ABHINAV
International Monthly Refereed Journal of Research In Management & Technology
ISSN – 2320-0073 Volume II, March'13

THE ROLE OF DIGITAL SIGNATURES IN DIGITAL INFORMATION MANAGEMENT

Rachana C. R.

Associate Professor, Pooja Bhagavat Memorial Mahajana PG Centre, Mysore, India
Email: rachanacr@gmail.com

ABSTRACT

Digital signatures are also referred to as electronic signatures, or e-signatures. Digital signatures are often used to implement electronic signatures in a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. Practically speaking, each term refers to an electronic form of consent that authenticates a signer's identity. A digital signature can be thought of as a digitized mark of approval, and is equivalent to a signature made with pen and paper. Digital signature software gives businesses the ability to collect these legally-recognized signatures with more speed and efficiency.

Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. Furthermore, the ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later. It is commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. Digital signatures play a vital role in the organizations since this technology enables the businesses to reduce the human errors, ultimately minimizes the paper work.

Digital signatures enable the businesses to manage their monetary subsidiary and cost of paper work. Also, these signatures help the companies in proving that they are utilizing the green policies and ecofriendly procedures by cutting back the use of paper. This vast technology even reduces the time consumed in sending numerous emails and documents, since the entire work is entitled in few moments. The corporations prove their sharp time management skills through this technology. As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. This article reviews the importance and application of digital signatures.

***Keywords**:* Digital Signatures, Application, E-Governance, Electronic Signatures

INTRODUCTION

The advent of Information Technology revolutionized the whole world and fortunately India led a leading role and captured global attention. India passed Information Technology Act 2000 (The Act) which came into force on 17-10-2000. The Act applies to the whole of India and even to persons who commit offence outside India. The Act validates 'digital signature' and provides for enabling a person to use it just like the traditional signature. The basic purpose of digital signature is not different from our conventional signature. The purpose therefore is to authenticate the document, to identify the person and to make the contents of the document binding on person putting digital signature.

The arrival of digital signatures, and their legalization by Governments all over the world, has marked a new revolution in the world of electronic transactions. Digital Signatures will make business transactions over the Internet easier, and more reliable for businesses and consumers. Digital signatures are used to present any type of digital data, message or file in the form of numbers or mathematical format. It is a technique which is used for verifying the authenticity of the message and the user. It tells the receiver of the message that it has been sent by the known source and it also confirms that file is secure to be explored. They are most often used for the financial dealings and transactions and also in some scenarios where the delivery of information is required to be confidential.

The purpose of digital signature is the same as the handwritten signature. Instead of using pen and paper, a digital signature uses digital keys(public-key cryptology). Like the pen and paper method,a digital signature attaches the identity of the signer to the document and records a binding commitment to the document.The real value is in avoiding the paper and keeping your data electronic.

In addition to improved security, digital signatures provide the following advantages:

1. No need to print out documents for signing;
2. Reduced storage of paper copies;
3. Improved management and access (anytime/anywhere) of electronic versus paper documents;
4. Elimination of need for faxing or overnight mailing—reduction of cycle time;
5. Improved security of document transmission; and
6. Enhanced management processes outside the ''final signature'' step.

Difference between Electronic Signatures and Digital Signatures

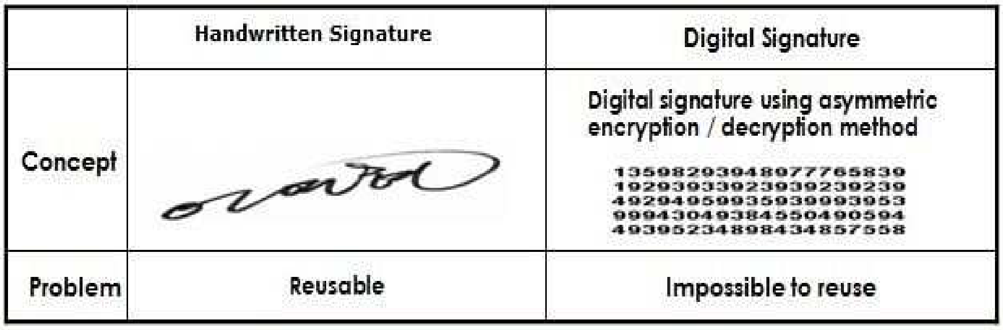
An electronic signature means authentication of an electronic record by a subscriber by means of electronic techniques. An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

Digital signatures go beyond electronic versions of traditional signatures by invoking cryptographic techniques to dramatically increase security and transparency, both of which are critical in establishing a trust and legal validity. As an application of public key cryptography, digital signatures can be applied in many different settings, from a citizen filing an online tax return, to a procurement officer executing a contract with a vendor, to an electronic invoice, to a compliance officer signing an audit log or a software developer publishing updated code.Multiple technologies are available for creating and verifying digital signatures.

