Multi-Knowledge Electronic Comprehensive Journal For Education And Science Publications (MECSJ)

ISSUE (21), July (2019)

ISSN: **2616-9185**

www.mecsj.com

Studying and evaluating the most secure digital signature methods for information

Fahad B M Alajmi

E-mail: ajmiq8@gmail.com

Abstract:

In the last few years, with the proliferation of computers and with the increasing number of individuals, organizations and companies and many communities who use computers connected together on the Internet, in the light of these developments appeared the term digital signature. So the current research aims to Studying and evaluating the most secure digital signature methods for information. To achieve the aim and objectives of the research was used descriptive approach that corresponds to the nature of research. The current research has confirmed that the use of digital signature improves the services provided to individuals by reducing time, effort and safety. In addition to, the use of digital signature technology increases the security, reliability and ease of service delivery and protects against intrusions and piracy that have increased in the world in recent years.

Keywords: digital signature, key, hash, function, internet, technology.

1. Introduction

Today's science is witnessing a huge digital revolution in the Internet, in addition to the increase in the number of Internet users and the explosion in the large applications and sites offered by the Internet world, which is critical to the good performance of governmental, commercial, educational, social, civil, recreational institutions and organizations. Despite the great benefits of digital technologies and developments, it has created a large number of problems and challenges such as abuse and digital crimes that have increased dramatically and include activities such as infiltration attempts, massive denial of service attacks, malware, identity theft, digital fraud and embezzlement on a scale And violation of intellectual property rights. [1]

A digital signature is a scientific method utilized for authorize the authenticity and integrity of a communication, electronic or digital file. A digital signature for handwritten or stamped signatures provides more essential security, and it is designed for resolve the issue of tampering and identity in digital communications.

Digital signatures can provide the additional confirmations to prove the origin, identity, or status of a digital file, operation or message and may acknowledge informed approval through the signer. [2]

The proliferation of digital signature is one of the major advantages that will lead to the expansion of electronic commerce and secure all transactions at the international and local levels, Many Arab and international countries have been working on the enactment of many laws concerning the digital signature and methodology and the extent to which it is used to secure the confidentiality of information sent with the inability of anyone to see or modify part of it. [3]

1.1 Problem Statement:

With the growing role of the Internet in human life, the increasing volume of data and information exchange, the network contain a large amount of personal information and very important business transactions, the protection of these important data has become one of the most important challenges that specialists in this field seek to provide. Studies show a significant increase in the penetration of these important data, which requires the formulation and development of new ways to protect this information is priceless, as well as protect and secure all digital information, including digital commerce. One of these means of protection is the emergence of digital signature, which has become important in the present era. Therefore, the current research was conducted to study and evaluate the most secure digital signature methods of information.

1.2 Research Questions

The current search problem can be represented by answering the following main question:

- What are the most secure digital signature methods for information?

A set of sub-questions arises from the main question, most notably the following:

- What is the concept of digital signature?
- How digital signature technology works?
- How important is the application of digital signature technologies in the current era?

1.3 Research Aim and objectives

The current research aims to study and evaluate the most secure digital signature methods of information, the research aim can be achieved by achieving the following objectives:

- Identify the concept of digital signature.
- Identify the mechanism of digital signature technology.
- Revealing the importance of applying digital signature technologies in the current era.

1.4 Hypotheses of the research

H1: The use of digital signature improves the services provided to individuals by reducing time, effort and safety.

H2: The use of digital signature technology increases the security, reliability and ease of service delivery and protects against intrusions and piracy that have increased in the world in recent years.

2. Digital signature

The digital signature is a specific type of electronic qualified signature through which the authenticity and integrity of the digital document can be verified. The digital signature is a means of ensuring that the electronic document (e-mail, spreadsheet, text file, etc.) is authentic. It is a mechanism to ensure that the integrity of the document or file is verified and that it is not exposed to any change. [4]

Digital signatures are based on certain types of encryption to ensure authentication. Encryption is the process of taking all data sent by a computer to another device and coding it in a way that only the other computer can decrypt. Authentication is the process of verifying that this information comes from a trusted source, these two processes work side by side to produce digital signatures.

