Vol 4 Issue 8 Feb 2015 ISSN No :2231-5063

International Multidisciplinary Research Journal

Golden Research Thoughts

Welcome to GRT

RNI MAHMUL/2011/38595 **ISSN No.2231-5063**

Golden Research Thoughts Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.aygrt.isrj.org

Golden Research Thoughts
ISSN 2231-5063
Impact Factor : 3.4052(UIF)
Volume-4 | Issue-8 | Feb-2015
Available online at www.aygrt.isrj.org

LEGAL RECOGNITION OF DIGITAL SIGNATURE UNDER INFORMATION TECHNOLOGY ACT

Birendra Kumar Tiwari

Assistant Professor of Law – Rajeev Gandhi Law College Bhopal MP .

Abstract:-The speed of technological progress implies that many of the potential application fields for authentication and integrity services are difficult to ascertain of this stage. New application areas (for example protection of intellectual property rights, stored data, network security or electronic cash transactions) are developing continuously. In general way electronic communication digital signatures are considered to play a significant role. Digital signatures are not immediately readable and the signature, the carrier and the signed object are not physically related to each other in the same locked and prescribed form. The hand written signature furnishes the information with a physically unique sign of authenticity it is an original example.

Keywords: Equivalent of a Hand-written Signature, Cryptography, Picture, Encrypted, Digital Signature.

INTRODUCTION

Information technology has emerged as the most decisive, valuable and critical resource. It has emerged as an all pervasive force that impacts the lives of people across the global. Now paper based system is being replaced with automated electronic process. To combat the problem of forgery and cheating on both manual and electronic system, electronic signatures came into existence. Digital or electronic signature is equivalent of a hand written signature. They are more reliable cost effective and secure, compared to hand written signatures. Electronic signature is not just a "picture" of the hand written signature.

There are four fundamental principles to determine the trustworthiness of an electronic transaction – authenticity, integrity, non- reputability and confidently Authenticity to authenticate the identity of the person who signed the data so it is known who participated in the transaction. Thus the authenticity is about being able to prove at any point of time that a document is indeed signed by whoever it is that claims to be signatory. The second principle intergrity to protect the intergrity of the data so it is possible to know the message read has not been changed, either accidentally or maliciously. While integrity ensures that transmitted/ stored data cannot be changed without leaving a trace. Third principles are non reputability. Non- repudiation to allow it to be proved later who participated in transaction so that it cannot be denied who sent or received data. It is equally important that the signatory should not later be able to repudiate the validity of signature. A last confidentiality principle provides assurance that only the intended / authorized recipient or user can access the transmitted / stored data.

In the above principles it should be noted that in order to create a signed message, it is not necessary to send the message itself in encrypted form. Cryptography is a highly important instrument for achieving secure electronic commerce. The digital signature can be appended to the message and can be verified irrespective of the form of the message itself.

The information technology (I.T.) act passed in the year 2000 and amended in 2008, which provided the legal framework to guarantee authenticity, intergrity, and non- reputability of electronic transactions. Public key cryptography has been specified as the technology that can be used to create legally valid digital signatures for authenticating transmitted / stored data. The public key infrastructure (P.K.T.) that has been set up to implement this technology and other related provisions of the information technology Act, enables legally valid digitally signed electronic transactions and assures its authenticity, integrity and non- repudability.

Public key cryptography is the technology which has been specifically included in the I.T. Act for enabling authentication through digital signatures. There are number of ways that cryptography can work in an electronic environment.1

The most popular methods being used in present time is where the encoding and decoding of the message is performed by using two keys :- (i) a public key which is publicly know and (ii) a secret key which is only known by the sender or the recipient or both. The cryptography technique is generally known as 'public key encryption' this public key can be used by anyone to encrypt a message. Only the owner of the secret key can decrypt it. Thus when two parties want to send information to each other, they exchange their public keys. The public keys could also be retrieved from a database, which is open to the public. When A sends to B a message, A enciphers the message using the public key of B. only B can decipher the message using his secret key. The secret keys do not have to be transmitted or revealed to anyone. The primary advantage of a public key cryptography in increased security.2

