Hamut'ay
Biannual Scientific Journal
Coordination of research and extension scientific-technological (CIECT-DUED).
University Direction of Distance Education-ALAS PERUANAS UNIVERSITY
http://revistas.uap.edu.pe/ojs/index.php/HAMUT/index
ISSN: 2313-7878
Vol. 5(2). July-december. Hamut'ay 2018. Lima-Peru

Analysis of digital signature based on the public key infrastructure

Análisis de la Firma con base en la Información de Clave Pública

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

Received: 07-01-2018
Accepted: 11-19-2018

Citation

Holguín, F. (2018) Análisis de la firma digital con base en la infraestructura de clave pública. [Analysis of digital signature based on the public key infrastructure]. Hamut´ay, 5 (2), 89-98. http://dx.doi.org/10.21503/hamu.v5i2.1622

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 database 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.

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.

1 Systems Engineer, Master's in Information Technology Auditing. Espíritu Santo University, Ecuador. E-mail fholguin@uees.edu.ec.

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.

Introduction

Communications networks have evolved vertiginously allowing connectivity in the transmission of images, voice and data that transcends borders; for this reason every day different business models incorporate digital platforms as the main mechanism of their financial activities, which has led to a greater exchange of information and a raised awareness of the level of security of the data and messages transferred, which are prone to threats of interception and analysis of traffic, identity theft, reenactment, modification of messages, and fraudulent degradation of service, among others (Martin, 2015).

Taking into account these aspects, companies and academies related to Information and

Communication Technology (ICT) have implemented methodologies that can guarantee robust security of the information based on four principles: I. Confidentiality, the information is hidden from unauthorized third parties; II. Integrity, the data are genuine and have not been modified since their creation; III. Availability, information is accessible at any time requested; and IV. Non-repudiation, to prove that a message is from the sender and avoid the recipient denying having received the message (Sánchez & González, 2016). Urbina (2016) points out that one of the methodologies that has provided high efficiency guarding the data is cryptography that satisfies these pillars through encryption techniques.

According to Joshi & Karkade (2015) the process of encryption and decryption have particular characteristics according to their nature, asymmetric cryptography being one of the more reliable ones, especially for the incorporation of digital signature algorithms (current and not colliding up to date) that guarantee the identity of the signer and the integrity of a message. However, Espinoza (2018) says that given the possibility that an issuer or recipient is unknown the authenticity of a digitally signed document joined the public key infrastructure (PKI) as a mechanism that implements authorities of Certification to legitimize correspondence from the keys to their authentic owners, certify the origin of a message, and guard to ensure compliance with guidelines and policies in their format, among other aspects.

Considering that the digital signature based on public key infrastructure possesses cryptographic operations that generate greater robustness than a signature generated by traditional methods, which is currently used in banking, commercial applications, and E-government; and that its fundamental principles are very similar to those of a handwritten signature (only its owner can create it, it may be verified by its transmitter and receiver, it cannot be repudiated by the sender) (Lojan, 2016); It is necessary to know how this architecture in real time guarantees the legitimacy of a sent message.

Is in that sense, the objective is making a description of the architecture and functionalities that certification authorities exercise in the process of creation and verification of a digital signature based on the public key infrastructure, and thus know its reliability in the identification and authentication of the signer and integrity of transmitted data.

Methods

This article is an investigation of documentary review, which analyzes various sources of literature on public key infrastructure and its application in the digital signature in order to sustain, that this type of signature offers greater reliability and robustness than other systems of electronic identity, being created by asymmetric cryptographic mechanisms and backed by certification authorities.

For the selection of bibliographic material, on which rests the theoretical framework, included: printed and virtual books, obtained from Google Books; journal articles indexed in Google Scholar, repositories, digital libraries and open access database (SciElo, Wos, Dialnet, Redalyc). In addition, the following were used as descriptors: Cryptography, PKI, digital signature and public key infrastructure trusted authorities.

Within the inclusion criteria it was defined that articles, books and analyzed documents correspond to the last five years of the issue; resulting in major publications of magazines.

