DIGITAL AND ELECTRONIC SIGNATURES- KEYS TO THE GLOBALIZED WORLD

Nagarjun K.B.

C.B.R. National College of Law, Karnataka

In the age of rapid growth and technological advancement, securing and maintaining confidentiality have become vital focal points. While globalization has led to digitization, this in turn has led to the advent of modern approaches through new forays of scientific research. Privacy and security concerns regarding access to sensitive or particular information has to be looked into specifically. Therefore, a very useful tool in so far as to digital communication is the digital and electronic signature. Digital and electronic signatures have been serving the purpose of an end-to-end encryption in communication of information and this has been squarely applied by consistent efforts to increase accountability. Verification of the contents and also the identity of the individual transmitting such information electronically has become its prominent feature. Legal ramifications are of major concern as this field indulges both into digital security and privacy, which are both novel and concomitant concepts. Hence knowledge and application of laws pertaining to this has become important. Every field has its own set of goals and challenges and hence a holistic approach is the need of the hour.

Introduction

A new era of information dissemination where swift exchange is pivotal, security of such information is also an important aspect. Digital and electronic signatures have become a means to reach a common goal of cyber protection. The traditional form of signatures is mainly handwritten and is unique to each individual. Signing the document is a social affair and not a scientific one. Document signing is an act upon which person shows consent to the contents of the document and another checks this confirmation implying reception. Any evidence that implies on such commitment is subject to question and doubt; in other words, signing documents involves considerable risk factor attached to it.

Meaning

Digital or e-signatures as they are widely known have the intent to verify and authenticate the substance of information. It is a digital code (generated and authenticated by public key encryption), which is attached to an electronically transmitted document to verify its contents and the sender's identity. It is a binary code that, like a handwritten signature, authenticates and executes a document and identifies the signatory. A digital signature is practically impossible to forge and cannot be sent by itself but only as a part of an electronic document.

UNCITRAL Model Law on Electronic Signatures 2001[1]

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. 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."

Section 2 (ta) of Information Technology Act 2008 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."

Section 2(p) defines Digital Signature as means of authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section.

Brief History on Digital Signatures

A *digital signature* is the term used for marking or signing an electronic document, by a process meant to be analogous to paper signatures, but which makes use of a technology known as public-key cryptography. The majority of early on personal plans had been of the comparable type as they call for conditions trapdoor permutation, such as the RSA perform, or perhaps in true with the Rabin personal system, computing rectangular modulo amalgamated. A trapdoor permutation family is a family group associated with permutations, particular by a parameter, that is simple to work out inside the forward route, yet is hard in order to figure out inside the invert path with no by now knowing the private essential.[2]

In India, MCA-21 program launched by the Ministry of Corporate Affairs (MCA) really revolutionized the use of digital signature by making E-filing mandatory for most of the documents required to be filed under the Companies Act 1956 and under the Limited Liability Partnership Act 2008 (LLP Act). The Income tax department followed suit and provided compulsory filing of returns in the electronic mode except a few under the Income Tax Act 1961. The Central Excise Act and Finance Act 1994 (dealing with service tax) also provides schemes for E-filing. Now the application for registration under Foreign Contribution Regulations Act provides that it shall be filed electronically. The application

[1] *UNCITRAL Model Law on Electronic Signatures*
https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

[2] *Digital Signatures – Best Practice for e-Business Transactions*
https://www.entrust.com/wp-content/uploads/2013/05/digsig_transactions.pdf

for IEC code is to be filed electronically with DGFT (Director General of Foreign Trade). In Kerala the Department of Commercial Taxes Mandates E-filing of returns using DS under the Kerala Value Added Tax Act 2003. Now C forms and F forms are to be downloaded from the website of the department of commercial tax department of Kerala using DS. In India, other states also amended their VAT laws to make provision for E-filing. Likewise, under the Partnership Act 1932 also, firm registration application is to be filed electronically.

- **1976:** Whitfield Diffie and Martin Hellman first described the idea of a digital signature scheme, but they only theorized that such schemes existed
- **1977:** Ronald Rivest, Adi Shamir and Len Adleman invented the RSA algorithm, which could be used to produce a kind of primitive digital signature.
- **1988:** Lotus Notes 1.0, which used the RSA algorithm, became the first widely marketed software package to offer digital signatures.
- **1999:** The ability to embed digital signatures into documents is added to PDF format.
- **2000:** The Information Technology Act, 2000 makes digital signatures legally binding.
- **2008:** The Information Technology Act was amended and the PDF file format becomes an open standard to the International Organization for Standardization (ISO) as ISO 32000, which includes digital signatures as integral part of format.[3]

Technical Aspect

The public-key is made public and is distributed widely. The private-key is never distributed and must be kept secret. Given a key pair, data encrypted with the public-key can only be decrypted with its private- key; conversely, data encrypted with the private-key can only be decrypted with its public- key. This characteristic is used to implement encryption and digital signature.

