THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 2 | Number 2 Article 4

2007

Information Technology Act 2000 in India - Authentication of E-Documents

R. G. Pawar
Sinhgad Institute of Mgmt., Vadgaon (Bk.)

B. S. Sawant
K. B. P. Institute of Management Studies & Research

A. Kaiwade
Sinhgad Institute of Mgmt., Vadgaon (Bk.)

Recommended Citation

Pawar, R. G.; Sawant, B. S.; and Kaiwade, A. (2007) "Information Technology Act 2000 in India - Authentication of E-Documents," *Journal of Digital Forensics, Security and Law*: Vol. 2 : No. 2 , Article 4.
DOI: https://doi.org/10.15394/jdfsl.2007.1023
Available at: https://commons.erau.edu/jdfsl/vol2/iss2/4

Information Technology Act 2000 in India - Authentication of E-Documents

Prof. R. G. Pawar
Asst. Professor, MCA Dept.,
Sinhgad Institute of Mgmt.,
Vadgaon (Bk.),
Pune (India) – 411 041
http://WWW.Sinhgad.edu
rgpawar@rediffmail.com

Dr. B. S. Sawant
Director, Rayat Shikshan Sanstha's,
K. B. P. Institute of Management Studies & Research,
Satara – 415 001
drbssawant@rediffmail.com

Prof. A. Kaiwade
Lecturer, MCA Dept.,
Sinhgad Institute of Mgmt.,
Vadgaon (Bk.),
Pune (India) – 411 041
http://WWW.Sinhgad.edu

ABSTRACT

The Information Technology Act 2000 has enacted in India on 9th June 2000. This Act has mentioned provision of authentication of electronic document. It is the need of hour at that time that such provision is needed in the Indian Law system, especially for electronic commerce and electronic governance. Electronic commerce", which involve the use of alternatives to paper based methods of communication and storage information. To do electronic commerce there should be authentication of particular document. The working of internet is the documents are traveling in terms of bits from one destination to other destination, through various media like – Co-axial cable, fiber optic, satellite etc. While traveling this document there is probability of making changes in that document by any third party is high or some document may get changed due to noise/disturbance in communication media. This Act required to provide legal recognition carried out by means of electronic data interchange and other means of electronic communication.

In this paper researchers studied technological aspects of Information

Technology Act 2000 like hash function, encryption, decryption, public key, private key etc. and its process. This paper gives details about certifying authority in detail. There should be some mechanism that will take care of document, that what ever the document is received should be the authentic one and it would not get changed in any manner due to any cause.

1. INTRODUCTION

Before 9th June 2000 there was no specially enacted law for the Information Technology. If any offence happens in cyber space then one has to prosecute under “The Indian Penal code 1872”. But due to some new concepts and technology, The Indian Penal code unable to cover the actual requirements of these concepts. So there was need to have some law which will perfect offences like pornography – publishing of information which is obscene in electronic form, hacking with computer system, cyber defamation, cyber stalking, Tampering with computer source documents etc.

2. SIGNIFICANCE

Due to new technology of digital communication any commercial transaction becomes very easy as well as fast. Businesses and consumers are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper document. Information stored in electronic form has many advantages. It is cheaper, easier to store and retrieve as well as to communicate to other. In case of paper based records documents should bear signature for the authentication. The law of Evidence is traditionally based upon paper based records. In electronic commerce paper based transactions are not there then how court will accept it in terms of evidence. For International trade e-commerce is growing rapidly in the last few years and many countries have accepted it and switched over from traditional paper based commerce to e-commerce.

3. NEED OF THE STUDY

Dealing with the e-commerce, the authentication of documents should be there and in this paper we are concentrating the discussion on authentication related topics for electronic documents like digital signature, hash function, encryption, decryption, private key, public key and the available software in the market for doing all things collectively. Anyone can send any document from one place to other. But for authentication, the provision mentioned in Information Technology Act 2000 is that the particular document should be signed by digital signature.