On the other hand, presented literature was qualitatively analyzed, helping the distribution of this document in sections that include a logical sequential structure form in relation to the public key infrastructure. It should be noted, that this document uses indirect quotations, which are presented without quotation marks and include the respective bibliographical reference.

Digital signature

In 1976 American investigators, Whitfield Diffie and Martin Hellman explained the structure of a digital signature theory, giving the pattern to Ronald Rivest, Adi Shamir and Len Adleman to develop the RSA algorithm a year after (Saravanan & Kumar, 2015). This algorithm allowed the creation of the first digital signatures, which obeyed the same principles of the autograph signature, but insecurity prevailed, so it was necessary to add a cryptographic hash function to the original message (Thangavel, 2014). In 1984, Shafi Goldwasser, Silvio Micali, and Ronald Rivest proposed the first safety guidelines in a digital signature; and at the same time, other cryptographic schemes were created as: Lamport, Merkle and Rabin; which did not acquire greater relevance (Thangavel, 2014). Later (1988), the first software with commercial purposes for digital signatures was born called Lotus Notes 1.0, it was based on RSA (Thangavel, 2014). Three years later, the National Institute of Standards and Technology of the United States developed the DSA algorithm oriented to the Digital Standard Signature (DSS) with disadvantages compared to RSA, which had a longer computer processing time (Nabarjun, 2017). Later (1999), the PDF format acquired the ability to embed digital signatures to documents, however, it was in the year 2008 when the International Standardization Organization (ISO) made this format an open standard that included digital signatures as an integral part of their scheme, originating that the implementation of digital signatures had greater acceptance in the world (Nabarjun, 2017).

Rocha, Castello & Bollo (2014) point out that the digital signature is a cryptographic method that allows you to verify the original source of a message to subsequently verify that it has not been altered. For his part, Gaona, Montenegro & Wiesner (2014) established that a digital signature is the result of encrypting a message using one-way hash functions that guarantee that the only one who can decrypt the message is the recipient with its corresponding private key. In the same way, Lojan (2016) defines digital signature as a variant of the electronic signature, which is built, based on asymmetric cryptography allowing the association of the identity of the signer with a digital document.

Consequently, a digital signature involves a process of encryption (Gallo, 2015), and therefore it is necessary to distinguish the term cryptography which, according to Zhou, Gong, Fu, & Jin (2016) is a discipline that studies the techniques to transform a plain text into ciphertext using cryptographic keys (parameter that allows a user to encrypt or decrypt data) and that in addition, it enables the prevention of security flaws in a computerized system ensuring the confidentiality, integrity, authenticity, and non-repudiation of information (Wadhwa, Hussain & Rizvi, 2013).

Medina & Miranda (2015) point out that Cryptography is classified into: symmetrical, which uses the same key to encrypt and decrypt the data; and asymmetrical, which uses a pair of keys (one is published and the other is securely stored) but, Boneh & Shoup (2017) demonstrate that there is hybrid cryptography, which combines the safety of a public key with the efficiency of a symmetric key algorithm. In this context, Joshi & Karkade (2015) show that asymmetric cryptography is mostly used in the creation of a digital signature because its methodology provides greater robustness.

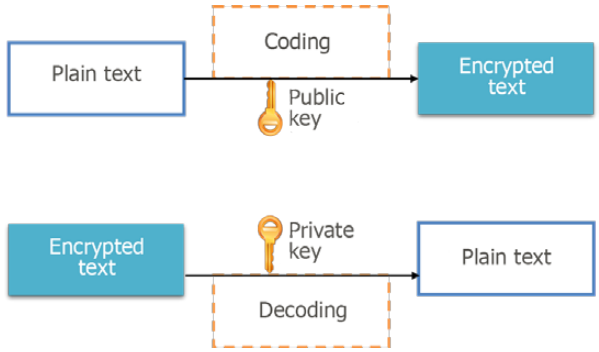

Figure 1: Process of encryption and decryption in Cryptography
Source: Medina & Miranda (2015, p.16)