Digital signatures are letters that determine and document a specific individual as the source of the email; and indicate such person's approval of the information contained in the email. It support users to realize main security building blocks like identification, authentication, and integrity. [5]

The digital signature algorithms usages several kind of complicated processes goals to deny the data access only to the authorized users, and computing such operations could exhaust the systems with limited computational resources; the problem statement affects the integrity of the data directly and minimizes the security level to facilitate the process of penetration, then the algorithms should be selected depending on the degree to maintain the integrity of the information regardless of the kind of device. [6]

The figure below shows the general framework for creating and verifying a digital signature that was used to send a message:

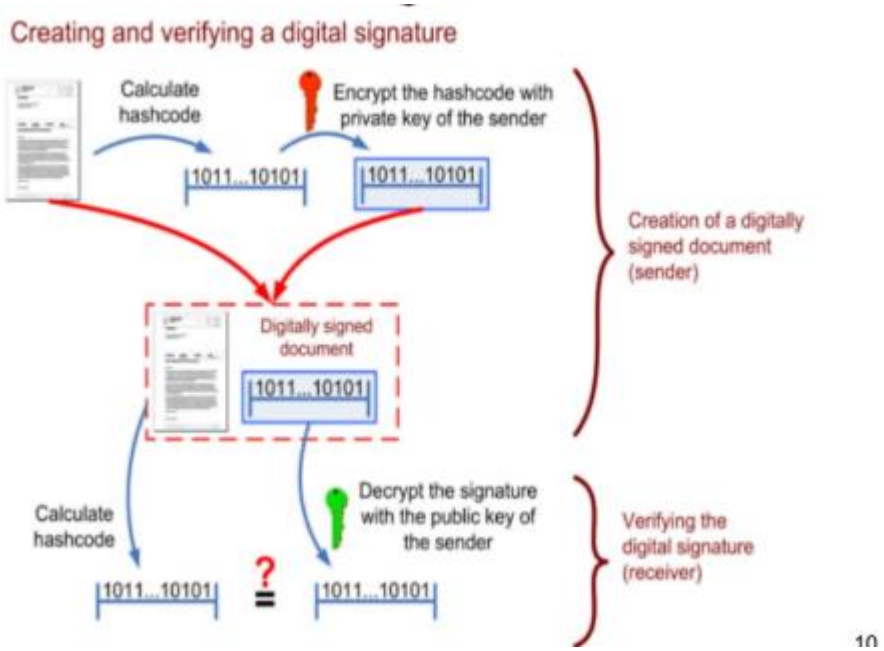

Figure 1: general framework of Digital Signature. *[7]*

The encryption process in modern information systems consists of four keywords used to describe all the different roles that encryption plays, which are the following points: [8]

- **Confidentiality and Privacy:** utilized for stamp information transmitted via remote transmission in open channels and stored on a server, so that attacker cannot access the data contents.

- **Authentication:** confirms the identity of the user who is transfer the information. The receiver of the information can validate the identity of the user who signed it.
- **Integrity:** safeguards that the content of message is not changed during transportation.
- **Non - repudiation:** has the purpose of safeguarding that the author of a message cannot incorrectly reject its transmission.

3. Types of digital signatures

In the digital signature, two different keys are created but are mathematically linked by a mathematical formula: the private key and the public key. The first, which is known only by the sender, is used to encrypt the data and the second is used to decode the message and is known to the recipient or Reliable sources for access if required. Digital signature takes many forms and types, the following are the most prominent types of digital signature: [9]

- **Key Based Signature**

In this type, the digital document is provided with an encrypted digital signature that diagnoses the user who signed the signature and signature time and information about the same person, which is usually distinctive to the signature owners.

- **Signature Biometric**

The user is here using an electronic pen that is connected to the computer and the user starts to sign using the pen, which records the pattern of the hand movements of the user and his fingers, each of us has a different style from the other where this feature is set.

4. Public Key Infrastructure

Digital signatures can be configured by different technologies; on the other hand, the only digital signature standard adopted by National Institute for Standards and Technology (NIST) uses public key encryption joint with a one-way hash function. This infrastructure, usually indicated to as the Public Key Infrastructure (PKI), is designed for every user to have a public-private key couple where the public key is existing to the domain while the private key is identified only through the user. In the Figure below shows the usage of PKI to creating digital signatures. [5]

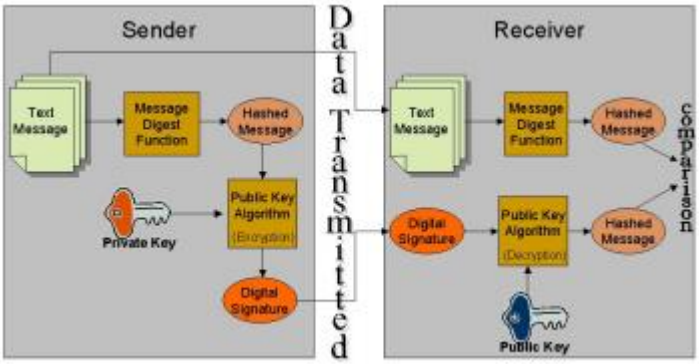

Figure 2: Digital signatures using PKI. *[5]*

In the PKI method, there is the digital certificate concept, which in general is a data structure that links user data like name, country, and institution to its public key. A digital certificate is typically utilized for bind a structure to a public key. To safeguard digitally if a PKI exists, the certificate is signed via the Certification Authority that released it and in the state of the standard confidence website, the certificate is signed via the entity and through others who say they confidence in that entity. In either state the signatures contained in a certificate are a statement issued via an entity that says confidence the information contained in that certificate. [8]

The usage of digital signature without some certification way of the public key may allow attacks in which the identity of the user is falsified, for example, "man in the middle" attack.

