



**USAL
UNIVERSIDAD
DEL SALVADOR**

FIRMA DIGITAL



**USAL
UNIVERSIDAD
DEL SALVADOR**

**Carlos Mariano Graziano
Universidad del Salvador
Facultad de Ingeniería
Ingeniería en Informática
Buenos Aires
2016**

Abstract

Históricamente la firma manuscrita fue utilizada como medio para identificar identidad y voluntad de quien la usa y su consentimiento en todo contrato o acuerdo comercial presencial.

La firma digital se originó como un concepto teórico en 1974 ante la necesidad tecnológica de otorgar las mismas certezas que da la firma manuscrita en los acuerdos presenciales a los acuerdos hechos a distancia por medio de los nuevos canales de comunicación. Posteriormente se implementaron distintos esquemas de firma digital que llevaron a la práctica este concepto teórico.

En el mundo y en la Argentina, se equiparó legalmente la firma digital a la firma manuscrita pero su uso está limitado a casos muy puntuales.

El objetivo de este trabajo es analizar los factores tecnológicos necesarios para la utilizar la firma digital como reemplazo de la firma manuscrita.



USAL
UNIVERSIDAD
DEL SALVADOR

Abstract	2
Introducción	5
La firma	5
La firma y las comunicaciones a distancia	6
Marco Teórico	11
Criptografía	11
La Firma Digital	11
Algoritmos de Firma Digital	13
Funciones Hash	14
Algoritmos de HASH	14
Funcionamiento conceptual del proceso de Firma Digital	15
Certificado Digital	16
Estándar de Certificados Digitales X.509	17
Marco Legal y Marco Normativo	17
El Código Civil y Comercial	17
Marco Legal de Infraestructura de Firma Digital	19
La Ley de Firma Digital	20
Autoridades Certificantes según el Marco Legal vigente	25
Estándares de Firma Digital según la Ley	26
Marco Metodológico	27
Objetivo del Proyecto	27
Pregunta del Proyecto	27
Hipótesis	27
Justificación del Proyecto	27
Marco Metodológico	28
DESARROLLO	29
Introducción	29
Factores Tecnológicos del Documento Digital	30
Conservación en el tiempo	30
Compatibilidad con PKI y Almacenamiento de Firma	32
Factores Tecnológicos del Proceso de Solicitud y Almacenamiento de Firma Digital	35
Introducción	35
Factores tecnológicos de la firma digital de un documento	40
Por medio de aplicaciones de terceros:	40
Por medio de un desarrollo propio.	43
Factores tecnológicos de validación de firma digital.	49



Por medio de la herramienta de un tercero,:	49
Por medio de un desarrollo propio	51
Verificación por Cadena de Certificación	51
Verificación vía OCSP	55
Conclusión	56
Bibliografía	57
ANEXO 1	
Código fuente completo para firmar digitalmente un documento.	59
Código fuente completo de aplicación para verificar una firma digital.	61



USAL
UNIVERSIDAD
DEL SALVADOR

Introducción

La firma

Etimológicamente la palabra firma proviene del latín “firmare” que significa afirmar.

La Real Academia Española, define a la firma como al “Rasgo o conjunto de rasgos, realizados siempre de la misma manera, que identifican a una persona y sustituyen a su nombre y apellidos para aprobar o dar autenticidad a un documento”.

Adicionalmente y a los fines de este proyecto cabe resaltar, pese a la obviedad, que la capacidad de firmar es propia de todos los seres humanos.

Coutoure (2004) en su obra “Vocabulario Jurídico” (citado en Sanchez, Pérez, Perinat, 2015) define la firma como “Trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse en lo que en ellos se dice”.

Podemos definir entonces que la firma:

- Identificar al autor de un documento.
- Declara voluntad de aceptar obligaciones y responsabilidades que se describen en el documento donde es realizada.

Adicionalmente, Zúñiga (2004) plantea que el uso de la firma como tal, presenta una serie de retos a considerar:

- Garantía de Autenticidad: La necesidad de asegurarse que la firma es de quien dice ser.

- Integridad del documento: La certeza de la no modificación del documento una vez firmado.
- Capacidad de Repudio: Sobre la capacidad que tiene el firmante de desconocer que esa firma le pertenece o haya sido hecha por él. “El firmante siempre podrá aludir no ser el autor de la misma y argumentar falsificación, obligando a seguir a este respecto” (Zuñiga, 2004)

La ciencia y el derecho utilizan la caligrafía como parte de sus procesos legales y/o periciales de validación y comprobación como método para mitigar la problemática planteada por estos retos. Esto hace a la firma como un método confiable para acreditar identidad y para demostrar voluntad o acuerdo con lo firmado.

La firma y las comunicaciones a distancia

Los riesgos mencionados de la firma se reducen en los actos presenciales, como el caso del cliente que va a la sucursal bancaria a abrir una cuenta. Pero en el caso de los acuerdos y las comunicaciones a distancia la realidad es otra y los retos que plantea Zúñiga se potencian, planteando dilemas tales como el de cómo saber que la firma de un documento recibido por un medio de comunicación inseguro o convencional es fehacientemente de quien se supone su autor o que el documento no fuera alterado por un tercero en el transcurso del envío.