Firmas digitales en México: conceptos, oportunidades y desafíos

Miguel Morales Sandoval
Cinvestav Tamaulipas
Ciudad Victoria, Tamaulipas, Mexico
miguel.morales@cinvestav.mx

RESUMEN

Las firmas digitales son el análogo digital de las firmas autógrafas a mano, las cuales se han usado de manera amplia para garantizar la autenticidad de un documento y de su contenido, así como de la aceptación de lo ahí especificado por aquellos que lo firman. Las firmas digitales han experimentado un proceso de adopción lento a pesar de los enormes beneficios que conllevan, como el ahorro de papel, la automatización de los procesos de firma, verificación, almacenamiento y recuperación de documentos firmados.

La necesidad de contar con herramientas tecnológicas que automaticen las tareas asociadas al uso de firmas digitales se evidenció con la pandemia de COVID-19, ya que muchos de los procesos administrativos en distintos ámbitos requirió del manejo de documentos digitales y de firmas digitales, para su fácil recolección, distribución y tratamiento. Aquellos que no contaron con este tipo de herramientas, vieron mermados sus procesos, al no poder contar con firmas sobre documentos en físico.

En este artículo se describen los principales conceptos de las firmas digitales, fundamentadas en algoritmos criptográficos que proveen servicios de integridad, autenticación, y cuando se usan certificados digitales, no repudio. Se presenta un análisis del caso de México, discutiendo los principales retos y oportunidades en el país para el uso amplio de firmas digitales.

PALABRAS CLAVE

Firma autógrafa, firma digital, automatización, certificados digitales, infraestructura de clave pública, digitalización

Citar como:
Miguel Morales Sandoval. 2022. Firmas digitales en México: conceptos, oportunidades y desafíos. En Miguel Morales Sandoval, José Gabriel Ramírez Torres y Javier Rubio Loyola (Eds.), *Ciencia e Ingeniería en Tecnologías Computacionales*, capítulo 3, 8 páginas. Cinvestav Unidad Tamaulipas, Ciudad Victoria, Mexico, ISBN: 978-607-9023-65-2.

1. INTRODUCCIÓN

La firmas manuscritas han sido, tradicionalmente, el medio más usado en la era contemporánea para garantizar la autenticidad de un documento. Mediante una firma, se puede identificar al suscriptor del documento que expresa su conocimiento y consentimiento del contenido del mismo, en el tiempo. La firma autógrafa es un mecanismo aceptado universalmente y que aún se usa ampliamente, mediante el cual se formalizan acuerdos, se adquieren derechos u obligaciones.

Jornadas de Divulgación - TopTamaulipas 2021, Noviembre 9–18, 2021, Ciudad Victoria, TAMPS

ISBN 978-607-9023-65-2.

Los dos retos principales en relación con las firmas manuscritas son [1]: 1) garantizar la autenticidad de la firma, esto es, identificar inequívocamente al firmante (*autenticación*) y que el firmante no pueda negar haber realizado la firma (*no-repudio*); 2) garantizar que el documento no se ha modificado en su contenido después de haber sido firmado (*integridad*). Para conseguir estos objetivos, la firma manuscrita no es suficiente y en algunos casos es necesario agregar elementos adicionales, como hologramas, sellos u otros elementos a los documentos físicos que se firman.

Aunque existen mecanismos para verificar que la firma autógrafa no se ha falsificado, eso no implica que se garantice que el documento no se ha modificado o alterado. Sin embargo, los mecanismos existentes para verificación de autenticidad de firmas autógrafas y de la integridad del contenido de los documentos firmados son difíciles de automatizar [2].

Por otro lado, es innegable la alta disponibilidad y cantidad de información y de documentos en formato electrónico en la actualidad. Esto ha motivado el uso de medios digitales para realizar el firmado de documentos electrónicos por medios electrónicos, que aceleren el proceso de firma del documento al permitir al firmante realizar el firmado desde algún dispositivo electrónico e incluso a través de internet. Al contar con estos mecanismos de firmado electrónico, se aceleran también los procesos de verificación de la autenticidad e integridad de los documentos firmados digitalmente, al permitir la automatización de dichos procesos por algoritmos computacionales.

La firma digital [3] es el equivalente electrónico a la firma autógrafa. El concepto está basado en matemáticas, particularmente en la criptografía asimétrica también conocida como criptografía de clave pública (PKC, por las siglas del inglés Public Key Cryptography), mediante las operaciones cifrar y descifrar [4]. Como medio de autenticación, las firmas digitales son tan o más robustas que otros mecanismos ya conocidos, tal como se muestra en la Tabla 1.

Las firmas digitales requieren de infraestructuras de clave pública (PKI, por las siglas en inglés Public Key Infrastructure) mediante certificados digitales y autoridades de certificación [6]. Este origen hace que el concepto sea complejo de entender para la mayoría de las personas, así como dificulta su asimilación y uso generalizado en organizaciones o por personas, a pesar de las ventajas que ofrece; permitir automatizar los procesos de verificación de autenticidad e integridad, así como garantizar el no-repudio de los documentos firmados por quienes los firmaron.

Actualmente, las firmas digitales no se usan ampliamente a pesar de que la mayoría de los personas cuenta con un equipo de cómputo (computadora de escritorio, portátil o tableta) y de que existen las condiciones tanto legislativas como tecnológicas para implementarlas. Su uso se ha dado mayormente en el entorno gubernamental

Tabla 1: Comparación de mecanismos de autenticación con base en 5 factores de desempeño [5].

