"E-Signature"

Prof. Kavita Kumari

** SD College/Dept. Of Computer Science and Applications, Ambala Cantt*

***Abstract*— In E-governance large amount of packets would be transferred using internet which is unsecure and time consuming. Intruders can change the information according to their requirements. So to ensure speedy communication and reduce the unauthorized access through information and communication technologies(ICT), it is required to use some techniques impose data Integrity, Privacy and Authenticity which must maintained with less communication costs using available bandwidth.**

The success rate of various electronic mechanisms depends on how securely and authentically data is being transmitted between the users at sending end and the users at receiving end. To attain the authenticity of digital documents, it must be digitally signed by its original sender. This paper made a study of e-signature schemes and tools.

I. INTRODUCTION

Applications like banking, stock trading, and the sale and purchase of goods are increasingly emphasizing electronic transactions to minimize operational costs. This has led to phenomenal increase in the amounts of electronic documents that are generated, processed, and stored in computers and transmitted over internet. This electronic information that we used to send is valuable and sensitive and must be protected against tampering by malicious third parties (who are neither the senders nor the recipients of the information).

There is a need to prevent some important information (in the form of some document such as business contracts) or items related to it (such as date/time it was created, sent, and received) from being tampered with by the sender (originator) and/or the recipient.

Traditionally, paper documents are validated and certified by written signatures, which work fairly well as a means of providing authenticity. For electronic documents, a similar mechanism is necessary. The concept of E- Signature is very much similar with the conventional signatures which are used to prove the originality of the document so that a recipient has a reason to believe that the document was send by the actual sender and was not distorted during transmission over networks.

E-signatures are somewhat similar to Digital Signatures and based on traditional pen-paper signature scheme. It serve the purpose of validation and authentication of electronic documents.

Validation refers to the process of certifying the contents of the document.

Authentication refers to the process of certifying the sender of the document.

II. NEED OF E-SIGNATURES

The traditional signatures are hand written and are uniquely representative of one's identity. The use of signature is mandatory in law in certain cases and holds an important legal position in the document as it signify two things, the identity of the person and its intent to it. The Signature is one's identity on a document and is used in day to day transaction and in case of illiterate persons its fingerprint is considered as his signature. The handwritten signature is prone to forgery and tampering hence insufficient for online transaction and contracts. The online transaction requires unique and strong protection which is served by electronic signatures.

III. TECHNICAL ASPECTS OF E-SIGNATURE

The E-signature is created and verified by using the Public Key Infrastructure (PKI) technology that requires two keys that is a public key and a private key for encrypting and decrypting the information.

The message is encrypted with a public key can only be decrypted using the corresponding private key and vice versa. The unique feature in public key infrastructure is that the public and private keys are related to each other and only the public key can be used for encrypting messages that can be decrypted using the corresponding private key. The public key is shared, whereas the private key is known only to its possessor.

The digital signature is based on Cryptography. Cryptography is the science to secure communications by converting the message (encrypting) into an unreadable format and only the person with a secret key can decrypt (read) it. Cryptography systems can be broadly classified into two types i.e., symmetric-key and asymmetric.

In symmetric systems, both the sender and recipient have same keys and asymmetric system each user has two keys a public key that is known to everyone and a private key that is known only the recipient of messages. In India signature uses an asymmetric system that has a public key and private key.

IV. LEGAL ASPECTS OF E-SIGNATURE

The concept of electronic signature was introduced under section 3A of the Information Technology (Amendment) Act 2008. An electronic signature means authentication of an electronic record by a subscriber by any means of electronic authentication techniques. An electronic signature technique can be used as an authorized electronic signature if such technique is notified by the central government in the official gazette or in the second schedule of the Act.

Legally, an electronic Signature shall be considered as reliable if it fulfills following requirements:

1) The technique should be such that it can be linked to the creator of the message.
2) The technique of electronic signature must be under the control of the maker of the signature.
3) Any change or alteration to the electronic signature after affixation must be detectable.
4) Any change or alteration of data after affixing electronic signature must be detectable.

