e-ISSN: 2458-8091

Journal Homepage: http://dergipark.gov.tr/ejsdr

DergiPark AKADEMİK

EJSDR

European Journal of Sustainable Development Research

CODEN: EJSDR

The Role and the Impact of Digital Certificate and Digital Signature in Improving Security During Data Transmission

Nexhibe Sejfuli - Ramadani[1]*, Verda Misimi[1], Erenis Ramadani[2], Florim Idrizi[1]

[1]*Tetova State University, Faculty of Math-Natural Sciences, Depratment of Informatics, 1200, Tetovo, Macedonia.*

[2]*Software Engineer, AdaptiveScale, 1200, Tetovo, Macedonia.*

**Corresponding Author email: nexhibe.sejfuli@gmail.com*

Publication Info

Paper received:
01 June 2016

Revised received:
19-23 October 2016

Accepted:
01 March 2017

Abstract

This paper is cryptographic oriented research, aiming to describe the notion, role and impact of digital signature and digital certificate for the wide audience. Security improvement during data transmission comes as a result of the huge growth of electronic communications. While one party is trying to secure these data, there is always another party trying to reach and use them in several cases, so understanding the importance of digital security is quite important for everyone using a computer nowadays. Thus, the research explains the need for these types of technologies. Reading the paper, you will meet a comparison between paper and digital signature and digital certificate compared to digital signature. During this research were used Observational and Correlational research methodologies. As a conclusion, we can say that electronic signatures and certificates are making life easier for organization leaders, HR and all of other company sectors in a variety of industries, allowing them to freely announce, communicate or exchange several documents or high sensitive data.

Key words

Cryptography, Digital Certificate, Digital Signature, Private Key, Public Key

1. INTRODUCTION

Increased use of water and energy

Digital signature notion was first used and described in late 1976 by Whitfield Diffie and Martin Hellman, although it was still just an assumption. Soon after that, RSA algorithm was invented by Ronald Rivest, Adi Shamir and Leonard Adleman, which, in that time, produced only primitive digital signature. Only in 1989, the first widely marketed software package using RSA algorithm was released. It was called *Lotus Notes 1.0*.

Later on, there were more digital signature schemes developed, such as *Lamport signatures*, *Merkle signatures* – also known as *Merkle trees* or *Hash trees*, and *Rabin signatures*.

In the other hand, *digital certificate* is an electronic document which is used to prove ownership of a *public key*. It contains information about the key itself, information about owner, and the digital signature that verifies correctness of certificate's content. In other words, the digital certificate is an electronic passport that allows information exchange securely over the Internet using the *public key infrastructure* (PKI).

Digital certificates are handled by a trusted *certificate authority* (CA). Thus, to provide validity of the certificate, it is digitally signed by a root certificate that belongs to these CA. Operating systems and browsers maintain lists of trusted CA root certificates so they can verify that the certificate is issued and signed. [1]

2. DIGITAL SIGNATURE

Digital signature is a mathematical technique for validating the authenticity and integrity of several electronic components, such as messages, software or digital documents.

It is intended to ensure that there will be no tampering or impersonation while communicating in electronic way.

2.1. How it Works?

Digital signature technology is based on public key cryptography, also known as *asymmetric cryptography*. The most used algorithm in this type of cryptography is RSA, where one can generate two linked keys: *private key* and *public key*. First, there is created a one – way hash of the electronic data that is required to be signed. The private key is used to encrypt this hash. Thus, encrypted hash – along with the rest of the information represent the digital signature.

- *But, why encrypting the hash instead of the entire message or document?*

Because, encrypting the entire document costs a lot of time. The hash function can convert an input into a fixed length value, which, compared to the document length, is much shorter.

The value of the hash is unique. It means that for a given amount of data, there is one and only one unique hash value. Changing a single character or a single bit of that data means a completely different hash value. Thus, using the signer's public key, the other party can decrypt the hash, and validate the integrity of the data. So, if the decrypted hash is computed again, and it matches with the first one, it means that the data has not changed after signing. In the other hand, if the decrypted hash does not match, it means that there has either been tampering in the data, or the signature was created with a private key generated separately from the public key used to decrypt these data.

But, all of this said above, does not mean that the message or the document has to be encrypted. Instead, the digital signature works with both, encrypted and decrypted messages or documents. It is meant to ensure that the sender of these messages or documents is the one expected to send.

Modern data – transmitting software, such as mail applications support the use of digital signature and certificate.

2.2. Application

The most common application of digital signature is authenticating the source of the message, ensuring message integrity and ensuring that the sender will not deny authenticity.

