



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

A Way for Secure and Authentic Data Transmission

Rituraj Rusia^{1*}, Dr. R. K. Tiwari^{2*}, Pooja Rusia^{3*}

^{1*}Ph.D. (CS) Research Scholar, MGCGVV, Chitrakoot (MP), INDIA

^{2*}Head of Dept. of Physics, Govt. M. S. Golvarkar New Science College, Rewa (MP), INDIA

^{3*} PGDCA, Research Scholar, Satna (MP), INDIA

Abstract: Digital Signature is a way for secure and authentic data transmission. Digital signatures are also known as electronic signatures, e-signatures or e-seal. At present we use electronic information to manage school, college, institute, firm, office, organization, etc. Digital signatures are used to secure our electronic information. Practically we can say that, 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 it is equivalent to a simple hand written signature made by us with a pen and paper. Digital signature software provides security for an electronic information with more speed and efficiency. Digitally signed information can be easily transferred to another place or user. It ensures that the original signed message arrives means that the information cannot be hacked or modified by the hacker. It is widely used for software distribution, fund transactions, and in other cases where it is important to detect forgery or tampering. Digital signatures play a vital role in the organizations, firms and offices. This article reviews the importance and application of digital signatures.

Keywords: Digital Signatures, DSC, Electronic Information, Application, E-Governance, Electronic Signatures.

I. Introduction

At present we are maintaining electronic records as well as manual records in the offices and organizations. Electronic record can easily be retrieved, copied, modified or distributed to more.

Electronic records have the advantage because they are reusable. One can very quickly and easily get a record or copy a new record on the basis of an existing one. This digital advantage is at the same time vulnerability because adaptations or changes are not always observable. Because of this, the reliability of electronic records might be questioned.

Finding methods for reliability of digital documents in general, or electronic records in particular, is the subject of research in various professional fields. At present, one of the most widely suggested solutions is digitally signed electronic records. More specifically, the use of asymmetric cryptography and the digital signature is advanced as a proof of authenticity and integrity for electronic records. This technique might also be usable to ensure the reliability of electronic records [1].

With the development of network and software technology, applications of internet make great influence on traditional working in terms of data or financial transaction. At the same time, E-commerce emerged and developed rapidly, playing great role in business activity. With contrast to traditional business pattern, E-commerce has characteristics of great convenience and high efficiency [2]. Even though, the volume of trade by E-commerce of the whole world today is still little. In E-commerce technology, computer and communication technology are widely used which has a lot of security flaw. In this reason e-commerce needs data integrity, reliability and high security [3]. The data transferred on E-commerce system must have the characteristics of anti-deniability, integrity, security, and identity-authentication. Authenticity and integrity are essential characteristics of a reliable or trustworthy record. Security restricts the development of E-commerce. Digital signature can resolve the problem because of its data integrity protecting and privacy. So digital signature is widely used in E-commerce system [4].

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 technology even reduces the time consumed in sending various emails and documents, since the entire work is performed 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 [5].

The major difference between hand written signature and digital signature is that, the hand written signature can be reusable but digital signature cannot be reusable. Also in the hand written signature has repudiation problem, i.e. in the future sender can refuse for the signature.

Figure 1: Difference between Hand written signature and Digital Signature

	Hand Written Signature	Digital Signature
Concept		101110001101010010 010111010001101010 100010010101010101
Reuse Problem	Reusable	Impossible to reuse.
Authenticity	Some times it is not authenticated.	Yes

In this case the data or electronic transaction is certified and reliability is extremely important. So the way it is proved that the ink of the signature placed on a particular post is authentic document issued by an authorized officer or person, so the authenticity of electronic documents, digital signatures can be perfected through. Thus the digital signature as a way to use the Internet safely is essential in the field of e-governance and e-commerce. This article reviews the importance and application of digital signatures.

II. Characteristics of Digital Signature

It provides authenticity, integrity and non-repudiation.

