Hamut'ay
Revista semestral de divulgación científica
Coordinación de Investigación y Extensión Científica Tecnológica (CIECT-DUED).
Dirección Universitaria de Educación a Distancia-UNIVERSIDAD ALAS PERUANAS
http://revistas.uap.edu.pe/ojs/index.php/HAMUT/index
ISSN: 2313-7878 DOI: 10.21503/hamu.v5i2.1622 Vol. 5(2). Julio-diciembre Hamut'ay 2018. Lima-Perú

Análisis de la firma digital con base en la infraestructura de clave pública

Analysis of digital signature based on public key infrastructure

Fresia Yanina Holguín García[1]
https://orcid.org/0000-0002-2589-7067
Universidad Espíritu Santo, Ecuador

Recibido: 01-07-2018
Aceptado: 19-11-2018

Cita recomendada

Holguín, F. (2018) Análisis de la firma digital con base en la infraestructura de clave pública. Hamut´ay, 5 (2), 94-104.
http://dx.doi.org/10.21503/hamu.v5i2.1622

Resumen

El análisis descriptivo del funcionamiento de la arquitectura de firma digital con base en infraestructura de clave pública determinó el objetivo central de toda la investigación, por ello se expusieron las responsabilidades, que cada Autoridad de Certificación ejerce en su proceso de creación y verificación, para garantizar la autenticidad, integridad y no repudio de la información transmitida. La metodología utilizada es la documental a través de la revisión bibliográfica de los principales conceptos de firma digital, criptografía y PKI obtenida de repositorios, bibliotecas digitales, base de datos de libre acceso y Google Académico.

A partir del estudio realizado se puede concluir que la firma digital con base en la infraestructura de clave pública es un proceso transparente que genera fiabilidad tanto al emisor como al receptor de que las claves generadas corresponden a sus legítimos propietarios, pero es necesario que esté amparada por un marco legislativo adecuado, se emplee un hardware y software sofisticado.

Palabras Clave: PKI, firma digital, criptografía, clave pública.

Abstract

The descriptive analysis of the functioning of the digital signature architecture based on public key infrastructure determined the central objective of all the investigation, for this reason the responsibilities that each Certification Authority exercises in its creation and verification process were explained, to guarantee the authenticity, integrity and non-repudiation of the transmitted information. The methodology used is documentary through the bibliographic review of the main concepts of digital signature, cryptography and PKI obtained from repositories, digital libraries, free access da-

1 Ingeniera en Sistemas, Magister en Auditoría de Tecnologías de la Información. Universidad Espíritu Santo – Ecuador. E-mail fholguin@uees.edu.ec.

tabase and Google Academic.

From the study carried out it can be concluded that the digital signature based on the public key infrastructure is a transparent process that generates reliability both to the sender and the receiver that the keys generated correspond to their legitimate owners, but it is necessary that it is protected by an adequate legislative framework, sophisticated hardware and software is used, and each user is aware of the responsibilities acquired when implementing it.

Keywords: PKI, digital signature, cryptography, public key.

Introducción

Las redes de comunicaciones han evolucionado vertiginosamente permitiendo una conectividad en la transmisión de imágenes, voz y datos que trascienden fronteras; por ello cada día distintos modelos de negocios incorporan las plataformas digitales como mecanismo principal de sus actividades financieras, lo que ha originado un mayor intercambio de información y la sensibilización del grado de seguridad de los datos y mensajes transferidos, los cuales están propensos a amenazas de intercepción y análisis de tráfico, suplantación de identidad, reactuación, modificación de un mensaje, degradación fraudulenta de servicio, entre otras (Martín, 2015).

Teniendo en cuenta estos aspectos, las empresas y academias relacionadas con la tecnología de la información y comunicación (TIC) han implementado metodologías que puedan garantizar que la seguridad de la información sea robusta en cuatro principios: i. Confidencialidad, la información queda oculta a terceros no autorizados; ii. Integridad, los datos son genuinos y no han sido modificados desde su creación; iii. Disponibilidad, la información es accesible en cualquier momento que sea requerida; y iv. No repudio, para demostrar que un mensaje procede de su remitente y evitar que el receptor niegue haber recibido el mensaje (Sánchez & González, 2016). Urbina (2016) señala que una de las metodologías que ha proporcionado mayor eficiencia en el resguardo de los datos es la criptografía que a través de las técnicas de cifrado satisface estos pilares.

Según Joshi & Karkade (2015) los procesos de encriptación y descifrado tienen características particulares de acuerdo a su naturaleza, siendo la criptografía asimétrica una de las más fiables especialmente por la incorporación de algoritmos de firma digital (vigentes y no colisionados hasta la fecha) que avalan la identidad del firmante y la integridad de un mensaje. Sin embargo, Espinoza (2018) manifiesta que ante la posibilidad de que un emisor o receptor desconozca la autenticidad de un documento firmado digitalmente se incorporó la infraestructura de clave pública (PKI) como un mecanismo que implementa Autoridades de Certificación para legitimar la correspondencia de las claves a sus auténticos propietarios, acreditar la procedencia de un mensaje, custodiar que se cumplan lineamientos y políticas en su formato, entre otros aspectos.

Considerando que la firma digital basada en infraestructura de clave pública posee operaciones criptográficas que generan mayor robustez que una firma generada por métodos tradicionales, que actualmente es utilizada en aplicaciones bancarias, comerciales y de gobierno electrónico; y que sus principios fundamentales son muy similares a los de una firma manuscrita (solo su propietario puede crearla, puede ser verificada por su emisor y receptor, no puede ser repudiada por su remitente) (Loján, 2016); es necesario conocer como dicha arquitectura en tiempo real avala la legitimidad de un mensaje enviado.