2.2.1. Authentication

Although digital messages contain information about the sender, these information may ofter be incorrect or not accurate. In this case, digital signature allows to make sure that the sender of a message, is the one we think it is. If a user is the owner of a digital signature secret key, a valid signature ensures that the message is sent by that user. The most sensitive is the financial section, where the importance of high confidence in sender authenticity is obvious. For example, if a branch of some bank requests from the central office to make changes in the balance of an account, acting on such a request, not being sure that the request comes from a known and authorized source could be a fatal mistake.

2.2.2. Integrity

During data transmition, there is always potencial risk that the transmited data can be altered in the meanwhile. Even if the message is encrypted, it can be altered without knowing its meaning or what is being changed. There are just a few algorithms that can prevent this scenario, but the most of them can not. However, if the message is digitally signed, every minor possible change of that message is detected. Additionally, because of the hash function, there is no way to produce a new message with a valid signature, after it has been signed.

2.2.3. Non – Repudiation

Non – repudiation is also an important reason to use digital signature. This property aims to make sure that, the entity that once has signed some information, can't deny it at a later time. Furthermore, having access to the public key only, does not allow someone to create a fake valid signature. [2]

3. DIGITAL CERTIFICATE

Digital certificate is some kind of certificate issued by trusted Certificate Authorities (CA) aiming to verify the identity of the certificate holder. Typically, a digital certificate contains the following information: unique *serial number* used to identify the certificate, identified *entity* or *individual* by the certificate, *the algorithm* used to create the signature, the *CA* that verifies the information in the certificate, period of time including *starting date* and *expiry date* of validity of the certificate, *public key* and *the thumbprint* (to make sure that the certificate is not modified "itself").

3.1. Application

Digital certificates are very important component of *Transport Layer Security* (TLS), also known as SSL (*Secure Socket Layer*), preventing cyber attackers from impersonating a website or server. Additionally, they are used in email encryption or code signing.

3.1.1. Website Security Using Digital Certificate

Web browsers validate that a TLS web server is authentic, so the users can feel secure in their interaction with the website, ensuring it does not have any third party listener and it is who it claims to be.

To get the certificate, a website operator must apply to a certificate provider with a *certificate signing request*. This request is an electronic document containing website name, contact email address, company information and the public key. The private key is not required for security issues. The certificate provider signs the request, producing a public certificate.

Before issueing the certificate, the provider requests the contact email address from a public *domain name registrar*, and ensures that published address matches with email address provided by the applicant.

So, when a user connects to a website who uses a link such as *https://www.example.com*, if the browser does not give any certificate warning message, then the user is good to go.

3.2. Public Key

Public key is very familiar notion in cryptography. It is a public value that is used for two main purposes: *authenticating* messages or other data originated with a holder of the paired private key; *encrypting* a message to ensure that only the holder of the corresponding private key can decrypt it.

3.2.1. Public Key Infrastructure (PKI)

A public key infrastructure supports the distribution and identification of public key encryption, enabling users to securely exchange data over network and verify the identity of the other party.

In other words, PKI is an arrangement that binds public keys with respective identities of entities. The binding is established through a process of registration and issuance of certificates at and by a CA. During registration process, *registration authority* (RA) makes sure that the registration is valid and correct. RA is responsible for accepting requests for digital certificates and authenticating the entity making the request.

A typical PKI consists of hardware, software, policies and standards to manage the creation, administration, distribution and revokation of keys and digital certificates.

3.2.2. Public Key Cryptography

Also known as *Asymmetric Cryptography*, it is a cryptographic technique that uses private and public keys to encrypt and decrypt data. The keys are not identical large value data, usually, 128 or 256-bit strings generated by random generator methods. They are mathematically linked between them.

The public key is meant to be shared, while the private key must be kept secure.

Using this technique, everyone can encrypt a message or data using the public key of the receiver, but that encrypted message or data can only be decrypted with the private key.

Unlike *symmetric key algorithms*, public key algorithms does not require a secure channel to exchange keys between communicating parties.

Authentication of messages is done by hashing messages to produce a unique value of the message, which is encrypted using the private key and produces a digital signature.

There are several manners to verify the signature, as mentioned in the sections above.

