INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY ISSN: 2456-6683 Volume - 4, Issue - 4, Apr – 2020
Monthly, Peer-Reviewed, Refereed, Indexed Journal Scientific Journal Impact Factor: 5.245
Received on : 30/03/2020 Accepted on : 13/04/2020 Publication Date: 30/04/2020

E-DIGITAL SIGNATURE PROCESSING

[1]Nuha Patel, [2]Prof. Garima Pathak

[1]Student, [2] Assist. Professor
[1, 2] Department of MCA, Parul Institute of Engineering and Technology,
[1, 2] Parul University, Waghodia, India
Email - [1]150510301014@paruluniversity.ac.in, [2]garima.pathak42076@paruluniversity.ac.in

Abstract: *Digital Signature was declared as a medium for authentication and security for the electronic documents by the knowledge Technology Act 2000 (IT Act). Binding of an entity and a knowledge record is made by digital signature which is additionally implies as electronic token. Authentication and validation are served as a purpose by them. The method of corroborating contents of the document refers to validation, while the method of corroborating the sender of the document is referred as authentication. During a way electronic version of handwritten signature is digital signature. With the assistance of Asymmetric Cryptography, signing process is implemented; the digital signature of a document is made by using the private key of the sender. It wants to make sure that the first content of the message or document that has been sent isn't modified. Its diverse nature has provided easy, faster, precise and convenient technique for creating, storing, transmission and recovery of knowledge without including traditional paper based formalities. This has increased the usage of digital technology in lifestyle which has led the planet to travel online that which has inflated techno-dependency. Paper based work has been transformed into digital based work. In both public and personal sector, there has been a rapidly growing demand for a working digital signature framework since previous couple of years. The study is predicated on the utmost information on digital signature which is that the way forward for Information Technology.*

Key Words: *Signature, public key, private key, encryption, authentication, hash value.*

1. INTRODUCTION:

For any electronic transactions, authentication, repudiation and verification of electronic data is vital. Hence, the authentication and secure electronic transaction will merely remain virtual unless these objectives haven't been achieved. The mechanism of digital signature is employed so as to realize the authentication and security of electronic data. Digital signature are often described as a way of authenticating data i.e. to verify that the received document is indeed from the claimed sender and its content has not been modified in any way since the person has created it. The digital signature plays the role of authenticating the electronic record, even as the stamps, seal or signature play role in traditional system to make the authentication of paper document. The authenticity of any electronic record which subscriber of digital signature wants to be authenticated is made and therefore the electronic record by attaching his digital signature. The signature is an unforgettable piece of knowledge verifying that a named person wrote or otherwise agreed to the document to which the signature is attached. Signer Authentication, Message authentication and Verification is performed.

1.1 Brief History of Digital Signature

Only the idea of a digital signature scheme was explained by Whitfield Diffie and Martin Hellman throughout 1976 but they only theorized that such schemes existed.

Soon after that Ronald Rivest, Adi Shamir and Len Adleman devised the RSA algorithm, which could be used to build a kind of primitive digital signature.

The very first widely marketed software package to offer digital signatures was Lotus Notes 1.0, which used the RSA algorithm in 1988.

The ability to embed digital signatures into documents is added to PDF format which in existence on 1999.

The ESIGN Act makes digital signatures legally binding done in 2000.

SIGNiX is established and becomes the most broadly used cloud-based digital signature software in 2002.

According to the International Organization for Standardization (ISO) as ISO 32000 the PDF file format becomes an open standard in 2002 which Includes digital signatures as integral part of format.

