I.J.E.M.S., VOL.3(2) 2012: 115 - 118 ISSN 2229-600X

INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES

www.scienceandnature.org

DIGITAL SIGNATURE

***Yadav Priyanka , Srivastava Sindhu & Trehan Vani**
Department of Computer Science, Dronacharya College of Engineering ,Gurgaon, Haryana

ABSTRACT
The Information Technology Act 2000 (IT Act) dictates digital signatures as a means of authentication and security of electronic documents. Digital signature is an electronic token that creates binding between an entity and a data record. They serve the purpose of validation and authentication of electronic documents .Validation refers to the process of certifying the contents of the document, while authentication refers to the process of certifying the sender of the document. It can be said that a digital signature is an electronic version of a handwritten signature. The signing process is implemented with the help of public key cryptography; the signatory uses her private key to create a digital signature for a document. It is used to ensure that the original content of the message or document that has been sent is unchanged. Its varied nature has provided easy, faster, accurate and convenient mechanism for creating, storing, transmission and retrieval of data without involving traditional paper based formalities. This has increased the use of digital technology in day to day life which has led the world to go online that in turn has increased techno-dependency. Increasingly the business dealings, communication, official data and commercial transactions are being carried out in cyberspace. There has been transformation of world from paper based to digital based work. In the last few years, there has been a rapidly growing demand for a working digital signature framework for both public and public sector. The study revolves around the maximum information on digital signature, the future of Information Technology.

KEYWORDS: Non Repudiation, Encryption, Authentication, Hash Function, Key-Pair, Information Technology, Recognition.

INTRODUCTION

Authentication, repudiation and verification of electronic data is important for any electronic transactions. Therefore, unless these objectives have not been achieved, the authentication and secure electronic transaction will merely remain virtual. In order to achieve the authentication and security of electronic data the mechanism of digital signature is used. Digital signature can be described as a method of authenticating data i.e. to verify that the received document is indeed from the claimed sender and its content has not been altered in any way since the person has created it.

Just as the stamps, seal or signature play role in traditional system to create the authentication of paper document, the digital signature plays the role of authenticating the electronic record. It creates the authenticity of any electronic record which subscriber of digital signature wants to be authenticated the electronic record by affixing his digital signature. The signature is an unforgeable piece of data attesting that a named person wrote or otherwise agreed to the document to which the signature is attached. It performs Signer Authentication, Message authentication and Verification.

DIGITAL SIGNATURE–NECESSITY AND OBJECTIVES

Digital Signature is created with the help of cryptographic method. The basic objectives of affixing of 'Digital Signature' are –

Create authenticity of the originator

Digital signature allow the recipient of a message or document to verify the sender. A digital signature is specific for a particular user and thus, a valid digital signature is used to affirm that a message originated from a specific user. So that at any moment after the creation of any digital material, the authenticity of the originator can be verified. It is also essential that at any latter moment, the originator will not capable to deny the creation of document by him

Create authenticity of the document

A digitally signed message or document cannot be altered without invalidating the signature. This is true whether the message is encrypted or not. A valid digital signature upon receipt of a message or document confirms that the message or document was not altered in transit. Any recipient will not be in a state to modify, change, alter, or tamper with the document created by originator. The mechanism should also ensure to the originator that no one else than him will be capable to modify, change, alter or tamper with the document

Non-repudiation

Since a digital signature is the equivalent to a handwritten signature, its use is taken to be a sign of acknowledgement of a message or document. Thus, if someone has digitally signed a document, he or she cannot deny such a document. So, the entire mechanism will ensure that the document and identify mechanism will not play foul and nobody will be in position at any latter moment to deny the responsibility and liability arising out of the document. For originator, that he will not be in position to repudiate what he had created, for recipient, he will not be in position by any means to modify the content created by originator.