Es en ese sentido que se tiene como objetivo realizar una descripción de la arquitectura y funcionalidades que las Autoridades de Certificación ejercen en el proceso de creación y verificación

de una firma digital con base en la infraestructura de clave pública y así conocer su fiabilidad en la identificación y autenticación del firmante, e integridad de los datos transmitidos.

Métodos

Este artículo es una investigación de revisión documental, en la cual se analiza en diversas bases de datos, repositorios y fuentes bibliográficas sobre la infraestructura de clave pública y su aplicación en la firma digital con la finalidad de sustentar, que este tipo de firma ofrece mayor fiabilidad y robustez que otros sistemas de identidad electrónica, al estar creada por mecanismos criptográficos asimétricos y respaldada por autoridades de certificación.

Para la selección del material bibliográfico, en que se apoya el marco teórico, se incluyeron: libros impresos y virtuales, obtenidos de Google Books; artículos de revistas indexadas expuestas en Google Académico, repositorios, bibliotecas digitales y base de datos de libre acceso (SciElo, Wos, Dialnet, Redalyc). Además, se emplearon como descriptores: criptografía, PKI, autoridades de confianza de la infraestructura de clave pública y firma digital.

Dentro de los criterios de inclusión se definió que los artículos, libros y documentos analizados correspondan a los últimos cinco años de la temática; teniendo como resultado mayores publicaciones de revistas.

Por otra parte, la literatura presentada se analizó cualitativamente, lo que permitió una distribución de este documento en apartados que abarcan una estructura secuencial de forma lógica en relación a la infraestructura de clave pública. Cabe señalar, que el presente documento utiliza citas indirectas por lo que se presentan sin comillas e incluyen la respectiva referencia bibliográfica.

Firma Digital

En al año 1976 los investigadores norteamericanos Whitfield Diffie y Martin Hellman expusieron la teoría de la estructura de una firma digital, dando la pauta para que un año después Ronald Rivest, Adi Shamir y Len Adleman desarrollaran el algoritmo RSA (Saravanan & Kumar, 2015). Dicho algoritmo permitió crear las primeras firmas digitales cuyos principios obedecían a los mismos de la firma autógrafa, sin embargo, prevalecía la inseguridad, por lo que fue necesario adicionar una función criptográfica hash al mensaje original (Thangavel, 2014). En 1984 Shafi Goldwasser, Silvio Micali y Ronald Rivest propusieron los primeros lineamientos de seguridad en una firma digital; y paralelamente se crearon otros esquemas criptográficos como: Lamport, Merkle y Rabin; los cuales no adquirieron mayor relevancia (Thangavel, 2014). Más tarde (1988), nace el primer software con fines comerciales para firmas digitales denominado Lotus Notes 1.0, el mismo estaba basado en RSA (Thangavel, 2014). Tres años después, el Instituto Nacional de Normas y Tecnología de los Estados Unidos desarrolla el algoritmo DSA orientado para el Estándar de Firma Digital (DSS) cuya desventaja frente a RSA era el mayor tiempo de procesamiento de cómputo (Navarjun, 2017). Posteriormente (1999), el formato PDF adquiere la capacidad de incrustar firmas digitales a los documentos, sin embargo, fue en el año 2008 cuando la Organización Internacional de Normalización (ISO) convierte este formato en un estándar abierto que incluye firmas digitales como parte integral de su esquema dando origen a que la implementación de las firmas digitales tenga mayor anuencia en el mundo (Navarjun, 2017).

Rocha, Castello & Bollo (2014) señalan que la firma digital es un método criptográfico que permite corroborar la fuente original de un mensaje para posteriormente verificar que no haya sido alterado. Por su parte, Gaona, Montenegro & Wiesner (2014) establecen que una firma digital es el resultado de cifrar un mensaje mediante funciones hash unidireccionales que garantizan que el único que pueda descifrarlo sea el destinatario con su correspondiente clave privada. De la misma manera, Loján (2016) define la firma digital como una variante de la firma electrónica que se construye en base a la criptografía asimétrica permitiendo asociar la identidad del firmante con un documento digital.

Por consecuencia un firma digital implica un pro-

ceso de encriptación (Gallo, 2015), y por ello, es preciso distinguir el término criptografía que, según Zhou, Gong, Fu, & Jin (2016) es una disciplina que estudia las técnicas para transformar un texto claro en texto cifrado utilizando claves criptográficas (parámetro que permite cifrar o descifrar datos) y que además, posibilita la prevención de fallas de seguridad en un sistema computarizado garantizando la confidencialidad, integridad, autenticidad, y no repudio de la información (Wadhwa, Hussain & Rizvi, 2013). Medina & Miranda (2015) señalan que la criptografía se clasifica en: simétrica, que utiliza la misma clave para encriptar y desencriptar los datos; y asimétrica, que emplea un par de claves (una se publica y la otra se almacena de forma segura); pero Boneh & Shoup (2017) evidencian que existe la criptografía híbrida, la misma que combina la seguridad de una clave pública con la eficiencia de un algoritmo de clave simétrica. En este contexto, Joshi & Karkade (2015) manifiestan que la criptografía asimétrica es mayormente utilizada en la creación de una firma digital debido a que su metodología ofrece mayor robustez.

Al respecto, una firma digital construida con criptografía asimétrica utiliza dos claves distintas con una relación matemática entre sí: la clave pública es la responsable de la codificación y la clave privada permite el descifrado (Malhotra, 2015). De la misma manera, Joshi & Karkade (2015) manifiestan que al crear una firma digital con criptografía asimétrica se implementan algoritmos que generan un par de claves complementarias, las cuales realizan los procesos de cifrado y descifrado de un mensaje. Además, Pramendra & Vijay (2014) señalan que la clave pública está disponible libremente, mientras que la clave privada es únicamente conocida por el usuario propietario. En la Figura 1 se muestra un esquema de este proceso.