To obtain digital signature that person have to approach to Certifying Authority with the format given in the appendix of Information Technology Act 2000. The form should accompanied with the prescribed fee of Rs. 25,000/-. The Government of India will appoint the Certifying Authority. Any one Indian citizen or person in the eye of law can apply for the digital signature to the

Certifying Authority.

The General Assembly of the United Nations resolved in December 1996 to create the UNCITRAL (United Nations Commission on International Trade Law) with a mandate to promote unification of the law of international trade. The object is to remove unnecessary obstacles to international trade. The UNCITRAL enabled it to formulate International Conventions on Contracts for International Sale of Goods, International Bill of Exchange and International Promissory Notes. Model Laws are the UNCITRAL Model Laws on International Commercial Arbitration, on International Credit Transfers and Procurement of goods. The commission made the following observations:

- The use of automatic data processing (ADP) across the globe in many phases of domestic international trade.
- Authentication of ADP in the international Trade.
- There is a substantial difference in the rules of evidence.
- The developments in the use of ADP require adaptation of existing rules to these developments.

The Commission made the following recommendations to the Governments:

- To bring such changes in the existing rules so that the computers record will be admissible in the court of law,
- The rules framed should be consistent with the technology. These rules should help the courts for the credibility of particular document.
- To enable the parties to prepare the documents in the readable form and to enter into contract.
- To review the legal requirements of authentication in the computer readable format.

The electronic transactions and other parts of the globe are in vogue in India. The increasing growth in the e-commerce the Indian Government has take decision to give legal protection to such transaction. The Indian Parliament passed the Information Technology Act 2000. The objective of this act is:

- To respond to the United Nations call to all states to give favorable consideration to Model Law.
- To provide legal recognition to the transaction done with electronic data interchange (EDI).

4. THE TECHNOLOGICAL ASPECT

4.1 Initiative by International Organizations

Many countries have decided to make laws for the Digital Signature. While

UNCITRAL (United Nations Commission on International Trade Law) is working on to prepare a model for the digital signature. The OECD (Organisation for Economic Co-operation and Development) adopted cryptography as a guideline for the Digital Signature. The member countries of OECD are industrialized one like United States, Canada, European Nations, Japan and Australia. The guidelines aim is to promote cryptography. The following are the guidelines for the same:

1. Trust in Cryptographic Methods - What ever the cryptography method is using it should be trustworthy.
2. Choice of Cryptographic Methods - Users have a liberty to choose any cryptographic method. This method should be subject to relevant law.
3. Market Driven Methods - The methods developed should be as per the need of the society, should support business and Governments.
4. Standards for Cryptographic Methods - Standard methods for cryptography should be developed.
5. Protection of Privacy - The privacy rights of an individual should be protected, as well as personal data and communications should be protected and decide the national policies for cryptographic.
6. National Cryptography Policy - The policy may allow to access cryptographic method by the lawful means.
7. International Co-operation - Governments should avoid creating unjustified obstacles to international trade in the name of enforcing cryptographic policy.

Although the scope for the guidelines may vary form country to country, but initially OECD members have adopted these guidelines and decided to make review of those guidelines by every five years so that international cryptography policy will adopt the new requirements.

4.2 Initiatives by the United States of America

The US have enacted “The Utah Digital Signature Act of 1995” for the framework to use cryptography as a tool for data authentication purpose. Other states like Florida, Washington, Georgia, Hawaii, Oregon and Wyoming have enacted similar bills. Minnesota has established the third party as a Certifying Authority to take legal responsibility of Digital Signature. The Department of Commerce is responsible for licensing cryptographic devices like Automatic Teller Machines (ATMs), Proprietary Software, Access Control etc. As a part of policy US Government has taken upon the initiative, to permit companies to export encryption products using 56-bit Data Encryption Standards (DES).

4.3 Initiatives by the European Union

The European Commission has launched a Study on the Legal Aspects of Digital

Signatures.

4.4 Initiatives by the G-7 Countries

The European Association of Business Machines and Information Technology Industry (EUROBIT), the Information Technology Association of Canada, the Japan Electronic Industry Development Association (JEIDA) and the Information Technology Industry Council of the United States have jointly identified '**Data Security and Privacy**' as the most important parameters upon which the Global Information Infrastructure (GII) should be built.

