certificados digitales a fin de proveer confianza en el proceso, ya que al igual que en el mundo real, es necesario contar con algo o alguien que le de validez a la identidad de alguien. De forma análoga a un documento oficial que garantiza la identidad de una persona, los certificados digitales fungen como identificaciones para un usuario en una transacción que involucre una firma digital, ya que es el certificado digital de un firmante el que se usa para verificar las firmas que él genera. El estándar X.509 especifica, entre otras cosas, formatos para certificados digitales y un algoritmo de validación de la ruta de certificación. Los formatos de codificación más comunes son DER (Distinguish Encoding Rules) o PEM (Privacy Enhanced Mail). X.509 es la pieza central de la infraestructura de clave pública y es la estructura de datos que enlaza la clave pública con los datos que permiten identificar al titular. Un certificado contiene diversos campos, su estructura es la siguiente: La estructura de un certificado digital X.509 (versión 3) es la siguiente:

• Certificado

– Versión

– Número de serie

– ID del algoritmo

– Emisor

– Validez

∗ No antes de

∗ No después de

– Sujeto

– Información de clave pública del sujeto

∗ Algoritmo de clave pública

∗ Clave pública del sujeto

– Identificador único de emisor (opcional)

– Identificador único de sujeto (opcional)

– Extensiones (opcional)

• Algoritmo usado para firmar el certificado

• Firma digital del certificado

Una parte importante de los certificados digitales es el campo "Extensions", en el cual se puede agregar información propia de la aplicación de firma electrónica que se desarrolla, por ejemplo, el ID de empleado, ID de funcionario o Matricula de estudiante.