The digital signature was introduced through Information Technology Act 2000 in India, which is enhanced with hybrid concept of electronic signature which is based on UNCITRAL Model Law on Electronic Signatures 2001. The electronic signature is a technologically neutral concept and includes a digital signature. The object and purpose of electronic signature are similar to that of traditional signature.

The purpose of UNCITRAL Model Law on Electronic Signatures 2001 provides following statement which signifies the importance of electronic signature.

"The increased use of electronic authentication techniques as substitutes for handwritten signatures and other traditional authentication procedures has suggested the need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques (which may be referred to generally as "electronic signatures"). The risk that diverging legislative approaches be taken in various countries with respect to electronic signatures calls for uniform legislative provisions to establish the basic rules of what is inherently an international phenomenon, where legal harmony as well as technical interoperability is a desirable objective."

Sec 2 (ta) of Information Technology Act 2000 had defines electronic signature as:

"Authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature."

The definition of electronic signature includes digital signature and other electronic technique which may be specified in the second schedule of the Act, thus an electronic signature means authentication of an electronic record by a subscriber by means of electronic techniques. The adoption of 'electronic signature' has made the Act technological neutral as it recognizes both the digital signature method based on cryptography technique and electronic signature using other technologies.

It prescribes the use of an asymmetric crypto system and hash function for authentication of electronic records. Authentication of an electronic document is important as it ensures that the message has not been tampered and confirms the creator's identity, making it non reputable, i.e., the sender cannot deny its creation. The object of authentication is achieved by the use of asymmetric system and hash function which convent the electronic message into an unreadable format to prevent tampering.

A hash function is the method or scheme used for encrypting and decrypts digital signatures. A hash function produces a hash value which is also known as a message digest. It plays an important role in ensuring that the message has not been tampered and information is safe and secure. Among the commonly used hash functions in practice are MD-5 (message digest 5) and SHA (secure ash algorithm).These algorithms are fairly sophisticated and ensure that it is highly improbable for two different messages to be mapped to the same hash value.

V. OFFENSES RELATED TO ELECTRONIC SIGNATURE

The offenses related to electronic signature are generally related identity theft, publication of false electronic signature certificate, publication of electronic certificate with fraudulent purpose. Section 66C of the Act punishes for identity theft. This Act punishes fraudulent use of electronic signature of any other person and such person shall be punished with imprisonment of up to three years and will also liable to pay fines which may extend upto 1 lakh.

Misrepresentation or suppression of material fact in order to obtain any license or electronic signature is an offense under section 71 of the Act. This section is applicable in following cases:

1) If a person makes a misrepresentation to the Controller or Certifying authority.
2) If a person suppresses any material fact from, the Controller or Certifying authority.

Such misrepresentation or suppression of material fact with the intent to obtain any license or electronic certificate from, the Controller or Certifying authority is punishable with imprisonment of up to two years and fine up to rupees one lakh. The information to be provided to the Controller or Certifying authority should be proper and correct and presentation of wrong, incorrect or false information is an offense under Section 71 of the Act.

Publication of electronic signature certificate which is false in certain particulars is an offense under section 73 of the Act. The following shall amount to publication of false particulars in an electronic certificate:

(i) Publication of Electronic signature certificate which the certifying authority has not issued.
(ii) Publication of Electronic signature certificate which subscriber of the certificate has not accepted.

(iii) Publication of Electronic signature certificate which is revoked or suspended.

Sec 74 of the Act punishes creation, publication or providing of electronic signature certificate for fraudulent or unlawful purpose with imprisonment for a term which may extend up to two years or a fine which may extend up to one lakh.

VI. E- SIGNATURE SOFTWARES

Two major challenges involved while using electronic signatures:

1) Authentication of user

2) Trusted method of signing

Aadhaar based authentication is carried out to address the first challenge and for addressing the other one Authorized Electronic Signature Software is used.

There are many companies that provide Electronic signature technology and Digital Transaction Management services for facilitating electronic exchange of signed documents. Some of them are:

- DocuSign
- e-hastakshar:C-DAC's Online Digital Signing Service
- eSign Genie
- GlobalSign
- RightSignature
- RMail
- eSignLive
- SignNow and many more.