1.2 What does Digital Signature contain?

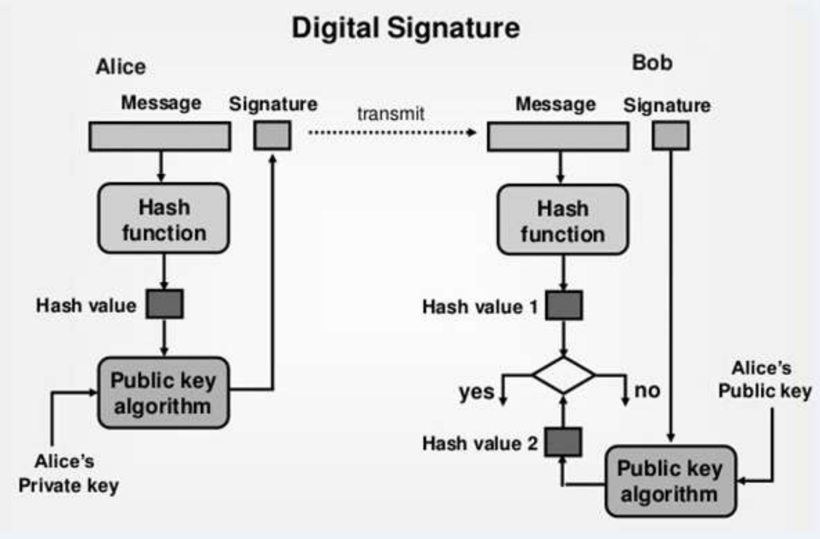

Figure 1

A digital signature scheme consists of 3 algorithms:

1) A key generation algorithm that chooses a private key at random from a set of possible private keys. The algorithm generates the private key and a corresponding public key.
2) A signing algorithm that, given a message and a private key, generates a signature.

A signature verifying algorithm that, given the message, public key and signature, either approves or rejects the message's claim to authenticity.

Two main properties are needed:

1) The authenticity of a signature created from a fixed message and fixed private key can be verified by using the corresponding public key.
2) It should be computationally impossible to generate a valid signature for a party without knowing that party's private key.

A digital signature is an authentication mechanism that allows the sender to attach a code that acts as a signature. The Digital Signature Algorithm (DSA) is an example of a signing algorithm, developed by the National Institute of Standards and Technology.

1.3 Difference between Paper Signatures and Digital Signatures

Parameter	Paper Signatures	Digital Signatures
Authenticity	May be Forged	Cannot be copied
Integrity	Signature Independent of the document	Signature depends on the contents of document
Non-Repudiation	a)Handwriting Expert Needed b)Error Prone	a)Any computer user b)Error free

Table 1

1.4 Application Areas of Digital Signature

Digital Signatures are used in:-

- Electronic Mail
- Data Storage
- Electronic Funds Transfer
- Software Distribution
- Smart Cards
- Integrated Services Digital Network(ISDN)
- Time Stamped Signature
- Blind Signature

1.5 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 modified. Moreover the forging signature is impossible.
- We are proving the document to be valid by having a digital signature. We are ensuring the recipient that the document is free from forgery or false information.
- A digital signature looks after any formal legal aspect of executing the document.
- An automatic date and time stamp, which is critical in business transactions is included. The speed and accuracy of transactions increases.
- Digital signatures are a computerized form of signature that verifies that a message 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 security.

Disadvantages:

- To encode the signatures one must have the necessary software, and if using hardware so that customers can sign physically, then the cost goes up even further. Digital signatures are an additional cost that should be considered against their potential security benefits.
- If the employees aren't sure how to use a digital signature, then one has to spend time training them about how the signature process works. This will take them away from their jobs, costing more money. Additionally, as with all computer- Digital signature 118 related applications, sooner or later there will be a hiccups in the system and someone will be needed to troubleshoot. If none of the employees can find and fix the problem, someone else has to be hired.
- Digital signatures are a great security feature, but that doesn't mean they become necessity. One might want to invest in a digital signature application for your clients, if one owns a law firm that deals in confidential materials. However you probably don't need it, if you own a small family business that deals primarily in cash.
- Technological compatibility refers to standards and the ability of one digital signature system to communicate to another. To develop standards across a wide user base is difficult.
- Efforts are constantly hampered by lost or borrowed passwords, theft and tampering, and vulnerable storage and backup facilities.