Mecanismo de autenticación	Fallas en la autenticación	Tasa de falsos rechazos	Tasa de falsos aceptados	Fácil de usar	Altamente seguro
Firma digital	●●●●●	●●●●●	●●●●●	●●●●○	●●●●●
Firma autógrafa	●●●○○	●●●○○	●●●○○	●●●●●	●●●○○
Contraseñas	●●●●●	●●●●●	●●●●●	●●●●●	●○○○○
Voz	●○○○○	●●●○○	●●●○○	●●●●○	●●○○○
Huella dactilar	●●●●○	●●●●○	●●●●○	●●●●○	●●●○○
Reconocimiento de rostro	●●○○○	●●○○○	●●○○○	●●●●○	●●○○○
ADN	●●●●●	●●●●●	●●●●●	●●●○○	●●●●●

y judicial. Un ejemplo del primer caso es en el Sistema de Administración Tributaria (SAT) de México, donde la mayoría de las operaciones y servicios que los mexicanos realizan ante esta dependencia deben realizarse usando firmas digitales. En el segundo caso, los mexicanos ya pueden presentar una demanda ante un juzgado en línea, usando su firma digital como medio de autenticación y para validación de la solicitud y documentos presentados.

Las robustez y seguridad de las firmas digitales se basan en dos premisas: 1) la dificultad de resolver un problema matemático y 2) la seguridad de una función hash (función resumen). La primera premisa está basada en la complejidad algorítmica, la cual permite estimar el costo computacional para resolver un problema. En las firmas digitales, el problema a resolver para vulnerar la seguridad, es inviable, aún usando la computadora clásica más potente [7–9]. Esto es, a un atacante le tomaría varias decenas de años corromper o falsificar un firma digital. En el caso de la segunda premisa, se trata de una función la cual recibe un conjunto de datos de entrada (el documento a firmar) y produce como salida un código de longitud fija (código hash), único e intrínsecamente relacionado a los datos de entrada. La seguridad de la función hash radica en que es inviable encontrar dos conjuntos de datos diferentes (dos documentos) que produzcan un mismo código hash. Las funciones que actualmente se especifican para uso criptográfico en firmas digitales cumplen con este requisito de seguridad [10, 11].

2. CONCEPTO E IMPLEMENTACIÓN

La Figura 1 muestra un esquema del proceso de creación de una firma digital. En esencia, una firma digital es el cifrado PKC del código hash del documento que se firma. Cabe hacer notar que el documento no necesariamente se cifra, ya que la firma digital solo considera el servicio de autenticación, integridad y no repudio, no el de confidencialidad. Por ello, el documento original junto con su firma deben hacerse disponible a todo aquel que requiera validar el contenido del documento mediante su firma digital asociada.

La verificación de la firma consiste en el descifrado del código hash (código hash del documento que originalmente se firmó), el cual se compara con el código hash del documento actual en posesión del verificador. Si los códigos hash, el decifrado y el obtenido, coinciden, el documento es considerado como auténtico e integro, y se reconoce al firmante como el autentico emisor de la firma.

Como en cualquier algoritmo PKC, el cifrado y descifrado requiere de un par de claves asociadas a un firmante (una es pública y la otra es privada, pero ambas están relacionadas matemáticamente), que son generadas por el mismo algoritmo PKC que se usa para la firma del documento y para la verificación.

De manera general, el ciclo de vida de un documento en la generación y verificación de su firma digital involucra tres etapas (ver Fig. 1) descritas con más detalle en las siguientes secciones.

2.1. Generación de las llaves del firmante

El firmante (persona física o moral) debe generar una pareja de claves mediante un algoritmo PKC. El algoritmo PKC más usado para firmas digitales ha sido RSA [12]. Otros algoritmos de amplio uso para firmas digitales es ECDSA [13]. El algoritmo PKC seleccionado para generación la pareja de claves será el mismo que se use para generar y para verificar las firmas digitales.

Una vez generadas, la clave privada es resguardada por el firmante. La clave pública junto con los datos de identidad del firmante (CURP, INE, RFC, etc) se envían a la PKI, la cual es un conjunto de componentes hardware, software, políticas y procedimientos, que permiten la generación, mantenimiento y manejo de certificados digitales. Un *certificado digital* es una asociación de los datos de identidad de un entidad con una clave pública. Dicha asociación está firmada digitalmente por una autoridad reconocida (*autoridad de certificación*), en la cual se confía.

Es mediante el certificado digital que una entidad no puede en el futuro negar la posesión de una clave pública. Dicha clave se usa, como se detalla más adelante, en el proceso de verificación de firmas digitales, donde inequívocamente, se demuestra que una firma digital fue generada con la clave privada asociada a dicha clave pública, con lo que se garantiza el no repudio.

2.2. Firmado

Una entidad que cuente con su clave privada k_A y con el certificado digital de su correspondiente clave pública P_A, está en posibilidad de generar firmas digitales que más adelante puedan ser validadas por cualquier otra entidad. En el paso 3, la firma digital de un documento D se genera de la siguiente forma.

- Primero, el firmante debe calcular el código hash de D, usando una función hash H ($h = H(D)$).
- El código hash resultante es cifrado (por ejemplo, con el algoritmo RSA o con ECDSA) usando k_A ($\sigma_{D,A} = CIFRADO - PKC(h, k_A)$). De esta forma, solo el propietario de la clave privada puede generar sus firmas, y nadie más. La notación $\sigma_{D,A}$ indica la firma de A del documento D. Cabe resaltar que las firmas de A son distintas para cada documento diferente.