Authenticity: Digital signature verifies the identity of sender who sent the electronic message or document to us.

Integrity: If a message is digitally signed, any kind of change or modification is not possible. If modification is made by any one, above message will have a new message and digital signature is also needed. It also provides you with a high level of security for your online transactions by ensuring absolute privacy of the information exchanged using a Digital Signature Certificate. You can use certificates to encrypt information such that only the intended recipient can read it.

Non-Repudiation: Sender cannot deny that the message or document is sent by them.

III. Uses of Digital Signature

Digital Signature Certificates are used for the following:

- For sending and receiving digitally signed and encrypted emails.
- For providing online acceptance of a matter or case.
- For online validation of computerized documents.
- For carrying out secure web-based transactions, or to identify other participants of web-based transactions.
- In e-Tendering, e-Procurement, Registrar of Companies e-filing, Income Tax for e-filing income tax returns Applications and also in many other applications.
- For signing documents like MSWord, MS Excel and PDFs.
- For online issuing license, permit, certificate, approval, etc.

Plays an important role in creating a paperless office

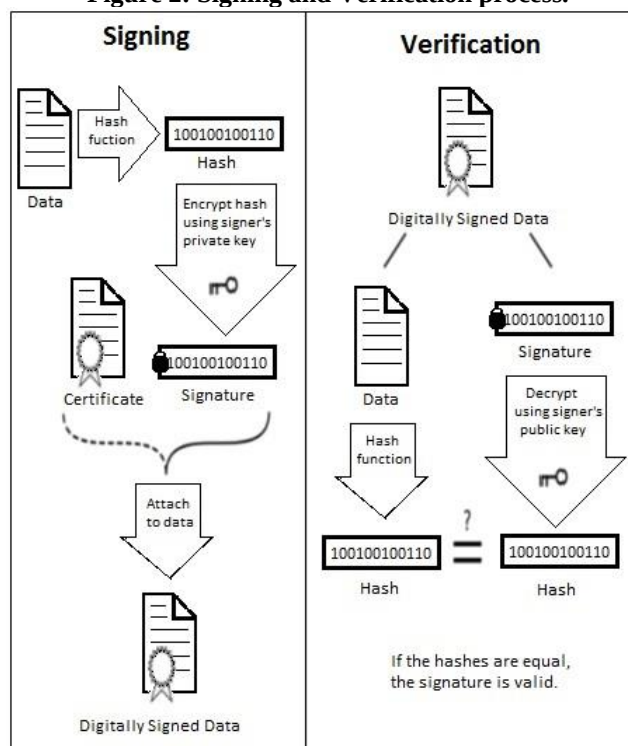
IV. Working process of Digital Signature

A Digital Signature Certificate explicitly associates the identity of an individual/device with a pair of electronic keys - public and private keys - and this association is endorsed by the Certifying Authority. The certificate contains information about a user's identity (for example, their name, pin-code, country, email address, the date the certificate was issued and the name of the Certifying Authority that issued it). These keys complement each other in that one does not function in the absence of the other.

In method of digital signature, two types of keys as 'private key' and 'public key' are used. "Private key is used like a secret password, private key information is only to digital subscribers, while the public key is public, which can be seen on website of Controlling Authority. The document or message is digitally signed, first the 'Hash Value' is produced. 'Hash value' is a numerical unique identification of any document, using the 'private key', message is encrypted.

Private key to encrypt the document, only the partners 'public key' can only be decrypted. Recipients of documents again produced 'hash value' on computer and decrypt the received 'hash value' by sender's public key. If both 'hash value' are the same then it is certain that the document is sent by the person is not fraud. The public key is disseminated with the encrypted information. The authentication process fails if either one of these keys is not available or do not match. This means that the encrypted data cannot be decrypted and therefore, is inaccessible to unauthorized user [6].

Figure 2: Signing and Verification process.



V. Types of Digital Signature Certificate

Class 0 Certificate: These certificates are issued only for demonstration or test purposes.