Peña (2015) indica que en un contexto ideal una firma digital posee las mismas propiedades de una firma manuscrita, porque es auténtica, infalsificable, inalterable, no reutilizable y no puede ser repudiada; por ello es importante que la tecnología que la genera proporcione un esquema seguro para cumplir estos atributos de lo contrario podría ser alterada/ corrompida. Según Rocha, Castello & Bollo (2014) una firma digital puede ser construida con diversas técnicas, pero el estándar de infraestructura de clave pública proporciona mayor robustez debido a que el titular tiene el control exclusivo de la firma, el proceso de verificación lo realiza cualquier entidad que conozca la clave pública del firmante, la identidad de un remitente es reconocida por las Autoridades de Certificación.

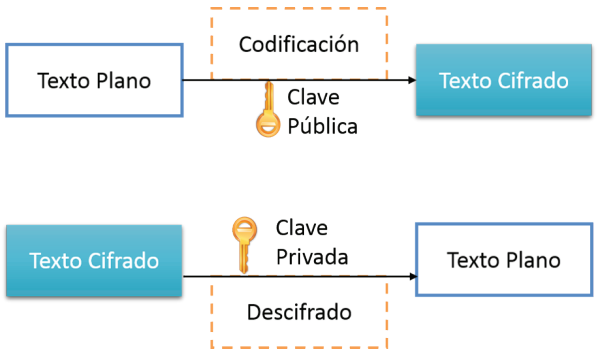

Figura 1: Proceso de Codificación y Descifrado en Criptografía Asimétrica
Fuente: Medina & Miranda (2015, p.16)

Infraestructura de clave pública (PKI)

Con el nacimiento de la criptografía asimétrica surgió el problema de la gestión de claves, el mismo que se mitigó con la creación de un directorio denominado Archivo Público que contenía nombre, número y clave pública del destinario (Albarqi, Alzaid, Ghamdi, Asiri & Kar, 2015). Cuando el remitente deseaba enviar un mensaje debía buscar al destinario por su nombre para encontrar la clave pública, lo cual no ofrecía las garantías necesarias para demostrar que esta clave pertenecía al destinario deseado (Afshar, 2015). Este contexto propició a que la Unión Internacional de Telecomunicaciones (UIT) construyera en el año 1980 un directorio que pudiera almacenar las claves de todas las personas y dispositivos del mundo, lo que dio origen al estándar X.500 que definía por completo las características de ese directorio (Albarqi et al., 2015). Pero ante la necesidad de garantizar Autenticación nació el modelo X.509 que precisaba el formato de los certificados digitales e incorporaba a un tercero de confianza para verificar la correspondencia de un titular a

una clave pública, siendo este el momento en que surge el concepto de PKI (Afshar, 2015).

Abobeah, Ezz & Harb (2015) definen la infraestructura de clave pública como una combinación de software, hardware, políticas y personas que tienen como objetivos administrar (crear, emitir, modificar, almacenar y eliminar) certificados digitales, autenticar la identidad del remitente y el receptor, y proporcionar la integridad de los datos. Por su parte, Cantero, Barán & Stuardo (2014) indican que es un modelo de arquitectura que permite manipular las llaves públicas y garantizar la correspondencia a sus legítimos propietarios. Según Ramos (2015) una PKI es un conjunto de tecnologías, procedimientos y políticas de seguridad para crear, emitir y gestionar certificados digitales cimentados en criptografía de llave pública.

Por consecuencia, la infraestructura de clave pública se utiliza para instaurar una autenticación robusta en los servicios y protocolos de seguridad basados en la criptografía asimétrica como es el IPSec, SSL/TLS; permitiendo asociar una entidad con su par de llaves generadas, realizar el cifrado y descifrado de un mensaje, y garantizar el no repudio de un envío (Sumalatha & Sathyanarayana, 2015).

Cantero, Barán & Stuardo (2014) aseveran que el objetivo de una PKI es crear un documento que permita verificar la autenticidad de una clave pública, el cual se denomina Certificado Digital. Ramos (2015) define un certificado digital como una estructura de datos que relaciona una clave pública a una entidad, el cual ha sido reconocido por una Autoridad de Certificación, tiene un periodo de validez especifico e incluye la firma digital de dicha Autoridad para validar su legitimidad. Angulo & Henao (2017) establecen que un certificado digital utiliza generalmente el estándar X.509 para definir la estructura y los campos correspondientes, y actualmente dicho estándar se encuentra en su versión 3. En la Figura 2 se detalla el formato del estándar X.509 v3.

Gutiérrez (2014) señala que al ejecutarse una operación criptográfica que use PKI intervienen como mínimo tres elementos: i. Usuario, que inicia el proceso; ii. Autoridades, que otorgan validez a los certificados; iii. Destinatario, quien recibe

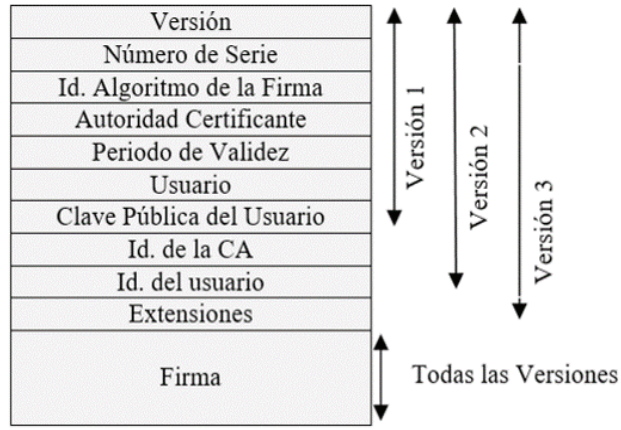

Figura 2: Formato de Certificado X.509 versión 3
Fuente: Hawanna, Kulkarni, Rane, Mestri, & Panchal (2016, p. 2)

los datos cifrados. Además, Albarqi et al. (2015) establecen que los componentes primordiales de una PKI son: i. Autoridad de Registro (RA), ii. Autoridad de Certificación (CA), iii. Políticas de Seguridad, iv. Aplicaciones habilitadas para PKI, v. Sistemas de Distribución y vi. Repositorio de Certificados.