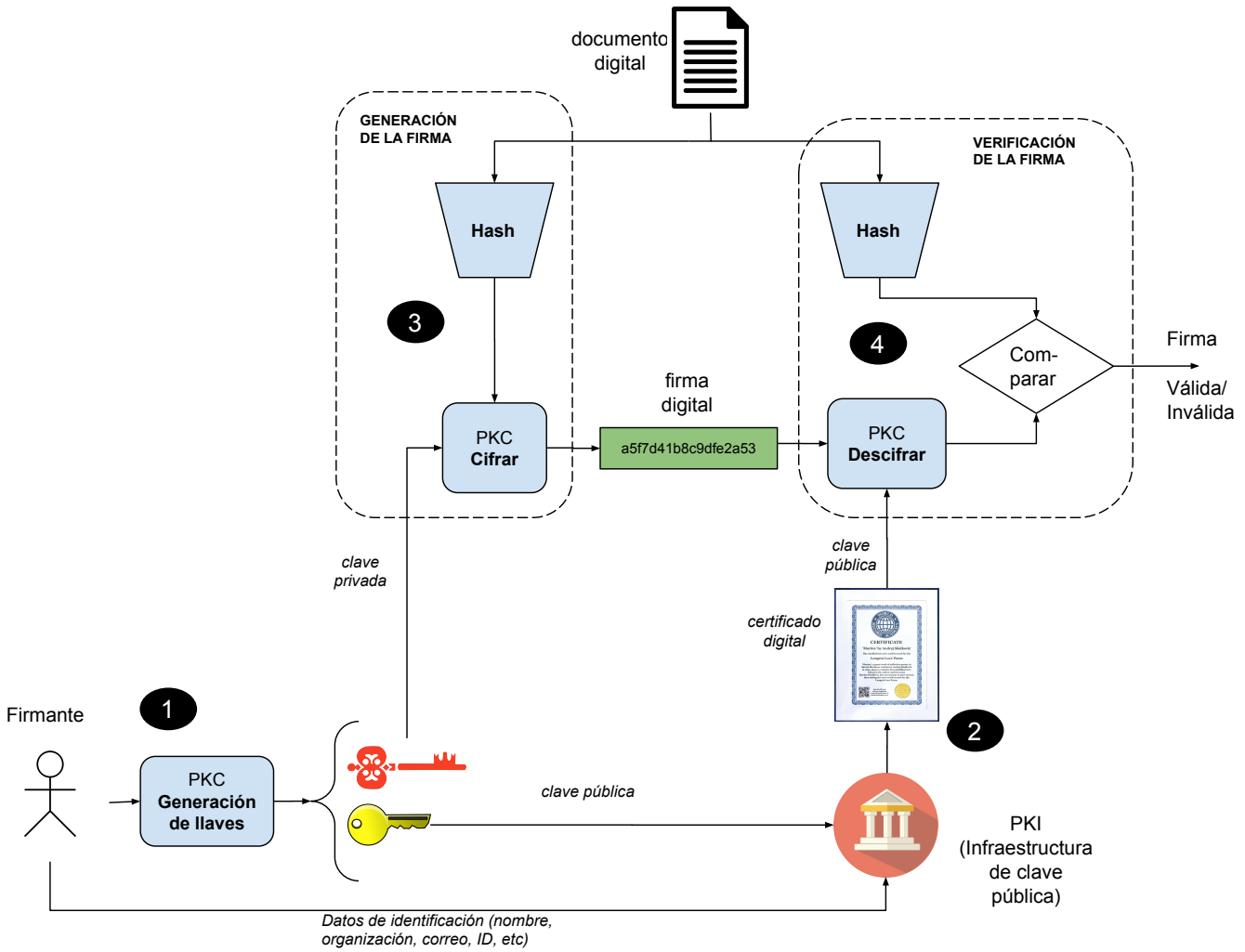

Figura 1: Esquema general de generación y verificación de una firma digital.

Es de suma importancia que el firmante mantenga de manera segura su clave privada y no la revele a nadie. Este aspecto es muchas veces tomado a la ligera, y en aras de la practicidad, las claves privadas son proporcionadas a terceros que son los que realizan las operaciones de firma (por ejemplo, en la firma de declaraciones anuales por parte del contador de una persona).

En la práctica, antes de realizar el cifrado de h es necesario verificar que el certificado digital del firmante sea válido (no esté caducado o no haya sido revocado). La verificación del certificado digital se realiza en línea, a través de la PKI que generó dicho certificado. La firma digital $\sigma_{D,A}$ es una pieza de información, carente de significado para cualquier entidad, pero con los elementos que permiten garantizar los servicios de autenticación, integridad y no-repudio de la firma sobre el documento firmado.

2.3. Verificación

El documento D y la firma creada $\sigma_{D,A}$ se almacenan en alguna parte o se distribuyen a los destinatarios interesados, para que posteriormente se pueda verificar la autenticidad de la firma y/o la integridad del documento firmado usando P_A. De esta forma, cualquiera puede verificar una firma digital dado que P_A es un componente público.

Nótese que para la firma digital, no es necesario que el documento sea cifrado. El contenido del documento puede mantenerse legible y entendible para cualquier entidad, como generalmente ocurre en las firmas manuscritas.

La verificación se realiza de la siguiente manera:

- Se debe contar con el documento D, la firma $\sigma_{D,A}$ de dicho documento y el certificado digital de A que contiene su clave pública P_A.
- Al documento D', en posesión del verificador, se le calcula nuevamente el código hash usando la misma función H que se usó en el proceso de firma ($h' = H(D')$). Denotamos a este documento como D' ya que no necesariamente podría ser el mismo que se firmó (alguien pudo alterarlo accidental o intencionalmente).

- Se descifra la firma digital usando P_A. Dado que el descifrado es la operación inversa del cifrado realizado durante el proceso de firma, si realmente P_A está asociada a la clave privada k_A usado en el cifrado, entonces DESCIFRADO-PKC($\sigma_{D,A}, P_A$)) = DESCIFRADO-PKC(CIFRADO-PKC(h, k_a), P_A)) = h. De esta forma, se recupera el hash original.