BRIEF HISTORY OF DIGITAL SIGNATURE

For centuries, signatures have been the most conventional means of authentication. Roman law documented a combination of seals and signatures as the primary source for authenticating documents and legal contracts. The 1830s saw the first signs of electronic communications and legally recognized "electronic" signatures with the invention of the telegraph and Morse code. But it was the introduction of public key cryptography by Martin Hellman and Whitfield Diffie in 1976 that established the first practical method of distributing cryptographic keys over an unprotected public network.

MECHANISM OF DIGITAL SIGNATURE

Digital signing and signature verification based on public/private key pairs can be done by using public key crypography. Any person can sign a digital message with his private key.

DIGITAL SIGNATURE CREATION

What is needed to create the digital signature

Public keys: The public key certificate creates confirmation of the identity of the signer by using the services of a certificate authority. A certificate authority uses a range of processes to associate a particular public key with an individual. You give your public key to anyone who wants to verify your signature. The combination of your public key and proof of identity result in a public key certificate - also called a signer's certificate.

Private Keys: The private key is something you keep with yourself. You sign a document with your private key. The public and private keys are associated mathematically. Knowing the public key allows a signature to be verified but does not allow new signatures to be created. If your private key is not kept "private," then someone could maliciously create your signature on a document without your consent. It is important to keep your private key secret.

The digital signing process

Step1: Calculate the message digest- A hash-value of the message (often called the message digest) is to be calculated by applying some cryptographic hashing algorithm (for example, MD2, MD4, MD5 or other). The calculated hash-value of a message is a sequence of bits, usually with a fixed length, extracted somehow from the message. The algorithms for message digest calculation apply such mathematical transformations that when just a single bit from the input message is changed, a different digest is obtained. Due to this behavior, it is almost impossible to find out the message itself from a given hash-value of a given message. It is also interesting that theoretically, it is possible for two entirely different messages to have the same hash-value calculated by some hashing algorithm, but the probability for this to happen is so small that in practice it is ignored.

Step 2: Calculate the digital signature-The information obtained from the first step (hash-value of the message) is encrypted with the private key of the person who signs the message and thus an encrypted hash-value called digital signature is obtained. For this purpose, some mathematical cryptographic encrypting algorithm is used. The most often used algorithms are RSA (based on the number theory), DSA (based on the theory of the discrete logarithms), and ECDSA (based on the elliptic curves theory). Often, the digital signature obtained is attached to the message in a special format which can be verified later if it is required.

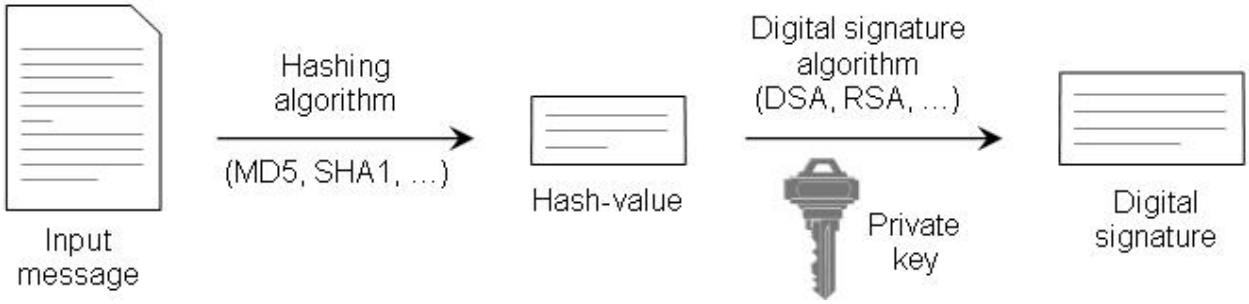

Fig. 1 Digital signature creation process

DIGITAL SIGNATURE VERIFICATION

Digital signature technology permits the recipient of given signed message to verify its real origin and its integrity. The digital signature verification process is purposed to determine if a given message has been signed by the private key that corresponds to a given public key. The digital signature verification process cannot determine whether the given message has been signed by a given person. If we need to examine whether a person has signed a given message, we are required to obtain his real public key in some manner. This is possible either by getting the public key in a secure way (on a floppy disk or CD) or by means of a digital certificate. Without using a secure way to obtain the real public key of given person, it is impossible to check whether the given message is really signed by this person.