Services by these companies are offered either by subscription or free as an App. Signatures and documents are encrypted after it has been uploaded. Each party must agree to review the document and apply the signature. Signature may be added from a stored copy of a signature or generated automatically by the software itself. Phone confirmation and background checks are also offered as premium services.

VII. HOW E-SIGNATURES SOFTWARE WORKS

1) Step1-User Subscription: User who needs their documents to authenticate must get a Digital Certificate by subscribing themselves to some authorized e-sign software company. This helps to verify the identity of user.

2) Step 2-Upload the document: After subscription it simply ask to upload the document (word document, PDF etc) which user wants to authenticate.

3) Step3-Indicate who needs to sign: Next we need to add the names and email addresses of the recipients.

4) Step4-Locate the signature place: Specify where you need a signature, initial, or date. Here the signatures can be automatically generated or user specified. Link the Signature with the document and Send.

VIII. BENEFITS OF E-SIGNATURE

A digital Signature has the same function as that of a handwritten signature. The Information Technology Act 2000 provides the required legal sanctity to digital signatures based on asymmetric crypto systems.

A. Secure Online Services

Document sent via courier or in person could be tampered with on the way but when sent using Digital signature it gets encrypted. Also document can effortlessly track and located in few minutes. Even the sender is authorized via third party verification entity known as Certificate Authority.

B. Enhance Customer Relationships

Digital methods provide a clear audit trail to minimize the risk of fraud and compliance issues. Unlike a traditional ink on paper signature, an e-signature is impossible to forge when combined with strong user authentication options. Digital solutions also provide clear proof of signer identity and show the document has not changed since it was signed. This lead to enhance the customer relationships.

C. Increase Speed and Reduce cost of sending Documents

Digital signatures save time, money and effort. It sends the documents in more secured way as compared to general courier services. For e.g. Business contracts are easily written, completed and signed by concerned parties in a little amount of time which results in reduced cost of sending documents.

D. Authentic ity

An electronic document signed with a digital signature can stand up in court just as well as any other signed paper document.

E. Imposter Prevention

No one else can forge the user digital signature or submit an electronic document falsely.

IX. DISADVANTAGES OF DIGITAL SIGNATURE

Just like all other electronic products, e-signatures have some disadvantages. These include:

A. Expiry

E-signatures, like all technological products, are highly dependent on the technology it is based on. In this era of fast technological advancements, many of these tech products have a short shelf life.

B. Certificates

In order to effectively use digital signatures, both senders and recipients may have to buy digital certificates at a cost from trusted certification authorities.

C. Software

To work with digital certificates, senders and recipients have to buy verification software at a cost.

D. Law

In some states and countries, laws regarding cyber and technology-based issues are weak or even non-existent. Trading in such jurisdictions becomes very risky for those who use digitally signed electronic documents.

E. Compatibility

There are many different digital signature standards and most of them are incompatible with each other and this complicates the sharing of digitally signed documents.

X. CONCLUSION

The growing online transactions and contracts require stronger protection which is currently fulfilled by electronic signature. Most businesses today are embracing the idea of paper-less offices. To do that, they have identified what is a digital signature and the advantages of using them. They are now using digital signatures to authenticate important documents and make legally binding agreements. They are looking for multiple method of authentication like the use of fingerprint. The multiple methods would permit easy identification of persons which will assist in curbing online frauds and ease online transaction and further enhance online security of users as to even today the factual identity of persons online is a mirage.

REFERENCES

[1] W. Stallings, Cryptography andNetwork Security, 3rd ed. Englewood Cliffs, NJ: Prentice-Hall, 2002.

[2] C.P. Pfleeger and S.L. Pfleeger, Security in Computing, 3rd ed. Englewood Cliffs, NJ: Prentice-Hall, 2002.

[3] Prabhu C.S.R " E-Governance concept and Case studies", PHI Learning Pvt Ltd,2009

[4] https://www.pcmag.com/business/directoty/electronic-signature

[5] www.pcworld.com

[6] JohnAngel"Electronic Law Journals",JILT,UK

[7] https://www.docusign.in