Lo que resta es verificar si $h' = h$. Si así es, el documento D' se considera como el documento D originalmente firmado por A. La comparación fallará si alguno de los casos siguientes se cumple: 1) se usa un certificado digital cuya clave pública asociada no corresponde a la clave privada que se usó durante el proceso de firma; 2) el documento al que se le calcula el código hash nuevamente, ha sido modificado respecto al documento que se firmó inicialmente.

De acuerdo con el proceso previamente descrito, las firmas digitales tienen la propiedad de asociar la firma al contenido de lo que se firma, algo que no es posible de realizar en el caso de las firmas manuscritas. Es por ello que aunque se trate del mismo firmante, las firmas digitales no serán las mismas (a menos que se trate de exactamente el mismo documento digital, bit por bit). De acuerdo con el algoritmo PKC seleccionado, el firmante siempre obtendrá la misma firma para un mismo documento.

3. INFRAESTRUCTURA PARA FIRMAS DIGITALES EN MÉXICO

La implementación oficial de firmas digitales en México data desde el año 2000. La firma digital, también conocida como firma electrónica avanzada (FEA), se diferencia de una firma electrónica simple por la propiedad de cumplir tanto con el requerimiento de autenticación así como vincular la firma al contenido del documento que se firma. La firma electrónica (simple) en cambio, puede ser cualquier signo, imagen o elemento digital 'añadido' al documento, el cual carece de la propiedad de autenticación (fácilmente falsificable) y no es vinculante al contenido del documento.

Por ejemplo, un documento en word con una imagen insertada de la firma manuscrita de una persona es un documento con firma electrónica simple, pero no es un documento con firma digital. En cambio, la declaración anual presentada al SAT y firmada con el certificado digital del contribuyente, sí es una firma digital, o como se conoce también en México, una Firma Electrónica Avanzada.

El 11 de enero de 2011 se publicó en el Diario Oficial de la Federación el decreto por el que se expide la Ley de Firma Electrónica Avanzada. Mediante este ley, se reconoce la equivalencia entre la firma autógrafa y la digital, y se definen las características de los certificados digitales y de PKI. De igual forma, con el decreto se da sustento jurídico a los actos realizados por los ciudadanos y las empresas ante los organismos del Gobierno Federal.

El uso y aplicación de la firma digital en México ha sido promovida por el Banco de México, así como a través de dependencias del gobierno federal, como el Sistema Administración Tributaria (SAT), la Secretaría de Economía, y la Secretaría de la Función Pública.

3.1. Infraestructura de clave pública (PKI)

Un proveedor de certificados digitales debe contar con una PKI para poder emitir y administrar dichos certificados. Como se ha mencionado, un certificado digital es un documento electrónico que asocia una entidad (su identidad) con una clave pública en el contexto de PKC. Dicho documento está firmado por la entidad que corrobora, mediante medios verificables oficiales, la identidad del posesor del certificado y la validez de su clave pública.

Al generar un certificado digital (usando documentos y/o datos de identidad y la clave pública del posesor del certificado) se garantiza que el certificado es único, esto es, se evita que una entidad cuente con más de una clave pública. Para un certificado creado, mediante la PKI se puede verificar, a través de un protocolo, que el certificado digital no haya sido revocado o esté caducado. En México, la PKI más conocida es el SAT (Servicio de Administración Tributaria), quien mediante un proceso bien definido, otorga a los mexicanos una pareja de claves para uso en firmas digitales. Estas claves son proporcionadas generalmente en un dispositivo USB: el archivo `.cer` contiene los datos de la clave pública y el archivo `.key` contiene los datos de la correspondiente clave privada. Por seguridad, la clave privada está potegida y su acceso requiere de una contraseña. En la Fig. 2 se muestra una página web del gobierno de México donde para realizar el trámite correspondiente, se solicitan los datos del certificado digital, y de la clave privada protegida por contraseña.

3.2. Infraestructura extendida de seguridad

La Infraestructura Extendida de Seguridad (IES) [14] es un sistema diseñado y administrado por Banco de México para la emisión y administración de certificados digitales. Se creó inicialmente bajo el contexto de uso de medios electrónicos en los sistemas de pagos en México. Sin embargo, la IES se usa ampliamente para la emisión de certificados digitales por dependencias del gobierno federal, siendo el SAT la entidad más conocida como emisora de certificados digitales para personas físicas y morales. La IES es flexible e independiente del sistema criptográfico PKC que se use (ver Fig. 1). En la IES, los participantes principales son:

1. *Agencia Registradora Central /ARC).* Crea su propio certificado digital (raíz) y certifica a Agencias Registradoras (ARs) y a Agencias Certificadoras (ACs), ver descripción abajo. Garantiza la unicidad de las claves públicas del sistema y administra la base de datos de las claves públicas correspondientes a los certificados digitales que las ARs tengan registradas en sus bases de datos. Difunde su clave pública y las claves públicas de las ARs y ACs a través del sitio www.banxico.org.mx.
2. *Agencias Registradoras (AR).* Registra certificados digitales siempre y cuando la ARC confirme la unicidad de las claves públicas. Administra las bases de datos con los todos los certificados digitales que ha registrado. Proporciona información de certificados digitales (electrónicamente). Revoca certificados digitales de acuerdo con las disposiciones aplicables e informa de dicha revocación a la AC que emitió dichos certificados.
3. *Agencias Certificadoras AC.* Emiten certificados digitales. Solicita a la AR que corresponda, la revocación de los certificados digitales que haya emitido, de acuerdo con las disposiciones aplicables o cuando los usuarios, directamente o a través de un Agente Certificador (ver abajo), lo soliciten. Puede auxiliarse de un agente certificador en la realización de sus funciones.