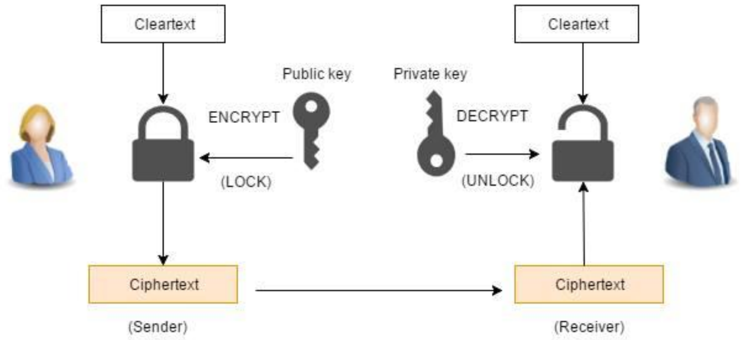

Figure 1: Encroytion/Decryption process using Public/Private Key

4. COMPARISON

In this section, readers will have the chance to read and see comparison between traditional and digital signatures, and also the comparison between digital signature and digital certificate.

4.1. Comparison Between Digital and Traditional Signature

A person’s signature is a very personal thing. Unique to handwriting, it may be the full name, a portion of the name or just the initials, but it can also include various loops and flourishes.

Like digital signature, the traditional one is developed as a way to create a unique identifier for each community member. For the most part, they are associated with written documents, although they may be added to just about anything. When they are added to paper, their main purpose is to signify some kind of approval or consent to what has been captured on that document.

However, adding signature to documents in not the perfect signature solution, because they can be very easily forged or copied. For example, Joseph Cosey was a famous forger that mastered the signatures of many famous figures, including Ben Franklin. Today, his forgeries are as famous as originals he doubled.

Below this paragraph is represented a table of comparison between digital and traditional (paper) signature.

Table 1: Comparison table of signatures

Property	Traditional	Digital
Can be applied to electronic documents and transactions	No	Yes
Signature verification can be automated	No	Yes
Signature automatically detects alterations to the document	No	Yes
Can be used to signify a commitment to a contract or document	Yes	Yes
Can be augmented by use of a witness to the signature process	Yes	Yes
Recognized by legislation	Yes	Yes

4.2. Comparison Between Digital Certificate and Digital Signature

Digital signature is a mechanism that is used to verify that a particular digital document or message is authentic, whereas digital certificates are used mainly in websites to increase their trustworthiness to its users. When digital certificates are used, the assurance is mainly dependent on the assurance provided by the CA. With digital signatures, the receiver of the message can verify that the information is from a trusted sender or is not modified.

5. RESULTS

Although digital certificates are widely used by large corporations, the practices may not be totally secure. Even though these certificates guarantee equity for the user of a website, the relation between the certificate owner, website operator and website owner might be ambiguous and thus, not guaranteed. Researches and studies have proven that authentication and authorization should be separated, although digital certificates adapt information with authorization inside their scope.

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit.

In some countries, including the United States, India, and members of the European Union, electronic signatures have legal significance. However, laws concerning electronic signatures do not always make clear whether they are digital cryptographic signatures in the sense used here, leaving the legal definition, and so their importance, somewhat confused.

Digital signature scheme is secure because these schemes are based in encryption supported in a secure way by concrete algorithms. The most common algorithm for digital signature should provide assurance that the signature guarantees non – repudiation, non – recidivist and the message can’t be changed. For furthermore, the signature should be able to resist all possible attacks.

6. CONCLUSION

After the effort put on this paper, we can freely say that security in electronic communicating is improving in a good rate, but there are a lot of things that require much more work and attention.

Cryptography may be a trending technology, but since security is an issue that lacks from humans, it is only as good as the practices of the people who are in touch with it. Normal users write keys everywhere, choose easy-to-remember ones or don’t even change them for life. The complexity of cryptography effectively puts it outside of most people, and thus, motivation for the practices of cryptographic security is missing.

ACKNOWLEDGMENT

We are pleased to acknowledge all the friends and colleagues for their endless support, our families also, and everyone contributed on finishing this research.

We are also very thankful to ICSD Organization Committee for making this conference possible.

Thank you!

REFERENCES

[1] H. Delfs and H. Knebl, Introduction to Cryptography: Principles and Aplications, Berlin: Springer, 2015.

[2] F. Idrizi, "Kriptografia e kombinuar si mjet per sigurine e transaksioneve elektronike ne Republiken e Maqedonise," 2013.

[3] J. Talbot and D. Welsh, Complexity and Cryptography: An Introduction, Cambridge University Press, 2006.

[4] R. Oppliger, Contemporary Cryptography, Norwood, 2005.

[5] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography.

[6] O. Goldreich, Foundations of Cryptography - A Primer, Hanover.

[7] W. Stallings, Cryptography and Network Security: Principles and Practies, 4th Edition, Prentice Hall, 2005.