In this regard, a digital signature built with asymmetric cryptography uses two different keys with a mathematical relationship among themselves: the public key is responsible for coding and the private key allows the decryption (Malhotra, 2015). In the same way, Joshi & Karkade (2015) show that when creating a digital signature with asymmetric cryptography, algorithms are implemented which generate a pair of complementary keys, which performs the process of encryption and decryption of a message. In addition, Pramendra & Vijay (2014) point out that the public key is freely available, while the user owner only knows the private key. Figure 1 shows an outline of this process.

Peña (2015) indicates that in an ideal context a digital signature has the same properties of a handwritten signature, because it is authentic, unforgeable, unalterable, non-reusable and cannot be repudiated; it is important that technology, which generates it, provide a secure scheme to meet these attributes otherwise could be altered/corrupted. According to Rocha, Castello & Bollo (2014) a digital signature may be built with different techniques, but the standard public key infrastructure provides greater robustness since the owner has sole control of the signature, the verification process is performed for any entity who knows the signer's public key, and the certification authorities recognize the sender identity.

Public Key Infrastructure (PKI)

With the birth of asymmetric cryptography, the problem of key management arose and was mitigated with the creation of a directory called Public Archive that contained the name, number and public key of the recipient (Albarqi, Alzaid, Ghamdi, Asiri & Kar, 2015). When the sender wanted to send a message, they should look for the recipient by name to find the public key, which did not offer the necessary guarantees to demonstrate that this key belonged to the desired recipient (Afshar, 2015). In 1980 this context led the International Telecommunications Union (ITU) to build a directory that could store the keys of all persons and devices in the world, which gave origin to the X.500 standard that completely defined the characteristics of that directory (Albarqi, Alzaid, Ghamdi, Asiri & Kar, 2015). However, given the need to ensure authentication, the X.509 was born, and pinned down the format for digital certificates and incorporated to a trusted third party to verify the correspondence of a title to a public key, leading to the moment in which the concept of PKI arose (Afshar, 2015).

Abobeah, Ezz & Harb (2015) defined public key infrastructure as a combination of software, hardware, policies and people that have objectives to manage (create, issue, modify, store and delete) digital certificates, authenticate the identity of the sender and the receiver, and provide data integrity. For their part, Cantero, Baran & Stuardo (2014) indicated that it is an architectural model that allows you to manipulate the public keys and ensure correspondence to their legitimate owners. According to Ramos (2015) a PKI is a set of security policies, procedures, and technologies to create, issue and manage digital certificates based on public key cryptography.

Consequently, the public key infrastructure is used to establish robust authentication services and security protocols based on asymmetric cryptography such as IPSec, SSL/TLS; allowing the associate of an entity with its pair of generated keys, performing the encryption and decryption of a message, and ensuring non-repudiation of a shipment (Sumalatha & Sathyanarayana, 2015).

Cantero, Baran & Stuardo (2014) assert that the objective of a PKI is to create a document that verifies the authenticity of a public key, which is called a Digital Certificate. Ramos (2015) defines a digital certificate as a data structure linking a public key to an entity, which has been recognized by a Certification Authority, which has a specific validity period and includes the digital signature of the Authority to validate its legitimacy. Angle & Henao (2017) established that a digital certificate is generally uses usually the X.509 standard to define the structure and the corresponding fields, and actually said standards were found in version 3. Figure 2 details the format of the standard X.509 v3.

Gutierrez (2014) says that running a cryptographic operation that uses PKI involved at least three elements: i. User, which starts the process; ii. Authorities, which validate the certificates; iii. Recipient, who receives the encrypted data. In addition, Albarqi, et al. (2015) establishe that the primary components of a PKI are: i. Registration Authority (RA), ii. Certification Authority (CA), iii. Security Policies, iv. Trusted applications for PKI, v. Distribution Systems and vi. Repository of Certificates

According to WebTrust (2017) the registration authority (RA) has as function to authenticate the identity of the user or device that requires a digital certificate but may not issue or sign a certificate. Similarly, Ormaza, Barrios & Fernandez (2017) assert that a RA unequivocally recognizes the applicant of a certificate and performs the registration process for their issuance.