5. SECURING E-DOCUMENT

It has been realized that Internet being a public network the documentation send from one place to other place with the help of any medium like co-axial cable, fiber optic, satellite communication etc. We cannot assure that the record received by one person is the authentic or it is free from any alterations, deletion, and interception. The reason behind is that we should use such technology that makes communication or transaction legally binding. In order to call it legally binding, it should follow the following three conditions:

Authenticity of the sender to sender who has actually sent the record.

Message's integrity, the recipient must be confidant that the message received by him in not altered or modified en route.

Non-repudiation, the ability to ensure that the sender can not falsely deny the message sent by him, nor falsely deny the content of the message.

Declaration of a few terms:

- Digital Signature: Means authentication of any electronic record by a subscriber by means of an electronic method
- Private Key: Means the key of a key pair used to create a digital signature.
- Public Key: Means the key of a key pair used to verify a digital signature and listed in the digital signature certificate.
- Key Pair: Is an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that public key can verify a digital signature created by the private key.
- Subscriber: Means a person in whose name the Digital Signature Certificate issued.
- Hash Function: An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:- (i) A message yields the same result every time the algorithm is executed using the same message as input. (ii) It is computationally infeasible for a message to be derived or reconstituted from the result produced by the

> algorithm. (iii) It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

The above thing will be satisfied with the acceptance of the cryptography technique. Cryptography has evolved into two Symmetric and Asymmetric cryptography. In symmetric cryptography only one secrete key is used for encryption and decryption. While in asymmetric cryptography two keys one Private key and one Public key i.e. key pair is using. Private key is for encryption and Public key is for decryption. As name indicate Public key is for public use and it is open for all while Private key is confidential it should be kept as a secrete. A Private key is mathematically related to Public key. Private key gives the authenticity of the sender while applying the Public key. The Digital Signature is based on the asymmetric cryptography it gives both keys Private key and Public key. Here these keys will be produced by the Certifying Authority which is the third party. We have to relay on Certifying Authority.

A digital signature is not the signature signed on the paper and makes the digital image of that signature. It is a block of data to be attached to the document and converted it in to another form. This conversion is called as encryption. For digital signature it requires key pair one is Private key and another is Public Key and hash function (algorithm). Digital signature is two way process having two parties:

Signer: Who is creating the digital signature?

Recipient: Who verify the digital signature?

A digital signature is said to be complete if and only if the recipient successfully verifies it.

