Global Journal of Enterprise Information System

Jan 2010-June 2010

Volume-2 Issue-1

'DIGITAL SIGNATURE : *NATURE SCOPE UNDER THE IT ACT, 2000 - SOME REFLECTIONS'*

Dr. Vijaykumar Shrikrushna Chowbe

Head, Department of Law, Sant Gadge Baba Amravati University, Amravati [Maharashtra], India.

vijuchowbe@gmail.com

ABSTRACT

This article has attempted to understand the nat meaning and scope of 'digital signature'. In turn, article has also focused on the mechanism of affixing 'digital signature' to electronic record. Signature sig authentication, verification and non-repudiation, bu electronic environment this mechanism happens altogether different sense as compare to paper-bc world because paper-based and paper-less world different in its context and contents.

The attempt is to understand the effect and impac 'digital signature' in the cyberspace, its techno-le effect and system if issuing, granting and maintaining 'Digital Signature' in India. The limitation of this artic the legal system it focused upon, i.e. Indian Legal syst This article has understand the effect and impact 'digital signature' in general sense, but keeping Information Technology Act, 2000 [Indian piece legislation dealing with Information Technology], t context different to that effect.

KEYWORD

Digital	Signature
IT Act	Legal system
India	IT

Preface

Authentication, repudiation and verification of electronic record is flesh and bone of the electronic transactions. Therefore, unless these objectives have not been achieved, the authentication and secure electronic transaction will merely remain virtual. In order to achieve the authentication and security of electronic record the mechanism of 'digital signature' has been introduced by the Information Technology Act, 2000.

Thus while endeavoring the research on regulatory mechanism of information technology, it is necessitated to focus on the 'digital signature', its functional mechanism, authorities involve and objectives it achieve in electronic environment. The present study title, 'digital signature' has focused its attention on this vary technological aspect which is meant for achieving the goal of authentication, repudiation and verification of electronic record by affixing digital signature.

Meaning of Signature

Signature signifies the legal identity of the person and requires authenticating the documents. The person affixing signature to the document owes legal responsibility oozing out of it. Thus, a signature is not part of the substance of a transaction, but rather of its representation or form. Signing writings serve the following general purposes: [i]

- **Evidence:** A signature authenticates writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the singer.[ii]
- **Ceremony:** The act of signing a document calls to the singer's attention the legal significance of the signer's act, and thereby helps prevent "inconsiderate engagements.[iii]
- **Approval:** In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it has legal effect.[iv]
- **Efficiency and logistics:** A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document.[v] Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.[vi]

What is digital signature?

Just the role the 'stamps', 'seal' or 'signature' play in traditional system to create the authentication of paper document, the digital signature plays the role to authenticate the electronic record. It establishes the authenticity of any electronic record which subscriber of digital signature wants to be authenticated the electronic record by affixing his digital signature. Digital signature in facts has two asymmetric pair of private and public key unique to the each subscriber. The private key and public key are corresponds to each other in such a way that the electronic record encrypted with the help of any private key can be decrypted only with the help of corresponding public

key. This digital signature creates digital ID for the subscriber holding digital signature certificate. This certificate is issued by Controller of Certifying Authority after due verification and adopting procedure.

This certificate contains basic information about the person holding it. The information such as, the name, public key, place of working, date of issuance, date of expiry of the certificate and name of the Certification Authority. The certificate is also publicly made available through the directories or public folders on WebPages. The law specifically made it clear that Controller will act as a repository for all Digital Signature Certificates issues under the Act and maintain a computerized data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.[vii]

This is essential because the public key of subscriber should be known to the interested person and should be readily available these information for them to verify the electronic record encrypted by subscriber of digital signature by affixing his digital signature.

Common features of Digital Signature: As stated above the digital signature play the same role as assigned to seal, stamps and signatures in the traditional system. It performs Signer Authentication, Message authentication and Verification.

a. **Signer Authentication: The digital signature must be capable to identify and link the signer with the electronic record which subscriber of digital signature has created. It is also necessary to ensure that the tampering of documents should not be happened after its creation. The private key belongs to subscriber who signs it and incurs legal responsibility out of it.**

b. **Message authentication:** The electronic record transformed by algorithm mapping with hash function by affixing private key of digital signature typically identify the matter to be signed, since verification also reveals any tampering with the message.

c. **Verification:** The ultimate aim of creation of digitally signed document is capability of its verification at latter moment of its creation. Thus the mechanism must be capable to verify the authenticity and non-repudiation to resolve the disputes between originators and recipient and a third party must be able to verify the signature as independent verifying institution.