WebTrust (2017) evidences that the certification authority (CA) is a trusted third party that guarantees the relationship between the public key and the user data registered within a digital certificate. Moreover, Cutanda (2013) says that when the

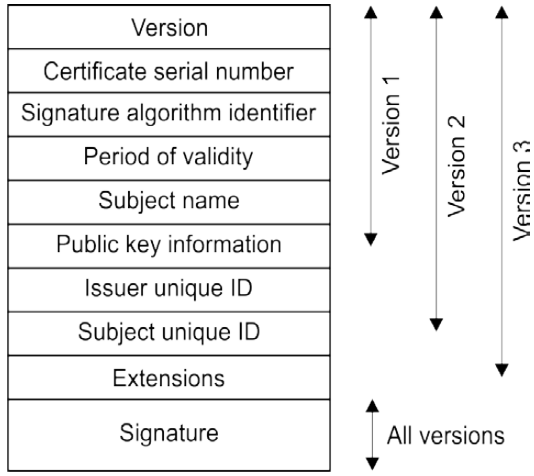

Figure 2: Format of certificate X.509 version 3
Source: Hawanna, Kulkarni, Rane, Mestri, & Panchal (2016, p. 2)(2016, p. 2)

CA issues a certificate it generates in the format X.509 v3 by adding their digital signature which allows a third party to verify its authenticity using the public key of the CA. Likewise, the functions of the certifying authority are: issue certificates, maintain and generate certificates revocation lists (CRL) and retain information regarding the expiration dates of certificates (Afshar, 2015).

Nelson & Nordenberg (2016) determined that security policies are operating procedures that govern the operations of the PKI and have technical and legal validity, for example: criteria that ensure that the method to validate the identity of the holder of the certificate is reliable, rules to establish who can revoke certificates, measures of how to distribute reversa lists, and guidelines that determine the frequency for filing certificates, among others.

Albarqi et al. (2015) outlined that the PKI-enabled applications are programs/software suitable for handling digital certificates, so, for example: web browsers, e-mail clients, and operating systems, among others.

Nelson & Nordenberg (2016) set up a distribution system that is intended to automate the management of digital certificates.

According to MICITT (2018) a Certificates Repository stores valid certificates for entities/applications, which require it to download them. These repositories used directories like the X.500

which are accessible via open protocols that allow the consultation of centrally saved information through the network, the most used being the Light Weight Directory Access Protocol (LDAP)) Abobeah, Ezz & Harb, 2015).

Nelson & Nordenberg (2016) show that the elements of the PKI described above present a process interrelated through phases, which begins when the applicant appears to the Registration Authority (responsible for the capture of registration information and key generation), and the entity communicates with Certification Authority to transmit the data of the applicant. After registration, the applicant can access the Certification Authority to obtain a digital certificate signed by this entity, but custody of the private key will be the responsibility of the Recipient during the valid time of the certificate. It should be noted that the applicant (using a cryptographic software) or the certification authority (Gallo, 2015) could perform the asymmetric key generation process. Figure 3 shows the operation of a PKI architecture.