Digital Signatures Vs. Ink On Paper Signatures

An ink signature could be replicated from one document to another by copying the image manually or digitally, but to have credible signature copies that can resist some scrutiny is a significant manual or technical skill, and to produce ink signature copies that resist professional scrutiny is very difficult.A handwritten signature scanned and digitally attached with a document does not qualify as a Digital Signature.

A Digital Signature is a combination of 0 & 1s created using crypto algorithms.



	Handwritten Signature	Digital Signature
Concept		Digital signature using asymmetric encryption / decryption method 13598293948977765839 19293933923939239239 49294959935939993953 99943049384550490594 49395234898434857558
Problem	Reusable	Impossible to reuse

Figure 1. Handwritten Versus Digital Signatures

Digital signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Paper contracts sometimes have the ink signature block on the last page, and the previous pages may be replaced after a signature is applied. Digital signatures can be applied to an entire document, such that the digital signature on the last page will indicate tampering if any data on any of the pages have been altered, but this can also be achieved by signing with ink all pages of the contract.

Important paper documents are signed in ink with all involved parties meeting in person, with additional identification forms other than the actual presence (like driver's license, passports, fingerprints, etc.), and most usually with the presence of a respected notary that knows the involved parties, the signing often happens in a building which has security cameras and other forms of identification and physical security. The security that is added by this type of ink on paper signatures cannot be currently matched by digital only signatures.

Overview of How Digital Signatures Work

Digital signatures have been with us since 1976, when Diffie and Hellman introduced the digital signature as an application of public key cryptography.

Figure 2 illustrates the digital signature process. Suppose you want to send a digitally signed document to John. After you create the document, you pass it through a message hash algorithm. The algorithm generates a hash of the document that is a checksum of the contents of the document. You then encrypt the message hash with your private key. The result is a digital signature. You append this digital signature to the document to form a digitally signed document, and then send it to John.

When John receives the document, he passes the document contents through the same message hash algorithm that you used, and creates a new hash. At the same time, John uses your public key to decrypt your digital signature, thereby converting the signature to the original hash. John then compares the newly generated hash and the original hash. If the hashes match, John can be sure that the document he received is really from you and that no one altered it during transmission. If the hashes don't match, John knows that tampering or a transmission error changed the document contents.

The most commonly used message hash algorithms are Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1). MD5 can produce a 128-bit hash, and SHA-1 can produce a 160-bit hash. The hash algorithm is a one-way function that generates a one-way hash. Therefore, no one can derive original document contents from a message hash. The chance that two documents will have the same hash is almost zero. For example, the possibility that MD5 will output the same hash for two different documents is $1/2^{128}$. (2^{128} translates into about 1,500 documents for every square meter of the earth's surface.)

A digital signature is superior to a traditional handwritten signature. A skilled forger can alter the contents of a document with a handwritten signature or move a signature from one document to another without being detected. With digital signature technology, however, any change in a signed document—such as content modification or signature replacement—causes the digital signature verification process to fail.

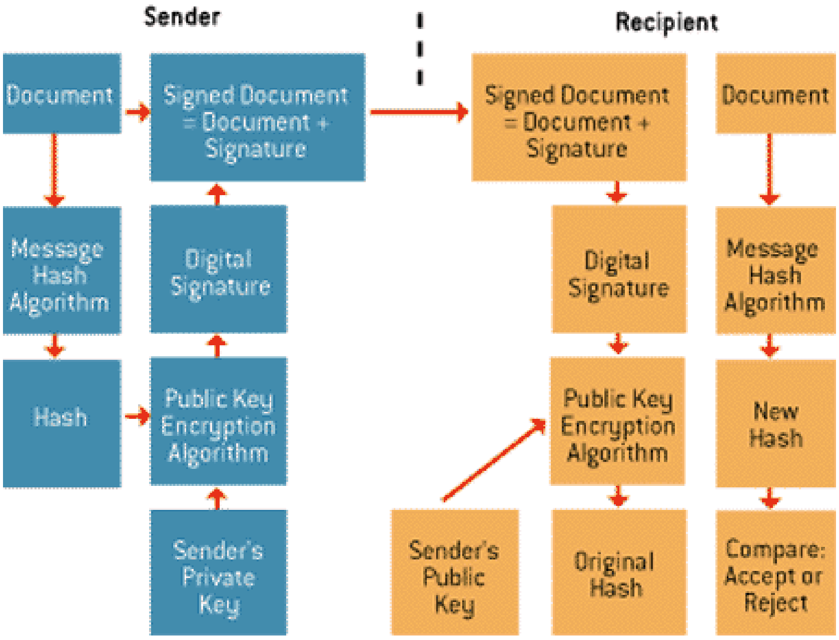


Figure 2. How digital signature works?