'Digital Signature' – techno-legal aspects

Due to its varied nature, digital technology has provided faster, easy, accurate and convenient mechanism for creation, storage, transmission and retrieval of data without involving traditional paper-based formalities. This hastens the increasing use of digital technology in everyday life. Distance, transportation, conveyance are withered away between two individuals when they sit in front of their respective terminals sharing common network. They can share information, data, communicate by remaining online without diminishing their efficiency in

executing their work. These characteristic features of digital technology have led the world to go online. It has, in turn, increased the techno-dependency. Increasingly the business dealings, communication, official data and commercial transactions are being carried out in Cyberspace. The transformation of world from paper-based to digital based work culture has shifted the attention of world to find out the consequences of this transformation. Despite the speed, convenience and preciseness of the digital technology, some of the weaknesses of this technology has expressly manifested during the course of time. The most debatable issue in forefront is absence of degree of 'privacy' and 'authentication' of transactions, dealings and communication one can enjoy in traditional paper-based culture.

Privacy is an essence of individual liberty. No one wants to enter into the zone where his privacy would be at stake. If one is unable to feel secure about and does not have confidence for the consequences the digital environment put him for, he would hardly chose such medium for his transactions. Therefore, a sense of privacy and assurance of its respect in the medium play vital role for an individual to chose the medium. It is only because of the danger of being prospective violation of privacy, the net is treated is most dangerous zone where the 'privacy' has involved as a basic issue. It should be noted down that the concept of 'privacy' discussed here is not from point of view of any right to privacy, but is should be understood as a part of all transactions, dealing, communication that is used to be carried out by an individual with a feeling to be maintained by the concept of 'privacy'. It can be simply understood by taking an example of 'E-mails' and 'chat rooms'. Nobody assure that how so far these 'E-mails' and 'chat-rooms' are safe to safeguard the privacy of an individual. The 'privacy' is at stake in digital environment in two different ways.

First, because if one remains connected to the network, he loses control over his data. It may possible that the data may be hijacked by someone else, driven out of the computers, or passes from one server to another server without the knowledge of user. Data in digital environment is in the form of bytes which is capable to move, transfer, copy, distribute, disseminate in number of ways sometime, with the knowledge, sometime without the knowledge of user. It is utmost difficult to check the various routes, channels and paths of data in network.

Secondly, because netizens use network for creation, transfer, distribution, storage or dissemination of their data of personal nature. Today, billions of netizens are using Internet and they use the services provided by the Internet Service Providers [ISP]. The netizens use Internet for creating their E-mail account(s), chatting, surfing, gathering information of government offices & companies, to search job opportunities and even put their personal information on matrimonial sites in search of prospective life partner. Once any private information or communicate in digital environment either uploaded or received, transmitted or stored in mail account, everything is stored in the server of the Internet Service Provider. In this case despite the information, which is of private in nature, does not remain in actual possession of the intended recipient, but stored in the server of Internet Service Provider. In most of the cases it is observed that Internet Service Providers treat either the subscriber of their services or the information they generate, as a commodity for their own business promotion or projecting their Internet Services in to Digital Market.

Bigger the number of subscribers availing services of ISPs, more the advertisement revenue generation for Internet Service Provider. This can be more clearly evident by surfing to the matrimonial sites that uses the photographs, liking and disliking, hobbies, what they are looking for, of their subscribers to put on their home page to attract the other. Even in most of the cases, the netizens can view, share, surf and retrieve the data from these matrimonial sites. Therefore, entering into the digital environment is appeared to be risky now a day. Privacy is an essence of individual liberty which remains at stake in digital environment.

Another, serious problem one can pose in digital environment is lack of degree of 'authentication'. 'Authentication' is a soul essential for transactional solidarity. In absence of 'authentication', there would be difficulties in fixing the responsibilities and liabilities arise out of transactions and dealing. If the respective parties do not have the sense of 'authentication' for their counterparts, the documents coming from them, or if it is difficult to scrutinize whether the originator is the same and documents is not tampered in between the transaction, it is always have gap to air the doubt which lead to complex problem of fixing respective responsibility. Therefore, 'authentication' is one of the important ingredients for any transaction and dealing in any medium.

The traditional medium has set a mechanism to safeguards the interest of parties with entering into transaction and dealing with regards to 'privacy' and 'authentication'. Transactions, communication, information are passes in closed enveloped, stored in a locked cabinet, marked as 'confidential' and places has restricted entry for authorized personnel only. Secrete envelopes are marked to be opened by 'only addressee' or even sometime by using secrete codes in cryptographic languages which is able to decrypt by recipient only. The legislation like 'the Official Secrete Act, 1923' is an example to safeguard the information of public offices. The degree of authentication is met out with the help of 'stamps', 'seals', identity cards, 'logos', 'official emblems', 'signatures', 'encrypted messages' and several times by agreements signed by parties and attested by competent witnesses to protect information of 'confidential nature'. Such agreements are generally known as 'Non-disclosure Agreement'. Thus, the mechanism of authentication of information is neither new, nor uncommon to the legal system and there are several ways to generate sufficient degree of 'privacy' and 'authentication'. The need of 'privacy' and 'authenticity' of transactions, information, data, communication is still not diminished at all, which in contrast was lacking in digital environment. Therefore, it was felt necessary to introduce the technological safeguards which would able to provide the same level of authenticity and privacy the traditional system claimed for. 'Digital signature' has been introduced with the purpose to provide a degree of 'authentication' and 'privacy' to digital content. The present mechanism of affixing 'digital signature' is able to provide 'authentication' and to some extend create a degree of 'privacy' in the digital environment.