Según WebTrust (2017) la Autoridad de Registro (RA) tiene como función autenticar la identidad del usuario o dispositivo que requiere un certificado digital pero no puede emitir ni firmar un certificado. De la misma manera, Ormaza, Barrios & Fernández (2017) aseveran que una RA reconoce de forma inequívoca al solicitante de un certificado y realiza los procesos de registro para su emisión.

WebTrust (2017) evidencia que la Autoridad de Certificación (CA) es un tercero de confianza que garantiza la relación existente entre la clave pública y los datos del usuario inscritos dentro de un certificado digital. Por su parte, Cutanda (2013) manifiesta que cuando la CA emite un certificado lo genera en el formato X.509 v3 agregando su firma digital lo que permite que un tercero pueda verificar su autenticidad usando la clave pública de la CA. Así mismo, las funciones de la Autoridad Certificadora son: emitir certificados, mantener y generar Listas de Revocación de Certificados (CRL) y conservar la información respecto a las fechas de vencimiento de los certificados (Afshar, 2015).

Nelson & Nordenberg (2016) determinan que

las Políticas de Seguridad son procedimientos operativos que rigen las operaciones de la PKI y que tienen validez técnica y legal, por ejemplo: criterios que aseguren que el método para validar la identidad del titular del certificado es confiable, reglas para establecer quién puede revocar los certificados, medidas de cómo deben distribuirse las listas de revocaciones, pautas que determinen frecuencia para archivar los certificados, entre otros.

Albarqi et al. (2015) detallan que las Aplicaciones Habilitadas para PKI son programas/software aptos para manejar certificados digitales, así, por ejemplo: navegadores web, clientes de correo electrónico, sistemas operativos, entre otros.

Nelson & Nordenberg (2016) establecen que un Sistema de Distribución tiene como función automatizar la gestión de los certificados digitales.

Según MICITT (2018) un Repositorio de Certificados almacena los certificados válidos para que las entidades/aplicaciones que lo requieran puedan descargarlos. Estos repositorios utilizan directorios como el X.500 los cuales son accesibles mediante protocolos abiertos que permiten consultar la información guardada centralmente a través de la red, siendo el más utilizado el LDAP (Light Weight Directory Access Protocol) (Abobeah, Ezz & Harb, 2015).

Nelson & Nordenberg (2016) manifiestan que los elementos de la PKI anteriormente descritos dan lugar a un proceso interrelacionado por fases, el mismo que inicia cuando el Solicitante se apersona ante la Autoridad de Registro (encargado de realizar la captura de información de registro y generación de claves), y dicha entidad se comunica con Autoridad de Certificación para transmitir los datos del solicitante. Finalizado el registro, el solicitante puede acceder a la Autoridad de Certificación para obtener el certificado digital firmado por esta entidad, pero la custodia de la clave privada será responsabilidad del Receptor durante el tiempo de validez del certificado. Es necesario señalar que el proceso de generación de claves asimétricas puede ser realizado por el Solicitante (empleando un software criptográfico) o la Autoridad de Certificación (Gallo, 2015). La Figura 3 muestra el funcionamiento de la arquitectura de una PKI.

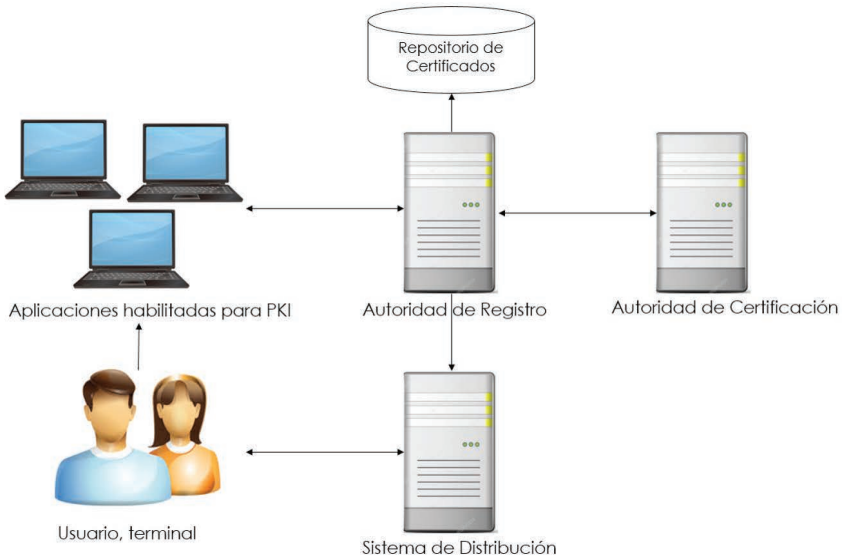

Figura 3: Arquitectura de una PKI
Fuente: Albarqi et al. (2015, p. 33)

Por otra parte, Cuno (2015) evidencia que ante la posibilidad de que un usuario requiera comprobar la legitimidad de un certificado digital puede recurrir a una Autoridad de Validación (VA), la cual determinará la validez del documento en base a las CRL u OCSP (protocolo que permite solicitar el estado de un certificado a un servidor). Además, de ser necesario, la VA incluye un sello de tiempo emitido por la Autoridad de Sellado a Tiempo, que reconoce inequívocamente la veracidad del certificado aun si ha expirado (Sánchez, 2016).