Digital Signatures for E-Business

Specifically, Digital Signatures serve three business purposes: Authentication, Data Integrity, and Non-repudiation.

Authentication

Authentication refers to positively establishing an individual's identity in an electronic transaction. Since a digital certificate is issued on proofing by a trusted third party, it unquestionably identifies a person as who he claims to be.

Data integrity

In an electronic transaction, data flows through open networks. It is essential to ensure that data remains intact, and is not tampered with while it passes from the sender to the recipient. Data integrity refers to ensuring that data is in its original form and is not altered in any way en route to the recipient. When digital signatures are applied to data, they are glued in particular manner to the data. Any change in data will remove this binding and render the signature invalid.

Non-repudiation

Now that authentication and data integrity are established, the only thing that remains is to bind signers to the information that they sign. This is exactly like in a real-world business process here once your signature is on a document; you are legally bound to it and its content. Even at a later date, none of the participants in the transaction can deny their involvement.

E-Governance Applications in India using Digital Signatures

The Digital Signature Certificates (DSC) utilized in India effectively serves as the digital equivalent of a hand written signature which has extra data attached electronically to any message or document.

The following are some of the e-Governance applications already using the Digital Signatures:

- MCA21 – a Mission Mode project under NeGP which is one of the first few e-Governance projects under NeGP to successfully implement Digital Signatures in their project.
- Income Tax e-filing
- IRCTC- Indian Railway Catering and Tourism Corporation.
- DGFT- Directorate General of Foreign Trade.
- RBI Applications (SFMS).
- NSDG- National e-Governance Service Delivery Gateway.
- eProcurement
- eOffice
- eDistrict applications of UP, Assam etc.

CHALLENGES AND OPPORTUNITIES

The prospect of fully implementing digital signatures in general commerce presents both benefits and costs. The costs consist mainly of:

- **Institutional overhead**: The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring quality in the performance of their functions.
- **Subscriber and Relying Party Costs**: A digital signer will require software, and will probably have to pay a certification authority some price to issue a certificate.

Hardware to secure the subscriber's private key may also be advisable. Persons relying on digital signatures will incur expenses for verification software and perhaps for access to certificates and certificate revocation lists (CRL) in a repository.

Digital signatures offer a wide range of advantages for business processes. However, organizations need to carefully consider what features are best suited to their individual business needs and then work towards implementing a complete digital signature solution rather than buying different products in a piecemeal manner to address various issues. A complete solution should address application interoperability, browser independence and ease of use.

Digital signatures if properly implemented and utilized offer promising solutions to the problems of:

- **Imposters,** by minimizing the risk of dealing with imposters or persons who attempt to escape responsibility by claiming to have been impersonated;
- **Message integrity**, by minimizing the risk of undetected message tampering and forgery, and of false claims that a message was altered after it was sent;
- **Formal legal requirements**, by strengthening the view that legal requirements of form, such as writing, signature, and an original document, are satisfied, since digital signatures are functionally on a par with, or superior to paper forms; and
- **Open systems**, by retaining a high degree of information security, even for information sent over open, insecure, but inexpensive and widely used channels.

Further, Digital signature, possible now only through computers in India, will soon be provided through mobile phones. The biggest beneficiary of mobile digital signatures would be m-Governance services, as all government services need signatures by citizens while sending their applications to any government department.

CONCLUSION

Digital signatures are a valuable technology for every major corporation. As digital data are not reliable, there are areas where they are not used. Most of all, contracts, receipts, approvals and similar data are almost worthless in a digital form, as they can easily be altered. Hand-made signatures don't change this situation, because it is easy to transfer a signature from one document to another or to modify a document that is signed. The solution for these issues has been around for two decades: digital signatures. Many traditional and newer businesses and applications have recently been carrying out enormous amounts of electronic transactions, which haveled to a critical need for protecting the information from being maliciouslyaltered, for ensuring the authenticity, and for supporting non-repudiation. The digital signature is here to stay and it should. The next challenge, however, is making it easier to get one.

REFERENCES

1. Alok Gupta, Y. Alex Tung, James R. Marsden, "Digital signature: use and modification to achieve success in next generational e-business processes", science direct. http://www-e.uni-magdeburg.de/evans/Journal%20Library/E-business/Digital%20signature%20and%20e-business.pdf

2. Rohas Nagpal, President, Asian School of Cyber Laws, Simple Guide to Digital Signatures, E-book.
3. http://www.digital-signature.com/digital-signature-software-guide/
4. http://technet.microsoft.com/en-us/library/cc962021.aspx
5. http://www.softpanorama.org/Algorithms/Crypto/digital_signatures.shtml
6. http://www.cse.unr.edu/~bebis/CS477/Papers/DigitalSignatures.pdf
7. en.wikipedia.org/wiki/Digital_signature.
8. http://www.windowsitpro.com/content1/topic/digital-signature-technology-4772/catpath/security