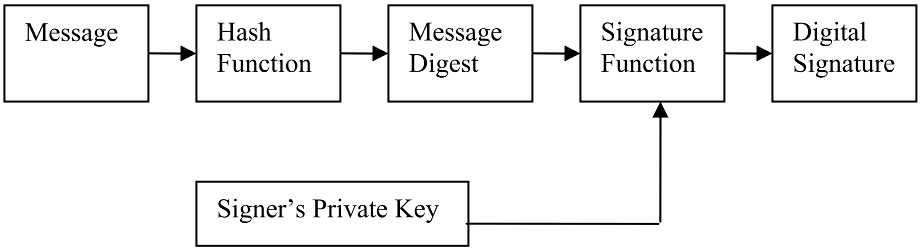

Figure 1. Creating a Digital Signature

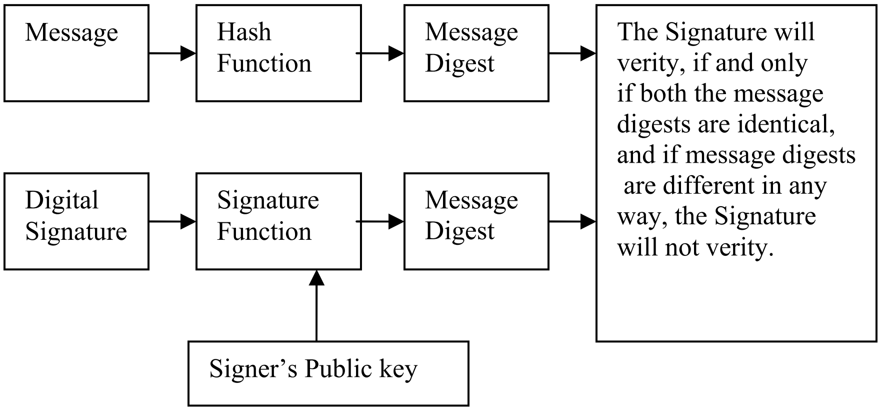
Message
Hash Function
Message Digest
Digital Signature
Signature Function
Message Digest
Signer's Public key
The Signature will verity, if and only if both the message digests are identical, and if message digests are different in any way, the Signature will not verity.

Figure 2. Verifying a Digital Signature

Here receiver receives digital signature and the message. Then the receiver applies signer's public key on the digital signature. Then recovers the hash result (message digest) from the digital signature, as well as computes a new hash result of the original message by means of the same hash function used by the signer to create the digital signature.

Lastly compares the hash results recovered from the first method and the second method. If both the results are same then the verification is done.

In this way the act is enable to make provisions for securing the transactions done with e-commerce

6. CERTIFYING AUTHORITY

The Certifying Authority is a trusted third party which not only authenticates a digital signature but also dispenses the public keys. Its function is to verify and authenticate the identity of a person in whose name the Digital Signature Certificate is issued (a subscriber). The Certifying Authority has first of all apply to Controller of Certifying Authority (CCA), upon certain conditional requirements CCA gives license to Certifying Authority for issuing digital signature as well as public keys.

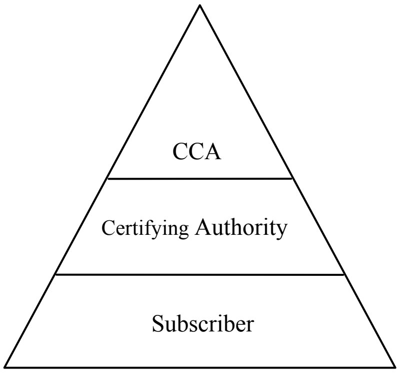

Figure 3. Levels of Hierarchy

The figure shows multi level authorities, often referred to as (PKI) Public Key Infrastructure hierarchy. Here Controller of Certifying Authority is the superior to Certifying Authority. CCA will keep the check on the Certifying Authority, so PKI system is much more than the 'subordinate-superior' relationship between certifying authority and controller. PKI represents a system of creating and authenticating digital binding relationships. PKI is consisting of software, set of policies, processes, sever platforms and workstations used for the purpose of administrating Digital Signature Certificates and public-private key pairs, including the ability to generate, issue, maintain, and revoke public key certificates. This relationship is based on trust. Basically it involves three parties and their relationships are as shown in the figure 4.

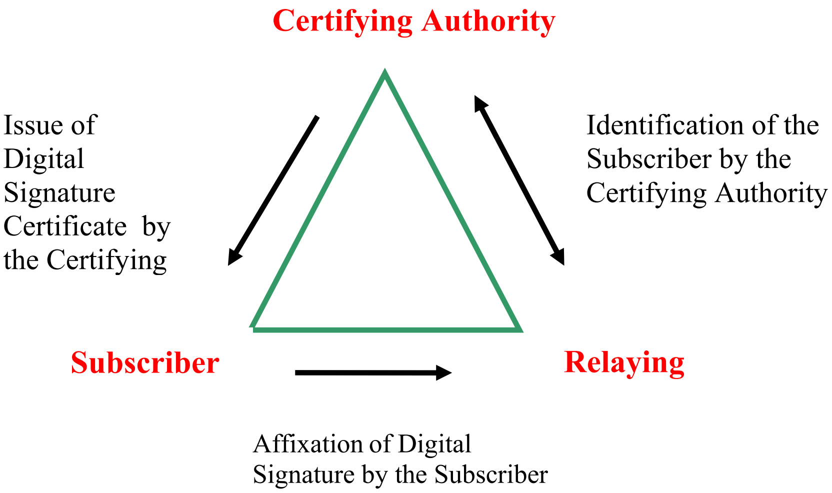
Certifying Authority
Issue of Digital Signature Certificate by the Certifying
Identification of the Subscriber by the Certifying Authority
Subscriber
Relaying
Affixation of Digital Signature by the Subscriber

Figure 4. Relation between CA, Subscriber and Relaying Party

- Subscriber - an individual or entity identified by the certificate.
- Certifying Authority – the issuer of certificate to subscriber.
- Relaying Party – the individual, agency or the company relaying on the certificate.