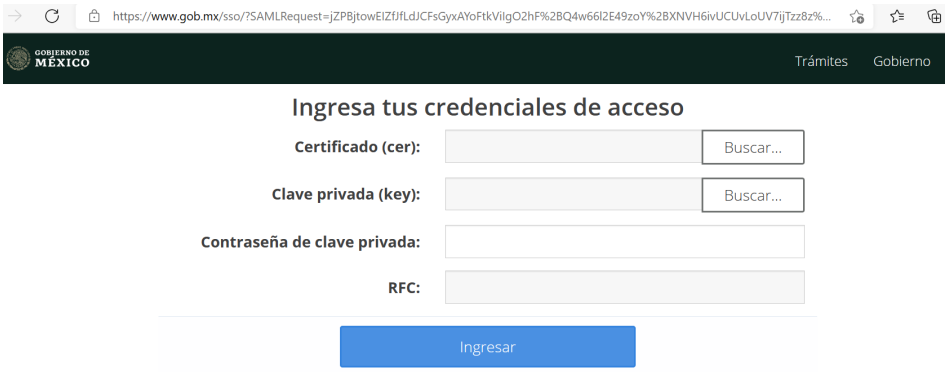

Figura 2: Sistema web del gobierno de México donde el trámite requiere el certificado digital y la clave privada del ciudadano.

4. *Agentes Certificadores AgC*. Es auxiliar de la AC. Verifica la identidad de los solicitantes que desean obtener certificados digitales, con base en los documentos oficiales que éstos les presenten. Proporciona al solicitante de un certificado digital los medios necesarios para la generación de datos de creación y verificación de su firma electrónica. Entrega al titular su certificado digital registrado y la carta de aceptación del referido certificado digital en la que conste su firma autógrafa. Finalmente, informa, en su caso, al titular de la revocación de su certificado digital.
5. *Usuarios*. Solicita su certificado digital a una AC directamente o a través de un AgC, presentando su requerimiento digital y documentos oficiales de identificación. Establece, en secreto y en forma individual, su frase de seguridad con la que podrá cifrar su clave privada para protegerla. Genera, en secreto y en forma individual, su par de claves (pública y privada). Mantiene en un lugar seguro su clave privada. Tiene acceso a un servicio que le permite revocar, en línea, su certificado digital en cualquier momento.

El Banco de México y la Secretaría de Economía han fungido como Agencias Registradoras en el contexto de la IES. Aunque la AC más conocida en México es el SAT, un usuario puede optar por obtener un certificado digital a través de una organización privada acreditada por el gobierno de México, conocidas como Prestador de Servicios de Certificación o PSC. Estas entidades están acreditadas por la Secretaria de Economía y cuentan con su propia infraestructura PKI.

Los datos que el firmante utiliza para crear una firma digital son su clave privada, frase de seguridad que permite acceder a la clave privada y el certificado digital asociado a la clave privada (ver Fig. 1). Lo que cualquier entidad necesita para verificar una firma digital es solamente el certificado digital del firmante, el cual se obtiene de la IES a través de una AR. El firmante y la entidad que verifica la firma deben contar con sistemas de cómputo para crear y verificar la firma, respectivamente, mediante la implementación de algoritmos criptográficos. Estos sistemas deben mantener comunicación con la IES, para solicitar y verificar la validez de los certificados digitales de los usuarios involucrados en los procesos de firma.

4. FIRMA DIGITAL EN MÉXICO

A diferencia de otros países, el uso de firmas digitales en México aún es incipiente. Uno de los principales obstáculos en el proceso de adopción de esta tecnología es la falta de confianza y de conocimiento de la misma. La mayoría, tanto personas físicas como morales, desconocen la tecnología de firmas digitales, consideran que es complejo desplegar dicha tecnología o creen que esta tecnología no cuenta con validez jurídica. Esto es, hay desconfianza en el sentido de que al moverse al dominio digital, en algún proceso legal, puedan tener dificultades al no presentar documentos con las tradicionales firmas autógrafas.

Sin embargo, con el decreto de la Ley de Firma Electrónica Avanzada en 2011, se ha dado reconocimiento a la equivalencia entre la firma autógrafa y la firma digital. Además, en muchos estados de la república se cuenta con una ley estatal de firma digital, por lo que su validez está contemplada. Al momento de escribir este artículo, en prácticamente todos los estados de la república mexicana existe legislación en relación con el uso de firmas digitales, las más recientes promulgadas en 2019 (Oaxaca) y 2020 (Chihuahua).

4.1. Requerimientos de sistemas de firma digital en México

Un sistema de firma digital, al menos para aplicaciones en México, debe cumplir con dos requerimientos principales, en concordancia con el Artículo 97 del Código de Comercio.

El primero es garantizar la asociación de la identidad de un firmante con su clave pública. Esto es, las AC encargadas de crear los certificados digitales deben ser reconocidas ante las AR y en este caso, las que sean reconocidas por el Banco de México de acuerdo a la IES. La validez del certificado debe corroborarse al momento de realizar la tarea de firma, por lo que la AC/AR que lo emitió debe proveer los mecanismos para realizar dicha consulta y verificar que el certificado no esté caducado o no haya sido revocado.

El segundo requisito es que el firmante debe tener control exclusivo sobre los datos que permiten generar firmas digitales en su nombre. Esto es, la clave privada que se usa para la generación de la firma digital debe estar en posesión y control exclusivo del firmante. De esta manera se evita que el firmante pueda negar haber realizado la firma de algún documento y argumentar que la firma la realizó un tercero que tuvo acceso a su clave privada. De esta

forma, es responsabilidad exclusiva del firmante salvaguardar el acceso a su clave privada.