2. DIGITAL SIGNATURE CREATION:

2.1 The digital signing process

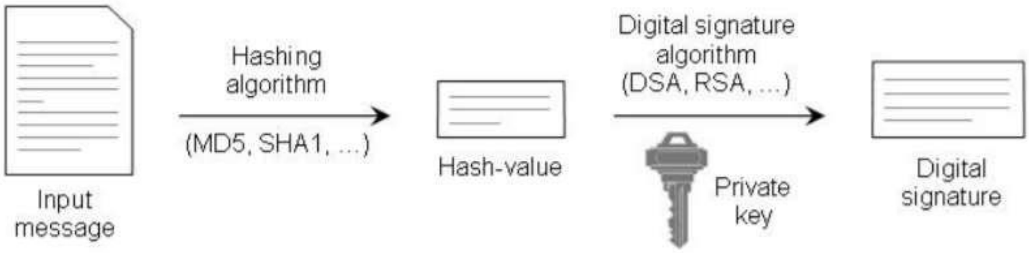

Figure 2

Step1: Calculate the message digest- A hash-value of the message is to be calculated by applying some cryptographic hashing algorithm. The obtained hash value of a message is a sequence of bits, usually with a fixed length, obtained somehow from the message. The algorithms for message digest calculation apply such mathematical transformations that a different hash value is obtained when just a single bit from the input message is changed. Due to this behaviour, it is not possible to find out the message itself from a given hash-value of a given message. It is possible for two entirely different messages to possess an equivalent hash value calculated by some hashing algorithm theoretically, but actually the probability for this to happen is so small that it's ignored.

Step 2: Calculate the digital signature-The hash value obtained from the primary step is encrypted with the private key of the one that signs the message and thus an encrypted hash-value called digital signature is obtained. For this purpose, some mathematical cryptographic encrypting algorithm is employed. The foremost often used algorithms are RSA, DSA, and ECDSA. Often, the digital signature obtained is attached to the message during a special format which may be authenticated later if required.

Received on : 30/03/2020 Accepted on : 13/04/2020 Publication Date: 30/04/2020

2.2 Digital Signature Verification

Digital signature technology permits the receiver of given signed message to verify its real origin and its integrity. The digital signature verification process is purposed to work out if a given message has been signed by the private key that corresponds to a given public key. The digital signature verification process is unable to work out whether the given message has been signed by a given person. If we'd like to see whether an individual has signed a given message, we are required to get his real public key in some manner. This is often possible either by getting the general public key during a secure way or by means of a digital certificate. Without employing a secure thanks to obtain the important public key of given person, it is not possible to see whether the given message is basically signed by this person.

Step 1: Calculate the present hash value- A hash-value of the signed message is calculated. For this, an equivalent hashing algorithm is employed which was used during the signing process. The hash-value obtained is named the present hash value because it is calculated from the present state of the message.

Step 2: Calculate the first Hash-Value- The digital signature is decrypted with the assistance of same encryption algorithm that was used during the signing process. The decryption is completed by the general public key that's associated to the private key used during the signing of the message. As a result, the first hash-value is obtained.

Step 3: Compare the current and the Original Hash Values- The current hash-value obtained (from first step) and the original hash-value obtained (from second step) is compared. If both values are same, the verification is successful and it is proved that the message has been signed with the private key that is associated with the public key used in the verification process and vice versa.

3. CONCLUSION:

Many conventional and modern businesses and applications have recently been completing huge amounts of electronic transactions, which have led to a critical need for shielding the knowledge from being maliciously modified, for ensuring the authenticity, and for supporting non-repudiation. Even as signatures provides validation and verification of the authenticity of paper documents, digital signatures serve the aim of validation and authentication of digital documents. It is a fundamental aspect for creating secure environment for electronic transactions. Digital signature has not only proved an important techno-legal requirement, but it's made the e-commerce meaningful.

REFERENCES:

Journal Papers:

1. Practical Security Aspects of Digital Signature Systems: Florian Nentwich, Engin Kirda, and Christopher Kruegel Secure Systems Lab, Technical University Vienna(JUNE2006).
2. Digital Signature Algorithm Based on Hash Round Function and Self-certified Public Key System by Chen Hai-peng, ShenXuan-jing, Wei Wei, 2009 First International Workshop on Education Technology and Computer Science.
3. A New Conic Curve Digital Signature Scheme by Xiang Can, You Lin, 2009 Fifth International Conference on Information Assurance and Security.
4. ABHISHEK ROY and SUNIL KARFORMA Research Scholar, Dept. Of Computer Science, The University of Burdwan, W.B. (INDIA) J. of Comp. and I.T. Vol. 3(1&2), 45-69 (2012)
   [A survey on digital signatures and its applications]

Web References:

5. www.inf.ed.ac.uk/teaching/courses/cs/1112/lecs/signatures-6up.pdf
6. https://www.signix.com/blog/bid/108804/infographic-the-history-of-digital-signature-technology
7. https://www.slideshare.net/jolly9293/seminar-ppt-on-digital-signature