Here certifying authority is playing 'twin' roles to perform. On one hand, it has to issue digital signature to the subscriber and other hand identify and authenticate the subscriber's information contained in the certificate in the said certificate for the benefit of the relying party. The role of CA is to keep binding relationship between the subscriber and the relying party.

7. CONCLUSION

By knowing all above technological aspects of authentication of any document which is traversing from one place to other and those aspects are covered in the Information Technology Act 2000. We come to the conclusion that the act has taken sufficient precautions for the authentication of any document even though it is traveling from various Medias like co-axial, fiber optic or satellite. Even though anybody intentionally does any thing while traversing at the receiving end it will easily detect that there is some change in the document and the document is not properly received or some noise has occurred or the document received is not from the particular person. So we conclude that "The Information Technology Act 2000" has taken proper require steps to authenticate a particular electronic document.

8. BIBLIOGRAPHY

1. Dr. Farooq Ahmad, "Cyber Law in India", Pioneer Books, Page 27 to 32.
2. Suresh T Vishwanathan, "The Indian Cyber Law with the Information Technology Act, 2000", Bharat Law House Pvt. Ltd., New Delhi-83.
3. Vakul Sharma, "Information Technology Law & Practice", Universal Law Publishing Co. Pvt. Ltd., Page 29-31.
4. Bare Act, "The Information Technology Act, 2000", Professional Book Publishers, New Delhi
5. Vaishali Bhagwat, "Law of Cyber Crimes in India".
6. Information Technology Act, 2000 – A Contractual Perspective by Devadatt Kamat.
7. Vishikha Jogwar, "E-Governance: Need of 21st Century", SIOM:IT UPDATES – 2K6, Page 76-80, February 2006, Pune – 41.
8. Timmers Paul "Electronic Commerce – Strategies and Models for Business-to-Business Trading", John Wiley and Sons Ltd., New York, 1999.

9. Supreme Court Yearly Digest, Eastern Book Company, Lucknow, 1996-2002.
10. Lutzker, Arnold P., "Copyrights and Trademarks for Media Professionals", Focal Press, Oxford, 1997.
11. Rodney D. Ryder, "Guide to Cyber Laws" 2nd Edition Reprint, Wadhwa and Company Nagpur, 2005.
12. Reed Chris, "Internet Law, Text and Materials", Butterworths, London, 2000.
13. Black's Law Dictionary, 6th Ed., 1990.
14. Bainbridge, D. "Software Copyright Law", 4th Ed., Butterworths, Lonson,1999.
15. Cracknell, D.G.(Ed.) "Obligations : Contract Law", Old bailey Press, London, 1998.
16. Nicholas B. "French law of contract", Butterworths, 1982.
17. P. Narayanan, "Intellectual Property Law", 3rd Ed.., Eastern Law House, New Delhi, 2005.
18. Lutzker, Arnold P., "Copyrights and Trademarks for Media Professionals", Focal Press, Oxford, 1997.
19. Narain, Pradeep, "A Handbook on Taxation of Non-Residents", Asia Law House, Hyderabad, 2002.
20. Norton's Peter: "Introduction to Computers", Tata McGraw-Hill, New Delhi,1998.
21. Ratanlal & Dhirajlal, "The Indian Penal Code", 28th Ed.., Wadhwa, Nagpur, 2002.
22. Soni Ashok, "Digest of Cases on Law of Contract", Universal Law Publishing Co. Pvt. Ltd., 2002.