Encryption and Decryption

Encryption is a mechanism by which any information is transformed so that only the sender and recipient can access that particular information.

Digital signature is a mechanism by which information is authenticated i.e. proving that information is effectively coming from a given sender, much like a handwritten signature on a document. Both encryption and decryption for a digital signature can be combined, hence providing privacy and authentication.

[3] *Infographic: The History of Digital Signature Technology* https://www.signix.com/blog/bid/108804/Infographic-The-History-of-Digital-Signature-Technology

A symmetric-key plays a major role in public-key encryption one-way encryption, i.e. it is impossible to derive the information from the digest. The main reasons for producing an information digest are:

1. The integrity of information being sent is preservedand any alteration will immediately be detected;
2. The digital signature will be applied to the digest, which is usually considerably smaller than the actual information.
3. Hashing algorithms are much faster than any encryption algorithm (asymmetric or symmetric).

The following sections explains what really happens when encrypting and signing information on one hand, and when decrypting the same and verifying its signature on the other hand.

1) Digital signature includes two steps:

a) *Information digest evaluation*: The main purpose for evaluating a digest is to ensure that the message is kept unaltered; this is called message integrity.
b) Digest *signature*: A signature is in fact an encryption using the issuer's private-key. Included in the signature is also the hashing algorithm name used by the issuer. The issuer's public-key is also appended to the signature. Doing so let's anyone decrypt and verify the signature using the issuer's public-key and hashing algorithm. Given the properties of public-key encryption and hashing algorithms, the recipient has proof that the issuer's private-key has encrypted the digest and the message is protected against any alteration.

2**) Information encryption:**

a) Creation *of a one-time symmetric encryption/decryption key:* Symmetric-key algorithms are very efficient and are therefore vital in information sharing.
b) Information *encryption*: The whole information (including the signature) is encrypted using SymK, the symmetric-key provided for evaluation.
c) Symmetric*-key encryption*: the recipient to decrypt the message also uses SymK. SymK must therefore be available to the recipient only. The way to hide the Symk from everybody except the recipient is to encrypt it using the recipient's public-key. Since SymK is a small bit compared to entire information, the performance penalty associated with the relative inefficiency of asymmetric-key algorithms is acceptable.

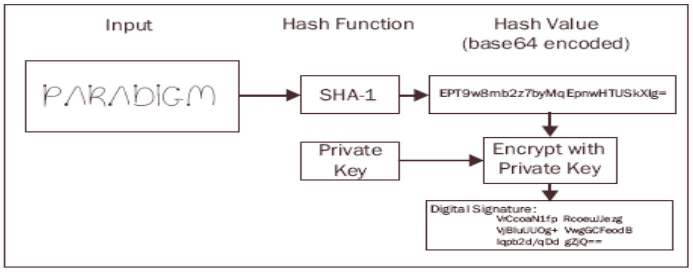

Figure 1.1[4]

Information decryption

a) Symmetric*-key decryption*: The one time symmetric-key has been used to encrypt the message. This key (SymK) has been encrypted using the recipient's public- key.

b) Information *decryption*: The complete information including signature is decrypted using SymK.

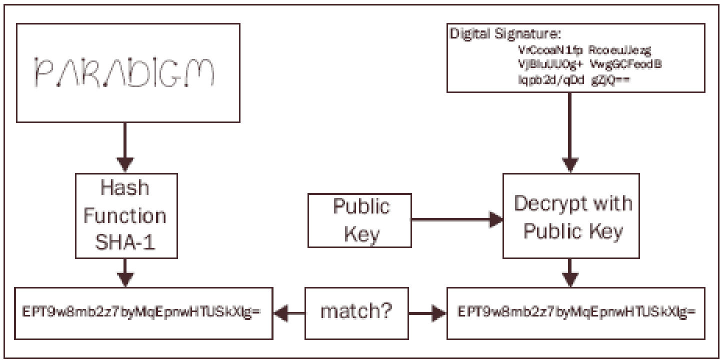

Figure1.2[5]

Signature verification:

1. *Information digest decryption*: The digest has been encrypted using the issuer's private-key. The digest is now decrypted using the issuer's public-key included in the information.