5. Hash function

An essential process of digital signature processes used in both digital signature creation and validation. Hash's function is an approach that creates a certain digital representation at a standard length that is usually smaller than the message but is actually limited to it. Any change in the message results in a different hash result when using the same hash function. [10]

When a user creates an accompanying message for his digital signature, they are usually merged with some code as a basic function called 'Hash function' and used at the beginning of creating and verifying the digital signature.

The way it works is based on the creation of a particular digital representation in the form of a numeric value 'Hash'. This value is usually smaller than the message and is placed either at the beginning or at the end and incorporated into it.

In this case if this message is manipulated, the value of 'Hash' calculated from the very beginning will be changed immediately when the message is created. Even if the value of the second 'Hash' is identified, it is difficult to trace the initial Hash value. [11]

Hash's functionality allows software to create digital signatures to work on a smaller, predictable amount of data while still providing a strong and clear correlation with the contents of the original message and thereby providing effective assurance and assurance that no modification has been made to the message since it was digitally signed. [12]

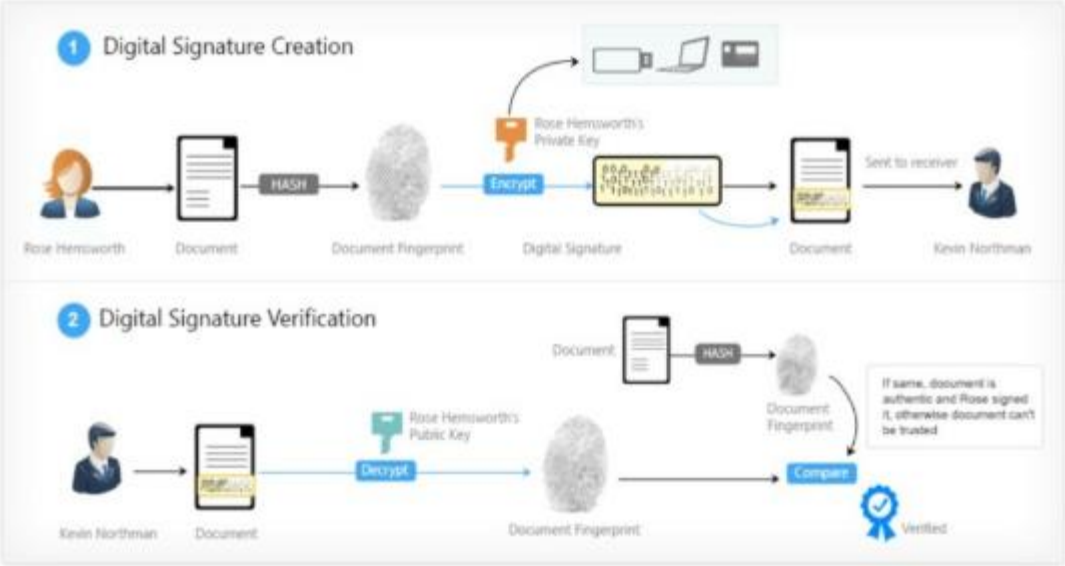

Figure 3: How digital signatures work. *[7]*

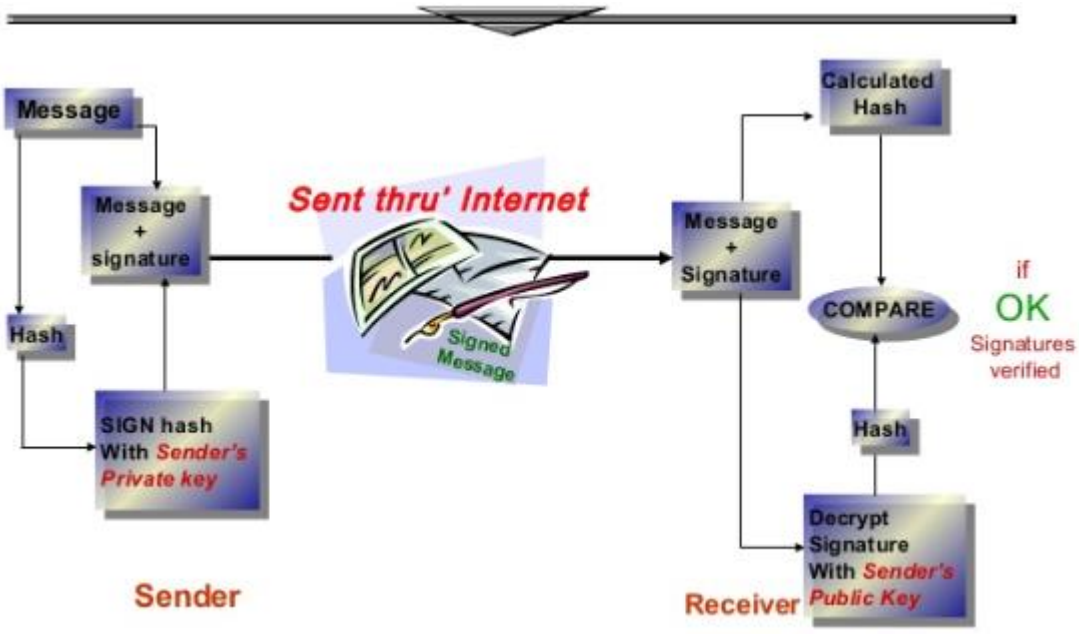

Figure 4: How digital signatures work. *[7]*

6. Evaluation

The signature is a prerequisite for documenting most documents, whether in manual or digital correspondence of all types, whether local or international, and with the emergence of new challenges facing the digital and security economy, in particular the emergence of e-government and the lack of adequate safeguards to protect the society In particular with the electronic system and dealing with it with confidence and safety has become the need for the emergence of a safe, fast and effective way to certify documents that are exchanged electronically at all levels in all stages and legalization And then archived digitally all this led to the emergence of so-called digital signature.

A digital signature, such as a written signature, is used to authenticate the content of the signed file, which is usually called a message. This can be in the form of an e-mail, a specific contract, or even a digital message. The digital signature is used to create a type of public key, so that the user's key is linked to a specific digital document and identity issued by a particular authority. Thus, this process is closely related to the user's specific information (name, address, phone number) of the user's own identification type or identity.

7. Conclusion