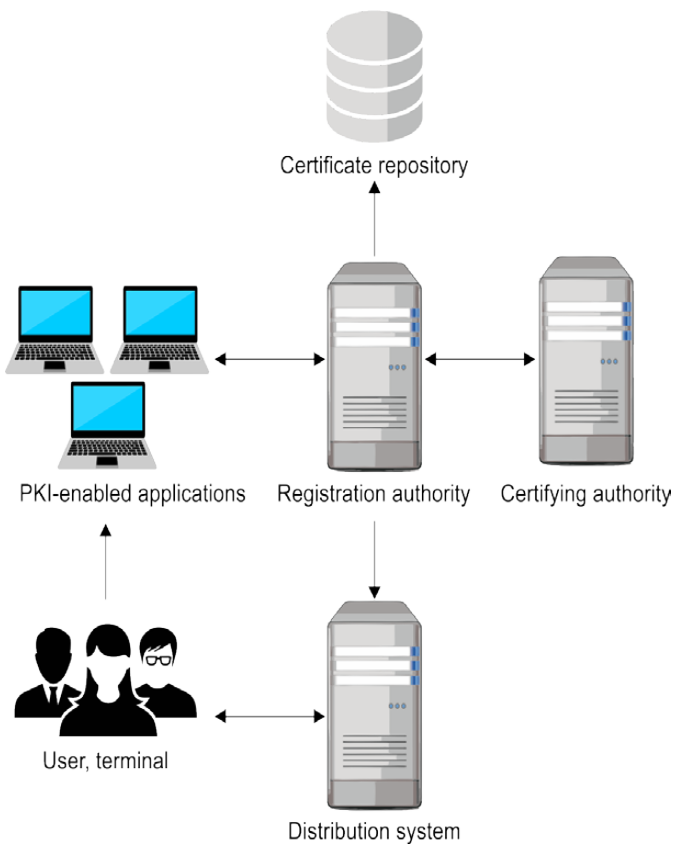

Figure 3: A PKI architecture
Source: Albarqi, Alzaid, Ghamdi, Asiri & Kar (2015, p. 33)

On the other hand, Cuno (2015) evidences that given the possibility that a user requires to verify the legitimacy of a digital certificate they can appeal to a Validation Authority (VA), which will determine the validity of the document based on the CRL or OCSP (Protocol that allows you to request the status of a certificate to a server). In addition, if necessary, it will include a time stamp issued by the Time Stamp Authority, which unequivocally recognizes the truth of the certificate even if it has expired (Sánchez, 2016).

Digital Signature based on the Infrastructure of Public Key

Peña (2015) defines the digital signature based on public key infrastructure as a procedure using cryptographic techniques that requires the participation of a trusted third party to prove the identity of the issuer. In this sense, Ramos (2015) says that PKI-based digital signature plays an important and irreplaceable role in the security of electronic transactions, authentication of identity, digital integrity and non-repudiation; for this reason, they are used in software distribution, financial transactions and in environments where it is important to detect the falsification and manipulation of data.

Gaona, Montenegro & Wiesner (2014) show that to build a digital signature based on public key infrastructure requires a function hash (SHA-2, SHA-3, RIPEMD-160) which converts a variable-length text in a block of length set in the summary form that is irreversible (cannot retrieve a text from your summary); and an asymmetric algorithm (RSA, DSS, ECDSA) that generates two keys, being the public key and the private key that allows you to sign and authenticate the signature.

Rocha, Castello & Bollo (2014) indicate when the process of signing is in progress; first, the sender creates a message, then applies the hash function and then encrypts it with their private key. A Certification Authority that will validate its origin and content shall review each message signed by the issuer, and only if it is correct will it be sent to the receiver attached to the Digital Certificate. Finally, the recipient receives the mes-

sage with two elements: the message (plaintext or encrypted with the public key of the receiver) and digital signatures (formed by the hash with the private key of the issuer and encrypted with the private digital key certificate of the Certification Authority).

According to Gallo (2015) to verify the validity of a digital signature, the receiver must decrypt the digital certificate of the issuer using the public key issued by the Certification Authority (having accessed the key through the web page of the CA). After decoding the certificate, the receiver will know the public key of the issuer, which will allow them to decrypt the received hash; and if the message was encoded, they can decrypt it with their private key. Finally, the receiver compares the hash received from the issuer with their hash retrieved, if both are equal it is considered that the message is authentic, the digital signature corresponding to the sender and that the message has been decrypted with a public key and encrypted with a private key. Figure 4 details the Signing and Verifying Process of a digital signature based in PKI and figure 5 is the frame of reference.