Firma Digital con Base en la Infraestructura de Clave Pública

Peña (2015) define la firma digital con base en la infraestructura de clave pública como un procedimiento que utilizando técnicas criptográficas requiere la participación de un tercero de confianza para acreditar la identidad del emisor. En este sentido, Ramos (2015) señala que la firma digital basada en PKI desempeña un papel trascendental

e insustituible en la seguridad de las transacciones electrónicas, autenticación de identidad, integridad digital y el no repudio; por ello son utilizadas en la distribución de software, transacciones financieras y en entornos en los cuales es importante detectar la falsificación y manipulación de datos.

Gaona, Montenegro & Wiesner (2014) manifiestan que para construir una firma digital con base en infraestructura de clave pública se requiere una función hash (SHA-2, SHA-3, RIPEMD-160) que transforma un texto de longitud variable en un bloque de longitud fija en forma de resumen que es irreversible (no se puede recuperar un texto a partir de su resumen); y un algoritmo asimétrico (RSA, DSS, ECDSA) que genera dos claves, siendo la clave privada que permite firmar y la clave pública autenticar la firma.

Rocha, Castello & Bollo (2014) indican que cuando se realiza el proceso de firmar, primero el emisor crea un mensaje, luego le aplica la función hash y posteriormente lo cifra con su clave privada. Cada mensaje firmado por el emisor deberá ser revisado por una Autoridad de Certificación que validará su origen y contenido, y únicamente si es correcto será enviado al receptor adjuntado el Certificado Digital. Finalmente, el destinatario recibe el mensaje con dos elementos: el mensaje (sin cifrar o cifrado con la clave pública del receptor) y la firma digital (conformada por el hash con la clave privada del emisor y el certificado digital cifrado con la clave privada de la Autoridad de Certificación).

Según Gallo (2015) para corroborar la validez de una firma digital el Receptor deberá descifrar el certificado digital del emisor utilizando la clave pública expedida por la Autoridad de Certificación (se accede a la llave a través de la página web de la CA). Luego de descifrar el certificado, el Receptor podrá conocer la Clave Pública del emisor, la cual le permitirá descifrar el hash recibido; y si el mensaje fue codificado podrá descifrarlo con su clave privada. Finalmente, el Receptor compara el hash recibido del emisor con su hash obtenido, si ambos son iguales se considera que el mensaje es auténtico, que la firma digital corresponde al emisor y que el mensaje ha sido descifrado con una clave pública y cifrado con una clave privada. En la Figura 4 se detalla el Proceso Firmar y Verificar una firma digital basada en PKI y en la Figura 5 su marco referencial.

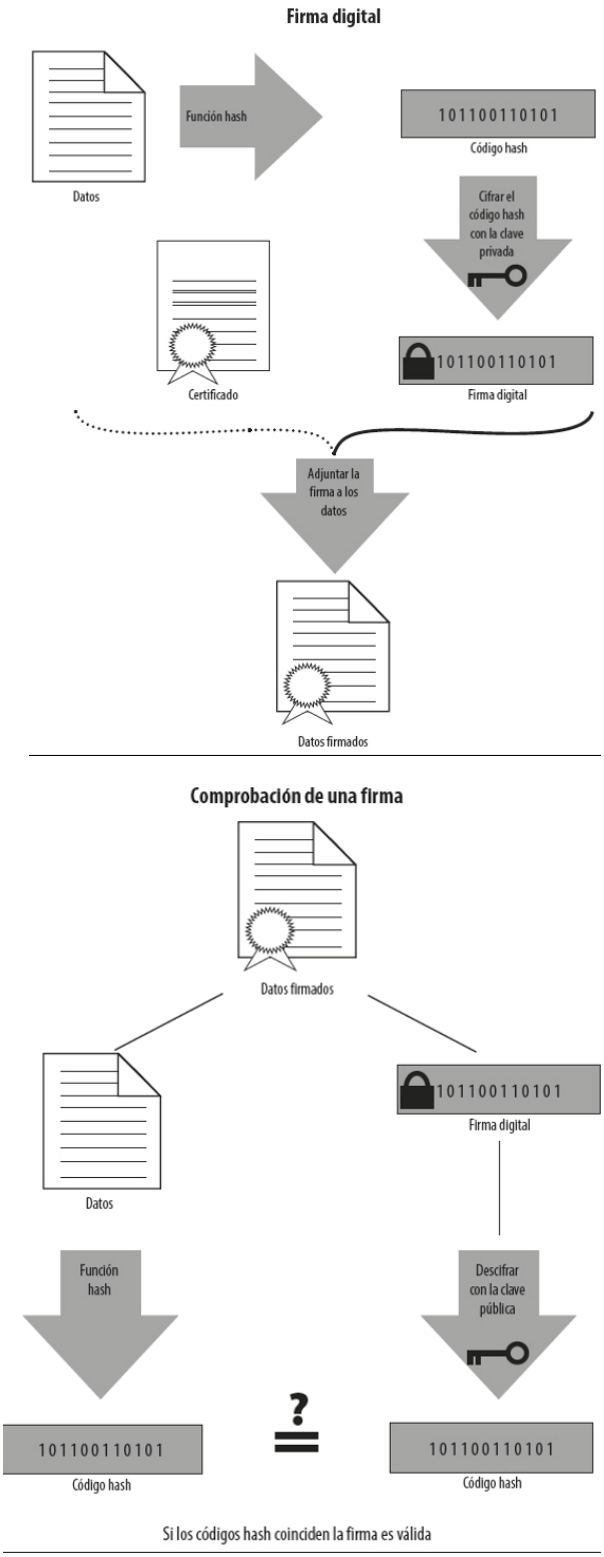

Figura 4: Proceso de Firmar y Verificar en una Firma Digital basada en PKI
Fuente: Ramos (2015, p. 3)