One of the asymmetric encryption algorithms is the authentication of data through the use of digital signatures. Simply put, the digital signature is a segmentation created using the data in the message. When sending this message, the signature can be verified by the recipient using the public key of the sender as a way to authenticate the message source and to make sure that it is not tampered with. In some cases, digital signatures and encryption are applied together so that the same fragmentation can be encrypted as part of the message. However, all digital signature schemes do not use encryption techniques.

When starting to create a digital signature through the authorized bodies, it requires a high degree of security according to international standards and licenses, which are usually approved by the digital site, and here, without a doubt, generate the highest security standards.

References

[1] S. Saleem, O. Popov and R. Dahman, "Evaluation of Security Methods for Ensuring the Integrity of Digital Evidence," International Conference on Innovations in Information Technology, Kista, Sweden, 2011.

[2] P. K. Sahoo and M. Lenka, "development of certificate less digital signature scheme and its application in e-cash system," 2011.

[3] A. Kamuzora and H. M. Twaakyondo, "Evaluation and Implementation of Digital Signatures to Improve Web Based Case Management System Information Security," *International Journal of Computer and Information Technology,* vol. 2, no. 4, 2013.

[4] S. Cavallini, F. Bisogni, D. Gallozzi, C. Cozza and C. Aglietti, "Study on the supply-side of EU e-signature market," Final Report for the DG Information Society and Media of the European Commission, 2012.

[5] B. Tulu, H. Li, S. Chatterjee, B. N. Hilton, D. Lafky and T. A. Horan, "Design and Implementation of a Digital Signature Solution for a Healthcare Enterprise," Proceed ings of the Tenth Americas Conference on Information Systems, New York, 2004.

[6] A. I. Ali, "comparison and evaluation of digital signature schemes employed in ndn network," *International Journal of Embedded systems and Applications(IJESA),* vol. 5, no. 2, 2015.

[7] M. Talaat, "Digital Signature," slideshare, Cairo, Egypt, 2018.

[8] V. Schoaba, F. E. Gomes and L. C. Branco, "Digital Signature for Mobile Devices: A New Implementation and Evaluation," *International Journal of Future Generation Communication and Networking* , vol. 4, no. 2, 2011.

[9] R. A. S. Al-Shnawa, "Enhancement of Digital Signature Scheme," 2018.

[10] JayakumarThangavel and S. Mckeever, "Digital Signature Comparative study of its usage in developed and developing countries," 2013.

[11] J. Buchmann, E. Dahmen and M. Szydlo, "Hash-based Digital Signature Schemes," 2009.

[12] S. Hameed and G. G. Jumaa, "Digital Signature Based on Hash Functions," *International Journal Of Advancement In Engineering Technology, Management and Applied Science (IJAETMAS)*, vol. 4, no. 1, 2017.