2. *Digest evaluation*: Since hashing is a one-way process i.e. the information cannot be derived from the digest itself, the recipient must re-evaluate the digest using the exact same hashing algorithm the issuer used.

3. *Digests comparison:* The digest decrypted and evaluated is compared. If there is a match, the signature has been verified, and the recipient can accept the information as coming unaltered from the issuer. If there is a mismatch this could mean that the information has either not been signed by the issuer or has been altered. In both situations, the message should be rejected.

[4] *Paradigm-Metadata for Digital Signatures* http://www.paradigm.ac.uk/workbook/metadata/authenticity-signatures.html

[5] *Paradigm-Metadata for Digital Signatures* http://www.paradigm.ac.uk/workbook/metadata/authenticity-signatures.html

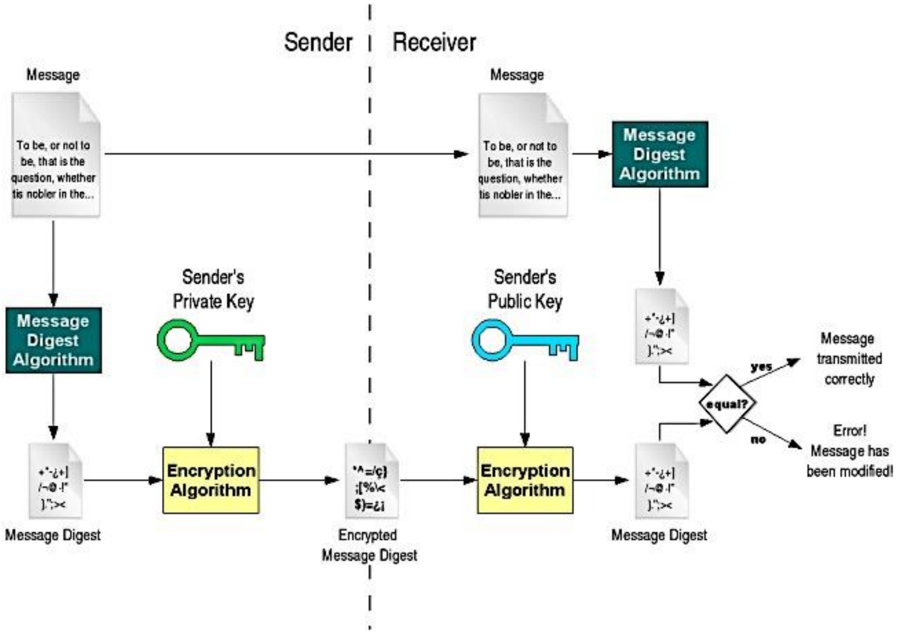

Figure1.3[6]

Digital Signature Certificates

Digital Signature Certificates are digital format certificate to prove identity in the digital world. Certifying Authority (CA) issues the digital signature certificates under the authority of Controller of Certifying Authorities. A Digital Signature Certificate is an electronic document that can be used to verify that the public key belongs to the particular individual. Digital Signature Certificates contains Public key of the certificate owner, name of the owner, validity "from" and "to" dates, name of the issuing authority, serial number of the certificate, digital signature of the issuing authority name of the person, etc. There are three different classes of digital certificate. They class I, class II and class III and depending on the type, each digital certificate provides specific functions.

Legal Aspects

As right to privacy is a fundamental right enshrined in Article 21 of the Constitution making it a constitutionally acceptable phenomenon. Section 3 of the Information Technology Act 2000 provided for authentication of electronic records. It gave forneed of the electronic records that can be authenticated by using digital signatures. It put down technical requirements for digital signatures. It prescribes the use of an asymmetric crypto system and hash function for authentication of electronic records. Authentication of an

[6] *Digital Signatures in pictures*
http://software-engineer-tips-and-tricks.blogspot.in/2012/08/digital-signature-staff.html

electronic document is important as it ensures that the information has not been tampered and confirms the sender's identity, so that it cannot be repudiated, 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 information into an unreadable format to prevent tampering of electronic record. 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. There are different types of electronic signature, however, all of them are not secure; hence only the techniques notified in the official gazette or in the second schedule can be used as a legitimate electronic signature. The electronic signature technique has to be reliable to be recognized as an electronic signature. Section 3A of the Information Technology Act 2000 is based on article 6, meaning "Compliance with a requirement for a signature" of UNCITRAL Model Law on Electronic Signatures 2001.