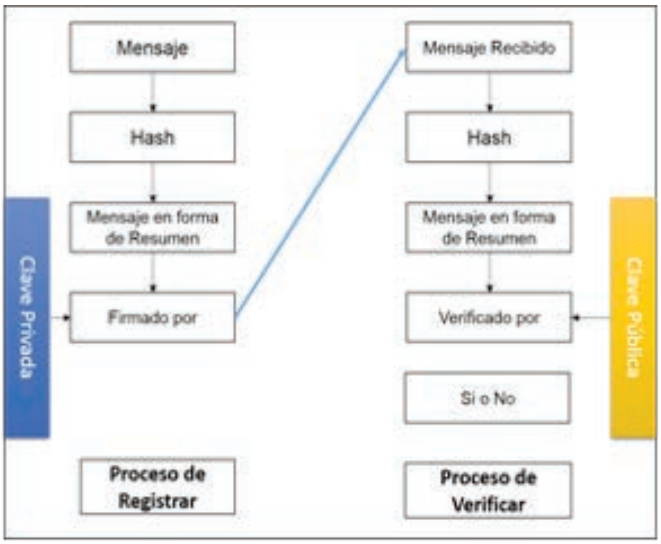

Figura 5: Marco referencial para Registrar y Verificar en una Firma Digital basada en PKI
Fuente: Ramos (2015, p. 4)

Cuno (2015) señala que el proceso de generar y verificar una firma digital basada en PKI se cimienta en dos entes: i. Autoridad de Certificación, que proporciona confianza tanto al emisor como al receptor que la distribución de las claves es segura; y ii. Lista de Revocación de Certificados, la cual debe estar permanentemente actualizada por la autoridad de certificación correspondiente; pero es necesario que la infraestructura de clave pública esté respaldada por un marco legal adecuado, cada Autoridad que la conforma esté provista de un sistema informático seguro, y que el firmante confíe en la transparencia de este proceso.

Por otra parte, Schaettgen, Levy, Schelnast & Socol (2014) distinguen dos tipos de firmas digitales, que se diferencian por la seguridad en la que se basa la autenticación, y son: i. Firma digital reconocida (FER), creada con un dispositivo exclusivo, es decir, distinto al que se utilizó para firmar el documento (lo que le otorga más seguridad); y ii. Firma Digital Avanzada (AES), desarrollada con el mismo dispositivo con que se firma el documento, por lo tanto, es menos robusta que la FER. En este contexto, Saavedra & Astolfi (2015) señalan que los dispositivos criptográficos que se implementan para la creación de firmas digitales se rigen a estándares como: FIPS 140-2 Nivel 3 o Common Criteria ISO 15408 EAL 4 +; y uno de los dispositivos más empleados es el HSM (Hardware Security Module), el cual genera, almacena y protege las claves criptográficas; por ello aporta mayor seguridad y rendimiento en las operaciones de criptografía.

En otro ámbito, Vigil, Buchmanna, Cabarcasb, Weinerta & Wiesmaierc (2015) manifiestan que los documentos firmados digitalmente se conservan por algunos años pero si se requiere preservarlos por décadas o por periodos mayores de tiempo se pueden presentar problemas tecnológicos como: obsolescencia criptográfica, los algoritmos pueden ser corrompidos en este intervalo; pérdida de integridad, fallas en los dispositivos físicos debido a la migración de nuevos formatos; obsolescencia de software, cambios evolutivos que satisfacen los requerimientos de la época; obsolescencia de hardware, deterioro físico o evolución tecnológica.

Finalmente, es preciso acotar que la tecnología de la firma digital basada en PKI además de ser utilizada en la identificación y autenticación de una entidad, también puede implementarse en el comercio electrónico, para salvaguardar un trámite; en la red, para identificar la autenticidad de un sitio web; en un software, para prevenir su manipulación, entre otros (Saavedra & Astolfi, 2015).

Conclusiones

El desarrollo de las redes de comunicaciones y la tendencia global de implementar principalmente actividades comerciales en línea ha despertado un mayor interés en salvaguardar los datos e información transmitida de amenazas y vulnerabilidades que destruyen la confiabilidad de todo proceso web, por ello las técnicas de cifrado se han constituido en un pilar fundamental que robustece los principios de la seguridad informática (Urbina, 2016).

La criptografía asimétrica permitió el desarrollo de la firma digital como un mecanismo para respaldar que la información intercambiada no haya sido alterada, por ello está siendo implementada con mayor anuencia en las transacciones electrónicas en donde una firma tradicional es impotente (Joshi & Karkade, 2015).

Coincidentemente con lo mencionado por Rocha, Castello & Bollo (2014) la infraestructura de clave pública constituye una arquitectura rigurosa, en la que cada elemento (Autoridad) tiene funciones definidas que avalan la transparencia del proceso de generación y entrega de claves e identifican inequívocamente una entidad, por ello es el estándar más empleado para crear firmas digitales seguras; sin embargo, barreras como: el costo de implementación, pocos especialistas en el país e interoperabilidad han limitado su uso extendido.

Una firma digital basada en infraestructura de clave pública es una tecnología que garantiza a través de algoritmos asimétricos, función hash y certificados digitales la autenticación, integridad y no repudio de un mensaje; y en este sentido Espinoza (2018) destaca que para su correcto establecimiento debe estar amparada por un marco legislativo adecuado, emplear un hardware y software sofisticado, y cada usuario debe ser consciente de las responsabilidades (no puede desconocer la autenticidad de un documento firmado digitalmente) que adquiere al implementarla.

Es importante evidenciar que la validez de una firma digital no es imperecedera, deben cumplirse distintos requisitos (surgen conforme a la evolución tecnológica) que garanticen su vigencia tanto a largo como a corto plazo. Además, su alcance puede ser global o limitado a un territorio específico (Vigil et al., 2015).