4.2. La norma oficial NOM 151

En México, la Secretaría de Economía emitió la Norma Oficial Mexicana NOM-151-SCFI-2016, conocida como NOM 151, que es una regulación para el tratamiento de contratos comerciales y otros actos celebrados por las empresas, incluyendo su almacenamiento y conservación. En general, esta norma exige garantizar la integridad de los documentos electrónicos (referidos como mensajes de datos) desde su generación, y hacer disponible dicha información cuando se requiera.

Para cumplir con la norma, se debe emitir una *constancia de conservación* por prestador de servicios de certificación (PSC) acreditado para tal fin. En tal constancia debe aparecer una estampa de tiempo indicando la fecha y hora en que se generó.

La NOM 151 estipula que la firma electrónica es uno de los requisitos fundamentales para emitir la constancia de conservación de datos. De acuerdo con la NOM 151, una constancia de conservación de mensajes de datos es una serie de sellos digitales emitidos por el PSC acreditado por la Secretaría de Economía, que permiten verificar la fecha y hora de emisión de un documento electrónico con su correspondiente firma digital.

La constancia de conservación es al análogo a un sello, donde quien emite dicho sello da fe de que un documento no podrá modificarse después, además de indicar la hora y fecha en la que el sello se ha emitido. Quien emite el sello, no requiere conocer el contenido del mensaje, solo debe validar la acción de emisión del documento. Bajo esa analogía, el PSC recibe el hash de un documento y emite el sello digital del mismo, el cual incluye la fecha y hora exacta de su recepción. El PSC firma digitalmente dicho sello.

En México, un PSC forma parte de la PKI, pudiendo ser una persona moral, una institución pública e incluso un fedatario público como un corredor o notario, siempre que cumplan con los requisitos establecidos de acuerdo a la normativa vigente. El SAT es el PSC más conocido en nuestro país[1]. Así, el PSC tiene dos tareas principales: *i*) emitir los certificados digitales para los firmantes y *ii*) emitir constancias de conservación, las cuales como se ha explicado, son el análogo a un recibo digital, que indica la existencia de un documento electrónico, de su(s) firma(s) a partir de una fecha claramente determinada.

En México, existen distintas herramientas tecnológicas para la creación de firmas digitales, las cuales solo permiten generar firmas digitales pero no constancias de conservación. Una de ellos es MiFiel, la cual genera firmas digitales a partir de certificados digitales emitidos por el SAT; puede gestionar la creación de una constancia de conservación para dicha firma a través de un PSC autorizado por la Secretaría de Economía.

Otras herramientas tecnológicas para generación de firmas digitales son Docusing, Globalsign, FirmaMex y Firmatya.

[1]Ver otros PSC en México en: http://www.firmadigital.gob.mx/directorio.html

5. OPORTUNIDADES Y DESAFÍOS PARA UN MAYOR USO DE FIRMAS DIGITALES EN MÉXICO

Dado que, tanto personas físicas como morales, cada vez producen más y más información en formato electrónico, y por tanto, en aquellas situaciones donde se requiere el manejo de firmas manuscritas, se puede aprovechar el uso de las firmas digitales y disfrutar de sus beneficios, que incluyen:

1. Mayor seguridad: Los documentos firmados digitalmente son más difíciles de modificar, además de que la firma digital está relacionada directamente con el contenido del documento. Un cambio mínimo en el documento causará que la verificación de la firma falle.
2. Automatización de procesos, lo que facilita el ciclo de vida de documentos (creación, firmado, almacenamiento, consulta, verificación de firmas). Además, el ciclo de vida de los documentos firmados, en formato electrónico, se beneficia ampliamente, puesto que se puede integrar con tecnologías como cómputo móvil, la nube u otras tecnologías disruptivas como Blockchain.
3. Ahorro de recursos: Menos uso de papel, lo que implica un ahorro económico y una reducción al impacto medioambiental; menor infraestructura para almacenar y mantener documentos en papel; y una mejora considerable en el manejo del ciclo de vida de los documentos firmados.

Sin embargo, existen distintas barreras aún que impiden el uso masivo de firmas digitales, entre ellas se encuentran:

1. Una poca cultura y motivación hacia la digitalización de los procesos, tanto por organizaciones como por personas.
2. Poco o nulo conocimiento tecnológico sobre firmas digitales, además de un arraigo a los métodos tradicionales basados en papel.
3. Poco trabajo de promoción de la tecnología para su uso masivo. Si bien no se puede implantar esta tecnología de manera obligatoria, si se puede incentivar más su uso.
   Las áreas de oportunidad para el uso de firmas digitales es amplio. Por mencionar algunas, tenemos el caso de la firma de las boletas de calificaciones en las escuelas, una actividad muy común. En los procesos gubernamentales, como el de compras, requiere de varias actividades donde se deben enviar solicitudes firmadas, requisiciones o cotizaciones. Toda esta documentación podría hacer uso de firmas digitales para no solo darle la validez al proceso en la organización sino también como un medio de autenticación de los documentos presentados, por ejemplo, en el caso de las cotizaciones.

En México, la investigación y desarrollo en el tema de firmas digitales es escaso, debido a que existen muy pocos grupos de investigación en el área de la criptografía y una ausencia del tratamiento de estos temas en la formación profesional.

En el Cinvestav Tamaulipas se ha realizado trabajo de formación de recursos humanos en materia de firma electrónica, particularmente a nivel licenciatura [15, 16].