Another advantage of the system is that the public key and secret key can be both be used for encoding as well as for discoding. Their function are inter changeable. This means A can encode a message with his own secret key, which B can decode by using the public key of A. On first sight, this seems a silly method, because everybody has access to the public key of A and can thus decrypt and read the message. It is indeed true. On the other way, B can be sure that the message can only originate from A, since he is the only one who knows the secret key. Without having contacted A before, B can trust on the authenticity of a message. It is on this technology of sharing a public key that digital signature are based. In the conventional methods, the same key was used for encryption and decryption which meant that everybody had to have access to the same key. In this case, however, every person has a pair of keys, of which one is public and the other private, known only to the owner of the key pair. If a document is encrypted with the private key, it can only be decrypted with the public key and vice versa. The most useful part of this technology – which is why it is easy to scale it up to large number, is that the private key does not have to be communicated to anyone, it remains with the owner. It is through the ownership of this private key that a non- repudiable digital signature can be created. The public key contributes towards the verification of the digital signature.

Digital signature technology opens up a whole new range of possibilities for the government to change the way it does business transactions electronically. The ability to transmit electronic message carrying legal binding signatures will allow business to conduct transactions and to inter into binding contracts entirely by electronic means.

Signing with digital signature:-

It is important to perform the signature function first and then an outer confidentiality function. In the case of a dispute, some third party must view the message and its signature, if the signature is calculated an encrypted message, the third party also needs access to the decryption key to read the original message. However, if the signature is the inner operation, the recipient can store the plain text message and its signature for later use in dispute resolution. Signing of the document depends on the software you have. First one needs to have some cryptographic software, installed on his computer. Further, he need to have a private key. Finally invokes his software and asks it to sign the document using the given private key and algorithm. After signing the document, it is verified by the authority and only then the originality of the document is counter checked.

Authentication and integrity digital signature-

Authenticity –

Authenticity has been and is still being, addressed through pass-words and challenge response system, but these methods are highly susceptible to attacks. Passwords are easily found out and usage of the same password for multiple applications makes them even more vulnerable to attacks. Mechanisms like finger prints or retina scans can only be used for access control and cannot be equated to digital signature. The requirement of confidentiality has been tackled by encrypting documents, where the receiver in order to access a document must possess the same secret key which was used to encrypt the document. This kind of sharing is impractical when a large number of people are being communicated with since separate secret keys will be required for each one of them. Besides, the identity of the person who has encrypted the document cannot be established.

Transmitting data in electronic form has may advantages compared with traditional systems. Documents can be made available at most instantly and in any quantity and the recipient is able to work on them directly. Transmission is considerably cheaper and faster- documents can be sent around the globe in a matter of seconds, without delay. However, the authentication and integrity services are needed for secure and trustworthy data transmission and communication over open networks3

Deference between traditional and digital signatures.

A hand written signature is physically tied to a to a carrier (the sheet of paper) which gives borderlines and

structure to the information in a immediately readable format.4 This 'lock' for the information, provided by the carrier and the signature representing the issuer's unique patterns of hand-writing, gives the reader reasons to believe that the object originates from the individual who is seen to be the originator and the identity tribute as inherent, not given to the signatory.

Digital signatures are not immediately readable and the signature, the carrier and the signed object are not physically related to each other in the same locked and durable forms. As the digital attribute making the signature unique for the individual is assigned not an inherent characteristic of the Signatory, the signature process may be performed by anyone who has access to the secret and the procedures.

The hand written signature furnishes the information with a physically unique sign of authenticity – it is an original example. Such signed object may be in a person's possession and can thus be a carrier of authority or a certain right. However, the unique aspect of a digital signed object has to be related to a pattern of data, which may easily be copied and the duplicate will have exactly the same qualities as the 'template'. Thus the unique existence of IT material is built upon the storing and transmitted of original contents and certain I.T. applications such as shipping documents demands some sort of registration.

There is no relationship to signer's hand written signature. While there's more to it behind the scenes, the visible portion of the digital signature is the signer's name, title, and the firm's name, along with the certificate serial number and the name of the certification authority.

When a digital signature made, it can be identified by receiver with the help of keys provided to him in advance. One is the private key which is used only him which is required during the signing process. The second key is public key. The public key is available for use by any one, wishing to authenticate one's signed documents. The public key will read with digital signature created by the private key and verify the authenticity of documents created within. This process is similar to accessing a safely deposit box. One key must work with the bank's key before opening the box.