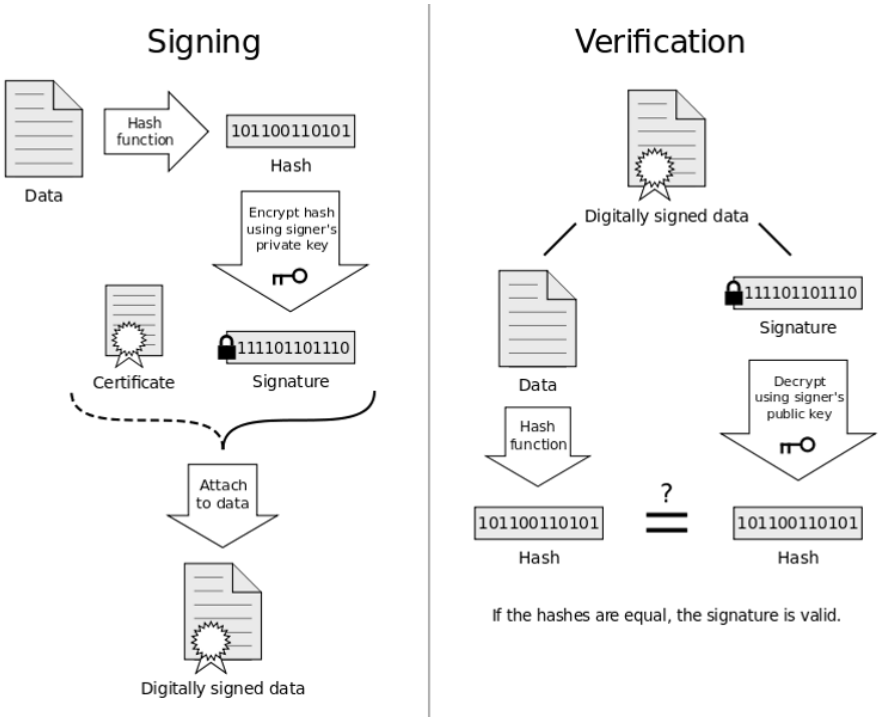

Figure 4: The process of signing and verifying a digital signature based on PKI
Source: Ramos (2015, p. 3)

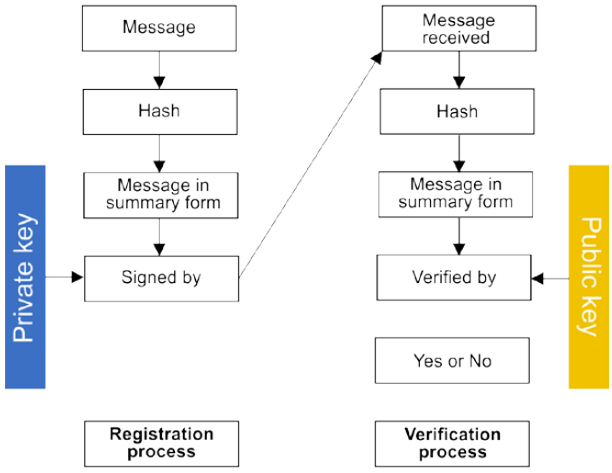

Figura 5: Reference framework to register and verify a digital signature based on PKI
Source: Ramos (2015, p. 4)

Cuno (2015) designates that the process of generating and verifying a digital signature based on PKI is based on two entities: i. Certification Authority, which provides confidence to both the transmitter and the receiver that the distribution of the key is secure; and ii. Revocation List of Certificates, which must be constantly updated by the corresponding Certification Authority; but it, is necessary that the public key infrastructure is supported by an appropriate legal framework, each authority that is equipped with a secure computer system, and that the signer relies on the transparency of this process.