En el posgrado, se han realizado investigación y desarrollo tecnológico firmas cortas usando emparejamientos bilineales [17], así

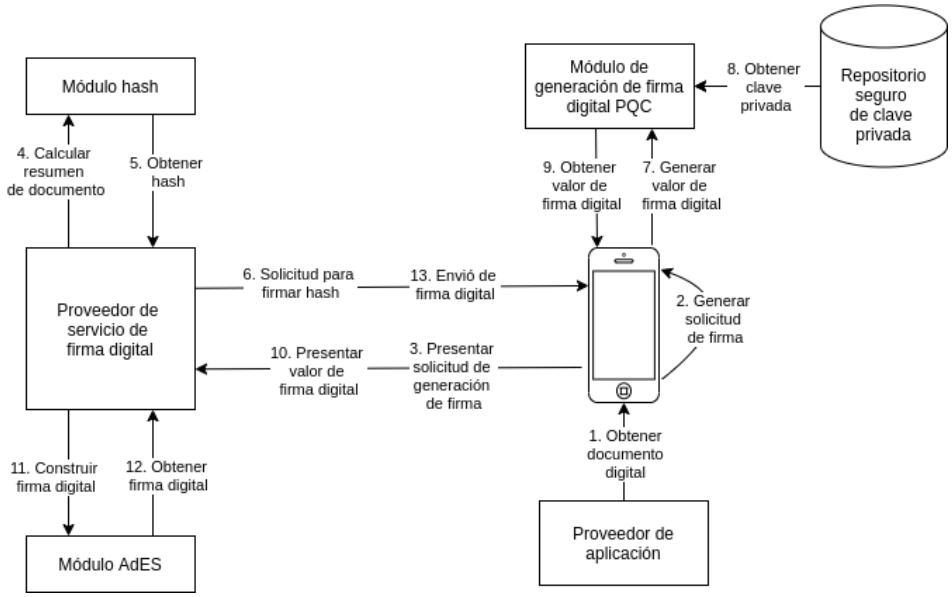

Figura 3: Arquitectura de un prototipo de firma digital en entornos de cómputo móvil y distribuido (generación de firma).

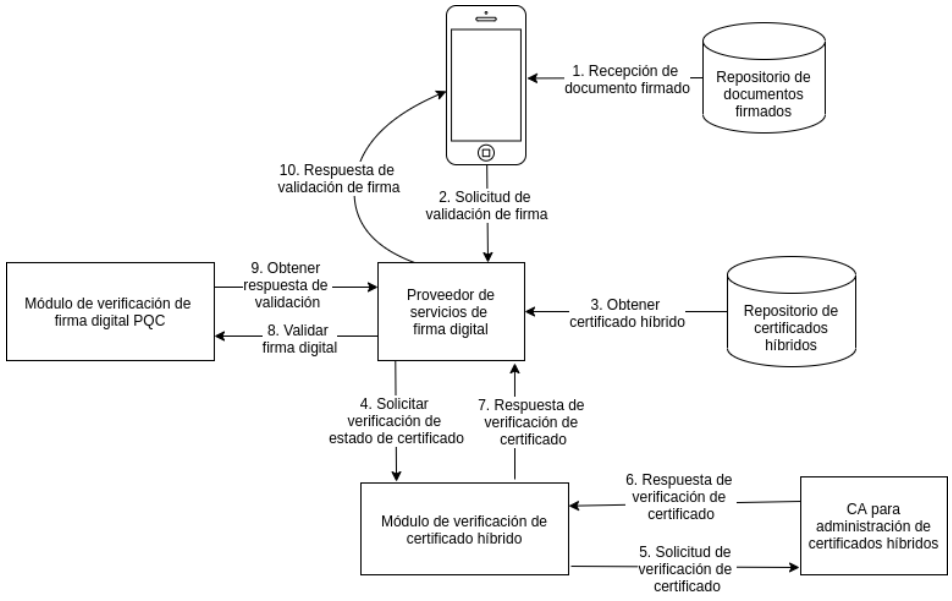

Figura 4: Arquitectura de un prototipo de firma digital en entornos de cómputo móvil y distribuido (verificación de firma).

como el desarrollo de módulos eficientes para firma digital postcuántica. Es en este último tema donde apunta la investigación y desarrollo sobre firmas digitales, ya que los esquemas actuales de firma digital, como RSA y ECDSA, están amenazados para ser vulnerados por una computadora cuántica.

Para hacer frente a la amenaza del cómputo cuántico, se está desarrollando a nivel mundial la línea de investigación sobre criptografía postcuántica [18], la cual permitirá contar con algoritmos de firma digital alternativos que sean resistentes a los ataques actuales con computadoras convencionales al igual que con computadoras cuánticas.

En el Cinvestav Tamaulipas se comenzó el desarrollo de soluciones PQC para el entorno del Internet de las Cosas, donde los dispositivos encargados de realizar las operaciones de firma y verificación están computacionalmente restringidos. Ejemplos de estos dispositivos son dispositivos móviles alimentados por baterías, como los teléfonos celulares de gama baja, los relojes inteligentes, sensores inalámbricos u otros dispositivos que tienen poca memoria y poder de cómputo comparados con computadoras de escritorio. El

bajo poder de cómputo en los dispositivos requiere que los procesos de generación y verificación de firma digital se descarguen en otros componentes, esto es, que el dispositivo no realice todas las tareas requeridas.

En la Fig. 3 se muestra el diagrama de un prototipo desarrollado en el Cinvestav Tamaulipas para firma digital postcuántica. Este prototipo contempla el uso de un dispositivo móvil que previamente ha generado su pareja de claves en el contexto de PQC, el cual interactúa con dos entidades:

1. Proveedor de aplicaciones. Sistema (por ejemplo en la nube) donde el dispositivo puede crear o recuperar documentos digitales.
2. Una vez obtenido el documento a firmar, el dispositivo solicita el servicio de un proveedor externo (proveedor de servicio de firma digital) para obtener el valor hash del documento. Una vez obtenido el valor hash, este se envía al dispositivo para que se realice la generación de la firma digital. Esto supone que el dispositivo debe contar con un módulo de generación de firma PQC y contar con un repositorio seguro de donde se pueda recuperar la clave privada para realizar la firma.
   Una vez obtenida la firma digital del documento, esta de envía nuevamente al proveedor del servicio de firma digital, que se encarga de crear el paquete de firma digital apegado a un estándar que garantice la interoperatibilidad de éste. En la Fig. 3 se hace referencia al estándar AdES (Advanced Electronic Signatures), un estándar promovido por la Unión Europea para el despliegue de firmas digitales en entornos de cómputo móvil y distribuido.