The digital signature cannot by generally forged, as it is protected by several layers of highly complex encryption. Secondly, as private key is stored on computer, even then the access to private key is not available as it is encrypted when it is stored on your computer.

The procedure of traditionally signed objects may in the name be replaced by digital equivalents. By making use of security techniques, such as digital signatures, the authenticity of the information can be maintained. An examination of electronic commerce, electronic handling of cases by administrative agencies and similar routines shows the same need for protection, in the I.T. environment

The key difference between hand-written signatures and digital signatures is that your digital signature is different for every document that is signed signature. When a document is changed and signed once again the digital signature will be different. In this way the signature is bound to the document and to the person who has signed it providing assurance of authenticity and integrity.

Legal recognition of digital signature's

When a signing a contract using a digital signature one is confronted with different issues or questions: does a declaration of intent have a legal value? Does the signature meet legal requirements? Is a digitally signed document recognized as evidence in court?

Income Tax return filing from the comfort of home, depositing utility bills online, and even applying for a loan without heaps of papers is now a reality with digital signature.

The Information Technology Act 2000 prescribed a technology with which digital signature may be made. The object of the Act has been described in its preamble as "An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce' which involves the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of document with government agencies.5

Section 5 of I.T Act 2000 provides "where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then, notwithstanding any thing contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such by means of digital signature affixed in such manner as may be prescribed by the central Government.

In the above provisions the document signed by the person authorized, the signatures shall have legal binding on the both parties. To avail this facility we need a digital signature certificate issued by certifying authority"
The liability of certifying authorities needs to be clearly defined. The possible escape from liability clauses may be precisely fixed so that the certifying authorities needs to remain responsible to subscribes for losses caused to subscribes caused by the acts or omissions at the end of C.A. (Certifying authority). Whether there is any liability of there in no negligence on the part of C.A., but loss has been caused to subscriber without his fault.
They issue certificates to individuals and companies to identify and authenticate the sender as well as the date using public key inscription. The controller's job is to see whether the certifying authority has the required infrastructure,

adequate security, and processes in place.

Verification of Digital Signature

Section 73A lays down the procedures to be followed for verifying the digital signature of any person subscriber. When a dispute arises as to whether a digital signature belongs to a person, the court may ask any of the following to produce the digital signature certificate of the person.
(1) The person himself
(2) The controller appointed under I.T. Act,
(3) The certifying authority who has granted the digital signature.

Publishing digital signature certificate false in certain particular

Section 73 of the information technology act, lays down penalty for publishing false digital signature certificates, as punishment with imprisonment for a term which may extend to two years or with fine which extent to one lakh rupees or with both. Section 74 further provides that "whoever knowingly creatures publishes or otherwise makes available a digital signature certificates for any. Fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees or with both.

In India 75% people are living in villages and illiterate, cannot use or understand the nature & scope of digital signature. Moreover in cities, the educated persons are also hesitating to adopt this technique of digital signature, because of the fear and social atmospheres. Digital signatures is breathing new6 life to business although threats to potential danger to make consumers victims of big industries. Now the ability to transmit electronic messages carrying legal binding signatures will allow business to conduct transactions and to enter into binding contracts entirely by electronic means.

The digital signature cannot be forged, unless the signer loses, control of the private key for example by divulging it or losing the media or device it has contained.

CONCLUSION

In the above discussion it appears that digital signature technology is rapidly becoming evasive, but not everyone finds this comforting. Trust in a digital signature is determined by the public key corresponding to the private key used to create the digital signature. The binding of public key to an identified person should therefore be certified by trusted agency. Public key certificate's or digital signature certificate are issued by certifying authorities who validate the credentials of the applicant and enable online access to all digital signature certificates issued by them.

FOOT NOTES:-

1- Rayson – Richard and peter brown 'Electronic Banking development'
2- Mruphy- maureen m encryption and banking 12 P. CRS report 97 – 835 Section 15 1999
3- Analysis of the electronic currency system and the legal Purifications Murdoch university electronic journal of law vol 6, No 3 (September 1999)
4- Ghose, rishab aiyer, 1995 "paying your readers", electronic dreams (31 ruly)
5- The Information Technology Act, 2000
6- More Rotenberg, execute director of electronic privacy information centre in Washington.

Birendra Kumar Tiwari
Assistant Professor of Law – Rajeev Gandhi Law College Bhopal MP .