The requirement of an electronic signature is its reliability and The Central Government's notification in the official gazette on the technique and procedure for electronic signature or as specify in the second schedule of the Information Technology Act 2000. The Central Government is the authority to declare the technique as reliable electronic signature and can add or remove any technique from the electronic authentication technique. As on date the central government has not issued any notification on the concept of electronic signature and thus the electronic signature has not gained much attention. In this regard the Delhi High Court has directed the Central Government to frame policy on electronic signature for authentication of electronic records. The only method of authentication of electronic records in India presently being digital signature as there are no guidelines on use of electronic signature.

The legal recognition of electronic signature has been provided under section 5 of Information Technology Act 2000. This section equates electronic signature as traditional handwritten signature. It provides that if any, information or document if confirmed by electronic signature shall have the same effect as the affixing of signature if done according to the prescribed manner. The central government shall prescribe the manner in which electronic signature has to be affixed.

Criminality associated with Electronic Signature-Indian Perspective

Digital Signature and Information Technology Act

The offenses related to electronic signature are generally related identity theft, publication of false electronic signature certificate, and publication of electronic certificate for fraudulent purposes. 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 up to one 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, if a person makes a misrepresentation to the Certifying authority or a person suppresses any material fact from, the Certifying authority.

Such misrepresentation or suppression of material fact with the intent to obtain any license or electronic certificate from, the 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 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. Section 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.[7]

Digital Signatures and Evidence Act

The Indian Evidence Act 1872 is a piece of legislation dealing with evidences that can be produced or admitted in a court of law by the litigating parties. The law, which was enacted in 1872 naturally, did not envisage electronic signatures and records as evidences. Hence in view of the widespread use of electronic records and Electronic signatures including DS it was felt necessary to amend the said Act to make it in conformity with the changing trends in the society.

Section 3 of the Evidence Act 1872 provides for interpretation or definition of certain words or expressions used in the Act. The said section was amended to include electronic records also in the definition of the term "evidence". Further section 47A has been inserted to provide that when the Court has to form an opinion as to the electronic signature of any person, the opinion of the Certifying Authority, which has issued the electronic Signature Certificate, is a relevant fact. Section 67A has been inserted which protects the secure electronic Signature (DS). It provides that if the electronic signature of any subscriber is alleged to have been affixed to an electronic record the fact that such electronic signature is the electronic signature of the subscriber must be proved except when the same is a secure electronic signature. Section 73A has been newly inserted to provide that the court may direct the concerned person or Certifying Authorities (CA) to ascertain whether DS is that of the person by whom it is purported to have been affixed. It may also direct any other person to apply the public key listed in the electronic Signature Certificate and verify the electronic signature purported to have been affixed by that person. Section 85B (1) provides that in any proceedings involving a secure electronic record, the Court shall presume unless

[7] *The Information Technology ACT, 2008*
http://www.tifrh.res.in/tcis/events/facilities/IT_act_2008.pdf

contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates. Section 85B (2) provides that unless the contrary is proved the court shall presume that the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record. It further provides that there shall be no presumption relating to authenticity and integrity of the electronic record or any electronic signature if the same is not secure. Section 85C deals with situations where the Court shall presume, unless contrary is proved, that the information listed in a Electronic Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

Digital Signature and Indian Penal Code

Indian penal code 1860 (IPC) is in operation in India very successfully for the last 152 years. Nobody seriously felt the need for an amendment because of its excellent draftsmanship. But a need was felt for addition of certain provisions to take care of the new developments in the field of electronics and information technology. Thus through the Information Technology Amendment Act 2008 IPC was also amended. The most significant insertion is section 73A. Section 73A has been inserted to provide the same provision as in section 47A of the Indian Evidence Act discussed above in this article. Section 464 has also been amended to provide that the said section shall be made applicable to electronic records and electronic signatures also. Section 464 deals with situations when a person is said to make false document or electronic record. Section 466 provides for forging of electronic records also.

Conclusion

The amplified reliance on electronic transactions and contracts requires stronger technical protection, which is currently fulfilled partly by digital signature. This indicates the extent of electronic revolution that has taken place and thus the importance and relevance of digital signature. Time is not far away when we may even forget our own hand signature due to non-usage. However, it would be in the interest of cyber community if the Government allows and initiates multiple methods of authentication like the use of fingerprint or identity proof based platform linked with password based electronic transaction. Proper codification on individual merits of the case must be considered while formulating legislation on this subject. The principle of *LEX REX* can only be justified if adequate regulations are in place. The multiple methods would permit easy identification of persons which will assist in curbing frauds and ease electronic mode for transaction enhancing privacy and security of users as to even today the factual identity of persons on any electronic platform is a mirage.