Digital verification process

Step 1: Calculate the current hash value- A hash-value of the signed message is calculated. For this, the same hashing algorithm is used as was used during the signing

process. The resultant hash-value is called the **current hash-value** because it is calculated from the current state of the message.

Step 2: Calculate the original Hash-Value- The digital signature is decrypted with the help of same encryption algorithm that was used during the signing process. The decryption is done by the public key that corresponds to the private key that was used during the signing of the message. As a result, we obtain the **original hash-value** (the original message digests).

Step 3: Compare the current and the Original Hash-Values- We compare the current hash-value obtained (from first step) with the original hash-value obtained (from second step), If the two values are same, the verification is successful and proves that the message has been signed with the private key that corresponds to the public key used in the verification process. If the two values are different, this means that the digital signature is invalid and the verification is unsuccessful.

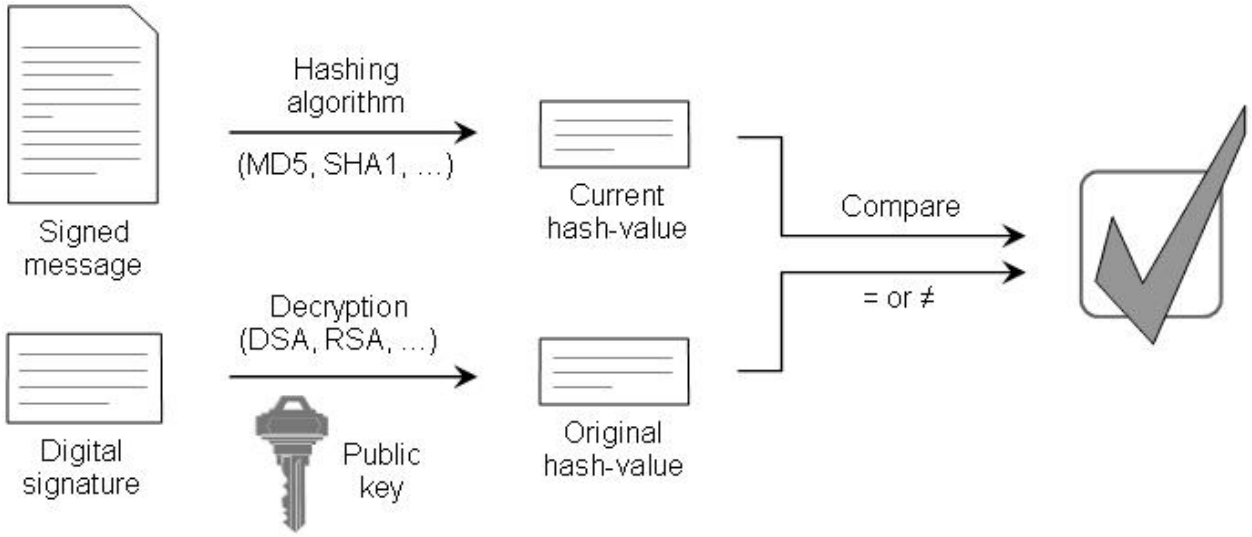

Fig. 2Digital signature verification process

Possible reasons for invalid digital signature

- If the digital signature is changed and decrypted with the public key, then the obtained original value will not be the original hash-value of the original message instead some other value.
- If the message was changed after its signing, the current hash-value obtained from this changed message will be different from the original hash-value because the two different messages correspond to different hash-values.
- If the public key does not match up to the private key used for signing, the original hash-value obtained by decrypting the signature with an incorrect key will not be incorrect.