On the other hand, Schaettgen, Levy, Schelnast & Socol (2014) distinguish two types of digital signatures, which are differentiated by the security that is based on authentication, and are: i. Recognized digital signature (RDS), created with a unique device, that is to say, distinguished from the one used to sign the document (which gives more safety); and ii. Advanced Digital Signature (ADS), developed with the same device that was used to sign the docu-

ment, and therefore, is less robust than the RDS. In this context, Saavedra & Astolfi (2015) point out that cryptographic devices that are implemented for the creation of digital signatures are governed to standards such as: FIPS 140-2 level 3 or Common Criteria ISO 15408 EAL 4 +; and one of the most widely used devices is the HSM (Hardware Security Module), which generates, stores and protects cryptographic keys; Therefore, it provides greater security and performance in operations of Cryptography.

In another area, Vigil, Buchmanna, Cabarcasb, Weinerta & Wiesmaierc (2015) manifest that digitally signed documents are retained for some years but if it is required to preserve them by decades or longer time technological problems may arise, such as: cryptographic obsolescence, the algorithms can be corrupted in this interval; loss of integrity, flaws in the physical devices due to the migration of new formats; obsolescence of software, evolutionary changes that meet the requirements of the time; obsolescence of hardware, physical impairment or technological evolution.

Finally, it is necessary to annotate that the digital signature technology based on PKI, in addition to being used in the identification and authentication of an entity, can also be implemented in electronic commerce, to safeguard a transaction; On the network, to identify the authenticity of a web site; in software, to prevent their manipulation, among others (Saavedra & Astolfi, 2015).

Conclusions

The development of communications networks and the global trend pf mainly implementing online trade has aroused increasing interest in safeguarding data and information transmitted from threats and vulnerabilities that destroy the reliability of any web process, therefore the encryption techniques have become a fundamental pillar that strengthens the principles of computer security (Urbina, 2016).

Asymmetric cryptography enabled the development of the digital signature as a mechanism to support that the information exchanged has not been altered, through this it is being implemented with greater consent in transactions where a traditional signature is powerless (Joshi & Karkade, 2015).

Coincidentally mentioned by Rocha, Castello & Bollo (2014), public key infrastructure constitutes a rigorous architecture, in which each element (Authority) has defined roles that guarantee the transparency of the process of generation and delivery of keys and unambiguously identifies an entity, therefore it is the standard most used to create safe digital signatures; However, barriers such as: the cost of implementation, few specialists in the country and interoperability have limited its use.

A digital signature based on public key infrastructure is a technology that ensures through asymmetric algorithms, hash function and digital certificates, authentication, integrity and non-repudiation of a message; and in this sense Espinoza (2018) highlights that its correct establishment should be covered by an adequate legislative framework, use a hardware and sophisticated software, and each user must be aware of the responsibilities (cannot disown the authenticity of a digitally signed document) that are acquired when they implement it. It is important to highlight that the validity of a digital signature is not imperishable, various requirements must be met (arising in accordance with technological evolution) to ensure its validity in both the long and short term. In addition, its scope can be global or limited to a territory specific (Vigil et al. 2015).

It is necessary to increase efforts so that the operation of the PKI-based digital signature as an instrument of public domain, encourages confidence in economic, administrative and governmental activities so that they increasingly incorporate this technology in their processes (Lojan, 2016).

On the other hand, we agree with Saavedra & Astolfi (2015), who distinguish that the security of an environment is the result of the combination of various processes and technologies; consequently, a PKI-based digital signature is not the solution to all the possible security problems in an organization.

Here we have shown only performance, architecture and advantages offered by the digital signature based on the public key infrastructure to authenticate a sender and integrity of a message based on the exploratory analysis of previous works. Therefore, future continuations of this investigative line could explore which formats, packaging and levels ensure greater interoperability and effectiveness, exposing current regulations in Ecuador that protect its legal validity and define a model of digital signatures implementation (zero papers project) for small and medium-sized businesses that have not yet migrated to this technology.

In addition, in a following moment, a comparison could be made about the performance characteristics of the traditional digital signature algorithms like RSA as opposed to elliptic curve based on those latest-used keys, which are much smaller and provide an equivalent level of security.

Bibliographic references

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 Jerar-

quía 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