Class 1 Certificate: Class 1 certificates are issued to individuals or private subscribers. These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.

Class 2 Certificate: These certificates are issued for both business personnel and private individuals' use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.

Class 3 Certificate: These certificates are issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals' only on their personal (physical) appearance before the Certifying Authorities.

VI. E-Governance Applications in India using Digital Signatures

In India, Digital Signature Certificates have got legal recognition which has been described in IT act 2000 and 2002. Therefore Digital Signature Certificates (DSC) are utilized in India effectively like 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:

- e-Panjiyan and e-Stamping department in Madhya Pradesh.
- e-Procurement and e-Auction
- e-Licensing authority
- 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.
- eOffice (for demand, permission, note sheet, acceptance, etc.)
- eDistrict applications of Madhya Pradesh, Uattar Pradesh, Aandhra Pradesh, Assam etc.

VII. Hash algorithm in Digital Signature

Generally MD5, SHA-1 and SHA-2 three types of hash algorithms are used in Digital Signature technology. [7]

Table 1: Types of Hash Algorithm.

Algorithm	Methodology	Output	Time Complex	Logical Operations	Performance
MD5	Divide to 512 bit, 64 times loop	32 Bits	O(n)	AND, OR, NOT, Rotating Shift	Collision After 2006
SHA-1	Divide to 512 bit, 80 times loop	40 Bits	O(n)	AND, OR, NOT, XOR, Rotating Shift	Collision After 2006
SHA-2	Divide to 512 bit, 64 times loop	64 Bits	O(n)	AND, OR, NOT, XOR, Rotating Shift	Without collision

VIII. Conclusion

Digital signature is an important and valuable technology for any type of firm, organization and offices. It provides authenticity, integrity and non-repudiation to the electronic data. It provides a secured and protected data transmission through internet network. It is a substitute of hand written signature. It is very useful for any type of transaction which is related to financial or confidential information. The next challenge, however, is making it easier to get one.

IX. References

- [1] D. PINKAS, Long-term preservation of signed documents, at: e-Archiving for posterity, Leuven, 26 June 2003; S. HACKEL, The ArchiSafe Project - legally secure and scalable long-term record keeping complying with the requirements of the German electronic signature law, at: DLM Forum 2005, Budapest, 6 October 2005.
- [2] Shiyong Zhang [M]: The Principle and Application of Internet Safety, Beijing: Science Press, 2003.
- [3] Bellare M, Miner S K. A Forward-secure Digital Signature Scheme[C]. Proc. of Advances in Cryptology-CRYPTO. 1999:431-448.
- [4] Krawczyk H.: Simple Forward-Secure Signatures from any Signature Scheme[C]. Proc. of the 7th ACM Conference on Computer and Communication Security. 2000-10: 1-4.
- [5] Rachna C. R. : The Role of Digital Signature in digital information management, Abhinav: International Monthly Refereed Journal of Research In Management & Technology, ISSN-2320-0073, Volume-2, March 2013.
- [6] <http://www.osmoindia.com>
- [7] Erfaneh Noroozi, Salwani Mohd Daud, Ali Sabouhi: Secure Digital Signature Schemes Based on Hash Functions, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-4, March 2013.

X. Acknowledgments

First and foremost, we would like to thank to our supervisor of this paper, Dr. R. K. Tiwari, Head of Dept. of Physics, Govt. M. S. Golvarkar New Science College, Rewa for the valuable guidance and advice. He inspired us greatly to work in this paper. We also would like to thanks to Dr. Bharat Mishra, Head of Dept. of Computer Science for guidance and inspiration. Finally, an honorable mention goes to our parents, family members and friends for their understandings and supports on us in completing this project. Additionally, we would like to thank our Almighty God for guiding and giving us natural endowment, skills, healthy mind and body, of whom the researchers are eternally grateful and dedicated having patience to make the research a better one. Without helps of the particular that mentioned above, we would face many difficulties while doing this.