ADVANTAGES AND DISADVANTAGES OF DIGITAL SIGNATURE

Advantages

- With the use of digital signature we can eliminate the possibility of committing fraud because the digital signature cannot be altered. Moreover the forging signature is impossible.
- By having a digital signature we are proving the document to be valid. We are assuring the recipient that the document is free from forgery or false information.
- Using a digital signature satisfies some type of legal requirement for the document in question. A digital signature takes care of any formal legal aspect of executing the document.
- Includes an automatic date and time stamp, which is critical in business transactions.
- Increases the speed and accuracy of transactions.
- Digital signatures are a computerized form of signature that verifies that a package was sent by a certain individual or business, or that the right person actually signed a document. These signatures are secure and legal, and they can greatly improve your security.

Disadvantages

- Cost-You must have the necessary software to encode the signatures, and if you're using hardware so that customers can sign physically, then the cost goes up even further. Digital signatures are an additional cost that should be weighed against their potential security benefits.
- Training and troubleshooting -If your employees aren't sure how to use a digital signature, then you'll have to spend time training them about how the signature process works. This will take them away from their jobs, costing you money. Additionally, as with all computer-

related applications, sooner or later there will be a hiccups in the system and you'll need someone to troubleshoot. If none of your employees can find and fix the problem, you'll have to hire someone else to do it.

- Necessity-Digital signatures are a great security feature, but that doesn't mean they're a necessary one. If you own a law firm that deals in confidential materials, you might want to invest in a digital signature application for your clients. However, if you own a small family business that deals primarily in cash, you probably don't need it.
- Technological Compatibility - refers to standards and the ability of one digital signature system to "talk" to another. It is difficult to develop standards across a wide user base.
- Security Concerns - These efforts are perpetually hampered by lost or borrowed passwords, theft and tampering, and vulnerable storage and backup facilities.
- Legal Issues - There is clear consensus that digital signature should be legally acceptable. However, many questions remain unanswered in the legal arena.

DIGITAL SIGNATURES IN REAL APPLICATIONS

Progressively, digital signatures are being used in secure e-mail and credit card transactions over the Internet. The two most common secure e-mail systems using digital signatures are Pretty Good Privacy and Secure/Multipurpose Internet Mail Extension. Both these systems support the RSA as well as the DSS-based signatures. The most widely used system for the credit card transactions over the Internet is Secure Electronic Transaction (SET). It consists of a set of security protocols and formats to enable prior existing credit card payment infrastructure to work on the Internet. The digital signature scheme used in SET is similar to the RSA scheme.

CONCLUSION

Many conventional and modern businesses and applications have recently been carrying out enormous amounts of electronic transactions, which have led to a critical need for protecting the information from being maliciously altered, for ensuring the authenticity, and for supporting non repudiation .Just as signatures facilitate validation and verification of the authenticity of paper documents, digital signatures serve the purpose of validation and authentication of electronic documents. It is an essential aspect for creating secure environment for electronic transactions. Digital signature has not only proved an essential techno-legal requirement, but it has made the e-commerce meaningful.

REFERENCES

http://www.developer.com/java/ent/article.php/3092771/How-Digital-Signatures-Work-Digitally-Signing-Messages.htm

Ecommerce - Legal Issuesauthored by Rohas Nagpal.

e-book:http://www.ebooktoyou.net/ebook/digital-signature-download-pdf.php

StallingsW., *Cryptography and Network Security*, 3rd ed. EnglewoodCliffs, NJ: Prentice-Hall, 2002.

FeghhiJ. and P. Williams, *Digital Certificates: Applied Internet Security* 1sted. Reading, MA: Addison-Wesley(1999).

Denning, D.E. Cryptography and Data Security. Reading, MA: Addison-Wesley(1982).

Stallings, W. Cryptography and Network Security: Principles and Practice, 4th ed. Englewood Cliffs, NJ: Prentice Hall(2006).

Practical Security Aspects of Digital Signature Systems: Florian Nentwich, Engin Kirda, and Christopher Kruegel Secure Systems Lab, Technical University Vienna(JUNE-2006).