El módulo de generación de firma debe ser lo suficientemente eficiente para que el impacto en el dispositivo sea bajo, en términos de consumo de energía. De acuerdo a la Fig. 3, dicho módulo puede implementarse mediante alguno de los algoritmos PQC actualmente sugeridos para uso general.

El proceso de verificación de firmas digitales por el dispositivo móvil se realiza como se describe en la Fig. 4. En este caso, se considera el uso de certificados digitales híbridos, esto es, certificados digitales que combinan datos de criptografía convencional (RSA o ECDSA)al igual que PQC. Esto se hace de esta manera porque una solución PQC debe ser interoperable con la criptografía convencional. Un dispositivo podrá realizar firmas PQC, pero si alguna aplicación aún no lo soporta, podrá seguir realizando operaciones de generación o verificación con los procedimientos tradicionales. La creación, mantenimiento y gestión de certificados híbridos es también un área activa de investigación.

Arquitecturas como las mostradas en las figuras 3 y 4 estarán siendo implementadas y evaluadas, en donde se deberán explorar arquitecturas de hardware y/o software de cada uno de sus componentes, principalmente aquellos relacionados con PQC.

6. CONCLUSIONES

Las firmas digitales pueden traer grandes beneficios para el tratamiento de documentos que tradicionalmente se firman de manera autógrafa. Actualmente se cuenta tanto con el marco legal como con las herramientas tecnológicas que permiten su despliegue. Lo que hace falta es un mayor conocimiento de estas posibilidades y cultura para incentivar la digitalización de los procesos, que permitirán agilizar y reducir costos asociados al ciclo de vida de documentos que requieren firmado.

México presenta particularidades con el tratamiento de mensajes electrónicos (documentos digitales), donde la firma digital es un componente crucial para poder satisfacer dichos requerimientos. Una mejor formación de profesionales en materia de firmas digitales y la incentivación del uso de firmas digitales por parte de la sociedad puede detonar una transición más rápida a la automatización de procesos de manejo de documentos digitales oficiales.

AGRADECIMIENTOS

Una parte importante del trabajo de investigación sobre criptografía en el Cinvestav Tamaulipas, incluido el tema de firmas digitales, ha sido apoyado por el Fondo Sectorial de Investigación para la Educación, Ciencia Básica SEP-CONACyT, en el proyecto 281565 titulado *Desarrollo de nuevos algoritmos y arquitecturas de cómputo para criptografía ligera*. El Proyecto estuvo a cargo del Dr. Miguel Morales Sandoval.

REFERENCIAS

[1] La evolución de la firma autógrafa a la firma electrónica avanzada. *Revista Digital Universitaria*, 12(3):3–9, March 2011.
[2] F. Nouboud. Handwritten signature verification: A global approach. In S. Impedovo, editor, *Fundamentals in Handwriting Recognition*. Springer, Berlin, Heidelberg, 1994.
[3] David K. Black. The digital signature standard: Overview and current status. *Computers & Security*, 12(5):437 – 446, 1993. ISSN 0167-4048. doi: https://doi.org/10.1016/0167-4048(93)90062-A.
[4] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. 1997.
[5] Alok Gupta, Y Alex Tung, and James R Marsden. Digital signature: use and modification to achieve success in next generational e-business processes. *Information & Management*, 41(5):561–575, 2004.
[6] William J Caelli, Edward P Dawson, and Scott A Rea. Pki, elliptic curve cryptography, and digital signatures. *Computers & Security*, 18(1):47 – 66, 1999. ISSN 0167-4048. doi: https://doi.org/10.1016/S0167-4048(99)80008-X.
[7] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985. doi: 10.1109/TIT.1985.1057074.
[8] A. M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *Advances in Cryptology*, pages 224–314, Berlin, Heidelberg, 1985. Springer.
[9] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. doi: 10.1109/SFCS.1994.365700.
[10] Helena Handschuh. *SHA Family (Secure Hash Algorithm)*, pages 565–567. Springer US, Boston, MA, 2005. ISBN 978-0-387-23483-0. doi: 10.1007/0-387-23483-7_388.
[11] Saif Al-Kuwari, James H. Davenport, and Russell J. Bradford. Cryptographic hash functions: Recent design trends and security notions. Cryptology ePrint Archive, Report 2011/565, 2011. https://eprint.iacr.org/2011/565.
[12] R.L. Rivest, A. Shamir, and L.M. Adleman. A method for obtaining digital signature and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
[13] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, 1(1): 36–63, 2001.
[14] Banco de México. Infraestructura extendida de seguridad. pages 1–10.
[15] Héctor Alán de la Fuente. Prototipo de un sistema de firma digital como un servicio en la nube. Bachelor's thesis, Universidad Politécnica de Victoria, 2019.
[16] Brandon Samael García García. Diseño y construcción de una aplicación móvil de firma digital. Bachelor's thesis, Instituto Tecnológico Superior de El Mante, 12 2021.
[17] Miguel Morales-Sandoval, Jose Luis Gonzalez Compean, Arturo Diaz Perez, and Victor Jesus Sosa Sosa. A pairing-based cryptographic approach for data security in the cloud. *International Journal of Information Security*, 17(4):441–461, 2018. ISSN 1615-5262. doi: 10.1007/s10207-017-0375-z.
[18] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. *Post Quantum Cryptography*. Springer Publishing Company, Incorporated, 1st edition, 2008.