Es necesario incrementar esfuerzos para que el funcionamiento de la firma digital basada en PKI sea un instrumento de dominio público, de esta manera se fomenta la confianza en las actividades económicas, administrativas y gubernamentales que cada día incorporan esta tecnología en sus procesos (Loján, 2016).

Por otro lado, se concuerda con Saavedra & Astolfi (2015) que distinguen que la seguridad de un entorno es el resultado de la combinación de diferentes procesos y tecnologías, por consecuencia una firma digital basada en PKI no es la solución a todos los posibles problemas de seguridad existentes en una organización.

Aquí hemos expuesto únicamente el funcionamiento, arquitectura y ventajas que ofrece la firma digital con base en la infraestructura de clave pública para la autenticación de un remitente e integridad de un mensaje basándose en el análisis exploratorio de trabajos anteriores; por ello, en un futuro continuando con esta línea investigativa se podría explorar cuales son los formatos, empaquetamientos y niveles que garantizan mayor interoperabilidad y efectividad, exponer las normas vigentes en el Ecuador que amparan su validez legal y definir un modelo de implementación de firmas digitales (proyecto cero papeles) para pequeñas y medianas empresas que aún no han migrado a esta tecnología.

Además, en un siguiente momento, se podría comparar las características de rendimiento de los algoritmos de firma digital tradicionales como RSA en contraposición a los de curva elíptica en base a que estos últimos utilizan claves mucho más pequeñas y proporcionan un nivel de seguridad equivalente.

Referencias bibliográficas

Abobeah, R., Ezz, M. & Harb, H. (2015). Public-Key Cryptography Techniques Evaluation. International Journal of Computer Networks and Applications, 2(2), 2-15. Recuperado de https://www.researchgate.net/publication/281373468_Public-Key_Cryptography_Techniques_Evaluation

Afshar, R. (2015). Digital Certificates. Recuperado de http://cs.indstate.edu/~rafshar/documents/paper2.pdf

Albarqi, A., Alzaid, E., Ghamdi, F., Asiri, S. & Kar, J. (2015). Public Key Infrastructure: A Survey. Journal of Information Security, 6(1), 31-37. https://doi.org/10.4236/jis.2015.61004

Angulo, D. & Henao, J. (2017). Análisis de herramientas de interceptación para el control de ataques reales de suplantación con certificados SSL. Redes de Ingeniería, 20(20), 1-19. Recuperado de http://repository.udistrital.edu.co/bitstream/11349/7812/1/AnguloCastroDianaCarolina2018.pdf

Boneh, D. & Shoup, V. (2017). A Graduate Course in Applied Cryptography. Recuperado de https://crypto.stanford.edu/~dabo/cryptobook/BonehShoup_0_4.pdf

Cantero, S., Barán, B. & Stuardo, F. (2014). Infraestructura de clave pública en una Universidad del Paraguay. COMTEL, 92-99. Recuperado de http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/692/COMTEL-2014-Paper9.pdf?sequence=1&isAllowed=y

Cuno, A. (2015). Conceptos de Firma Digital. En RENIEC (Ed.), Identidad digital. La identificación desde los registros parroquiales al DNI electrónico (pp. 107-122). Lima, Perú: Escuela Registral.

Cutanda, D. (2013). Fundamentos sobre Certificados Digitales. Recuperado de https://www.securityartwork.es/2013/06/12/fundamentos-sobre-certificados-digitales-iii-cadena-de-confianza/

Espinoza, J. (2018). Entre la firma electrónica y la firma digital: aproximaciones sobre su regulación en el Perú. Revista IUS, 12(41), 241-266. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100241&lng=es&tlng=en.

Gallo, A. (2015). Modelos de Confianza. En RENIEC (Ed.), Identidad digital. La identificación desde los registros parroquiales al DNI electrónico (pp. 107-122). Lima, Perú: Escuela Registral.

Gaona, P., Montenegro, C., & Wiesner, H. (2014). Hacia una propuesta de mecanismos para la autenticidad de objetos de aprendizaje en plataformas Learning Content Management Systems. Ingeniería, 19(1), 50-64. Recuperado de http://revistas.udistrital.edu.co/ojs/index.php/reving/article/view/5065

Gutiérrez, C. (2014). PKI, el paradigma de la criptografía asimétrica. Recuperado de https://www.welivesecurity.com/la-es/2014/06/24/pki-paradigma-criptografia-asimetrica/

Hawanna, V., Kulkarni, V., Rane, R., Mestri, P. & Panchal, S. (2016). Risk Rating System of X.509 Certificates. Procedia Computer Science, 89(1), 152-161. Recuperado de https://www.sciencedirect.com/science/article/pii/S1877050916310924

Joshi, M. & Karkade, R. (2015). Network Security with Cryptography. International Journal of Computer Science and Mobile Computing, 4(1), 201-204. Recuperado de https://www.ijcsmc.com/docs/papers/January2015/V4I1201544.pdf

Loján, E. (2016). Análisis Bibliométrico de la definición de la firma digital en las leyes del comercio electrónico. Gaceta Sansana, 1(7), 1-19. Recuperado de http://publicaciones.usm.edu.ec/index.php/GS/article/view/73

Malhotra, R. (2015). A hybrid geometric cryptography approach to enhance information security. J. Netw. Commun. Emerg. Technol, 3(1), 16-18. Recuperado de http://www.jncet.org/Manuscripts/Volume-3/Issue-1/Vol-3-issue-1-M-04.pdf

Martín, P. (2015). Inseguridad Cibernética en América Latina: Líneas de Reflexión para la Evaluación de Riesgos. Instituto Español de Estudios Estratégicos, 1-17. Recuperado de http://www.ieee.es/en/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf

Medina, Y. & Miranda, H. (2015). Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES. Mundo FESC, 1(9), 14-21. Recuperado de https://dialnet.unirioja.es/descarga/articulo/5286657.pdf

MICITT. (2018). Política de Certificados para la Jerarquía Nacional de Certificadores Registrados. Recuperado de http://www.mifirmadigital.go.cr/wp-content/uploads/2018/03/DCFD-Pol%C3%ADtica-de-certificados-v1.2.pdf

Navarjun, K. (2017). Digital and Electronic Signatures-Keys to the Globalized World. The World Journal on Juristic Polity, 3(1), 1-9. Recuperado de http://jurip.org/wp-content/uploads/2017/03/Nagarjun-K.B..pdf

Nelson, M. & Nordenberg, D. (2016). Public Key Infrastructure: A Trusted Security Solution for Connected Medical Devices. Recuperado de https://www.digicert.com/healthcare-iot/Whitepaper_PKI_ATrustedSecuritySolutionForConnectedMedicalDevices(1-10-17).pdf?mkt_tok=eyJpIjoiTURnM016azVPRGhoTmpFMCIsInQiOiJ0MlwvXC9hVkxHUHlRamM5TytSVHMrS1ZNcWhidEZmTmtCMmN6d00wWHUxRWQzQ2NocTl2NWMxXC93blwvM3dJTG9p

Ormaza, D., Barrios, S. & Fernández, E. (2017). Proyecto Ypografí. Implementación de la Firma Digital en la Universidad de Buenos Aires. RedClara, 1-13. Recuperado de http://documentos.redclara.net/bitstream/10786/1276/1/90-17-4Proyecto%20Ypograf%C3%AD.%20Implementaci%C3%B3n%20de%20la%20Firma%20Digital%20en%20la%20Universidad%20de%20Buenos%20Aires.pdf

Peña, D. (2015). De la firma manuscrita a las firmas electrónica y digital. Bogotá, Colombia: U. Externado de Colombia

Pramendra, K. & Vijay, K. (2014). Information Security Based on Steganography & Cryptography Techniques: A Review. International Journal of Advanced Research in Computer Science and Software Engineering, 4(10), 246-250. Recuperado de https://www.researchgate.net/profile/Pramendra_Prajapati/publication/268388237_Information_Security_Based_on_Steganography_Cryptography_Techniques_A_Review/links/546a140c0cf2f5eb1807745e.pdf

Ramos, J. (2015). Historia clínica computarizada y firma digital: su implementación práctica. Revista OCE, 1-5. Recuperado de https://www.oftalmologos.org.ar/oce/items/show/334

Rocha, M., Castello, R. & Bollo, D. (2014). Criptografía y Firma Electrónica/Digital en el Aula. DUTI, 1-19. Recuperado de http://www.editorial.unca.edu.ar/Publicacione%20on%20line/CD%20INTERACTIVOS/DUTI/PDF/EJE2/ROCHA%20VARGAS.pdf

Saavedra, R. & Astolfi, M. (2015). Servicios Electrónicos Seguros. En RENIEC (Ed.), Identidad digital. La identificación desde los registros parroquiales al DNI electrónico (pp. 107-122). Lima, Perú: Escuela Registral

Sánchez, D. (2016). Ciberseguridad judicial y sellado de tiempo. Red Seguridad, 52-53. Recuperado de http://didacsanchez.com/docs/ciberseguridad.pdf

Sánchez, G. & González, C. (2016). Matemáticas en Criptografía: Uso en Seguridad de Tecnologías de Información.

SIIDMA, 131-138. Recuperado de http://www.eumed.net/libros-gratis/2016/1541/index.htm

Saravanan, C. & Kumar, R. (2015). A Novel Steganography Technique for Securing User's Digitized Handwritten Signature for Public Authentication Systems. Discovery, 43(200), 193-197. Recuperado de https://www.researchgate.net/profile/Saravanan_Chandran4/publication/293821299_A_Novel_Steganography_Technique_for_Securing_User's_Digitized_Handwritten_Signature_for_Public_Authentication_Systems/links/56bc21c108ae3f979315592a.pdf

Schaettgen, N., Levy, D., Schelnast, J. & Socol, S. (2014). Digital Signatures. Recuperado de http://www.adlittle.fr/sites/default/files/viewpoints/ADL_2014_Digital-Signatures.pdf

Sumalatha, P. & Sathyanarayana, B. (2015). Enhanced Identity Based Cryptography for Efficient Group Key Management in WSN. International Journal of Application or Innovation in Engineering & Management, 116-128. Recuperado de de https://pdfs.semanticscholar.org/a971/df8be1127a2cc9500359123579aa4e1e7098.pdf

Thangavel, J. (2014). Digital Signature Comparative study of its usage in developed and developing countries (Tesis de Master). Uppsala University, Uppsala, Suecia.

Urbina, G. (2016). Introducción a la Seguridad Informática. México D.F., México: Grupo Editorial Patria.

Vigil, M., Buchmanna, J., Cabarcasb, D., Weinerta, C. & Wiesmaierc, A. (2015). Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: a survey. Computers & Security, 50 (1), 16-32. https://doi.org/10.1016/j.cose.2014.12.004

Wadhwa, N., Hussain, S. & Rizvi, S. (2013). A Combined Method for Confidentiality, Integrity, Availability and Authentication (CMCIAA). Proceedings of the World Congress on Engineering, 1-4. Recuperado de https://pdfs.semanticscholar.org/482d/d56d71134c39e00e90a9d549f7e9172f39f0.pdf

WebTrust. (2017). Principles and Criteria for Certification Authorities. Recuperado de http://www.webtrust.org/principles-and-criteria/docs/item85228.pdf

Zhou, X., Gong, W., Fu, W. & Jin, L. (2016). An improved method for LSB based color image steganography combined with cryptography. ICIS, 1-4. https://doi.org/10.1109/ICIS.2016.7550955