General and Technological aspects

This chapter attempted to understand the 'Digital Signature' in two different parts. The part – I has deal with the general & technological aspects of 'Digital Signature' in which various aspects are touched but from the aspect to understand the nature, scope, working phenomenon and modality of execution of

'Digital Signatures'. The other part will deal with the legal aspects of 'Digital Signatures'.

Digital Signature – Necessity and objectives

Digital Signature is created by using cryptographic method. For the purpose of under standing the affixing of 'Digital Signature' by way of cryptographic method, it is essential to bear in mind the purpose of affixing 'Digital Signature'. The basic objectives of affixing of 'Digital Signature' are –

Affixing of 'Digital Signature'

Create authenticity of the originator – so that at any moment after the creation of any digital material, the authenticity of the originator can be verified. It will be possible only if the mechanism is capable to create any impossibility of anybody else to represent himself with the digital material which he has not created. At the same time it is also essential that at any latter moment, the originator will not capable to deny the creation of document by him

Create authenticity of the document - so that any recipient will not be in position to modify, change, alter, or tamper with the document created by originator. The mechanism should also ensure to the originator that no one else than him will be capable to modify, change, alter or tamper with the document

Non-repudiation – so that the entire mechanism will ensure that the document and identify mechanism will not play foul and nobody will be in position at any latter moment to deny the responsibility and liability arising out of the document. For originator, that he will not be in position to repudiate what he had created, for recipient, he will not be in position by any means to modify the content created by originator

The 'Digital Signature' has evolved to achieve these objectives. It can be done with the help of 'Public Key Cryptography'. Therefore first it is essential to have fundamental understanding of the concept and meaning of term 'Cryptography'. It can be represented as:

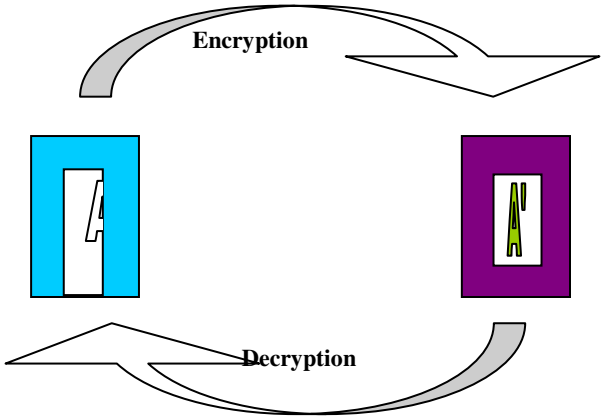

Fig: 2 Encryption/Decryption of an electronic record to convert it from one form to another

'Cryptography' is a way of scrambling of electronic record from one form to another form using hash function which leads to create hash result. Encryption stands for the modifying the electronic record in different form and decryption stands for bring it into the original form.

Normally, it is easier to encrypt any electronic record from one form to another and bring it back to its original form by decrypting it. It is important to note here that both encryption and decryption is easy for those who are aware about the methods used in this process. In this process generally a key is used to encrypt the electronic record and by using the same

key. This keys act as a secret password and generally know to both the parties i.e. originator and recipient. Therefore, if both the parties are aware about the keys required for encryption and decryption they can assure the authenticity of an electronic record.

Mechanism of Digital Signatures

However, recently, the mechanism has been developed to use two different keys. By one key the encryption can be carried out and decryption used to be carried out by different key. Both the public and private keys are different from each other commonly but correspond to each other in such a way that the public key can decrypt the document encrypted by private key. The main purpose of using two keys is very apparent. The first key of the set is 'private key' which is unique and only know to its holder.[viii] It acts as a secrete key of holder and plays very vital role. It helps any holder of this key to encrypt the electronic record. Once the electronic record is encrypted with the help of private key it scrambled the electronic record in such a clever ways so that putting it back to its original form is almost all impossible. Even the holder of private key now cannot put the electronic record into original form. Now only viewing this record is possible with the help of corresponding public key. The mechanism of private key is that it leads every time to the same result for same electronic record. Thus once any electronic record is encrypted with the help of private key the holder of private key cannot deny that it is encrypted with the help of his private key.

The second key in the set is public key which is used to verify electronic record and available and known to the public at large. Anybody who wants to verify the content of the electronic record encrypted with the help of private key, can use corresponding public key to verify the electronic record, however, only verification of electronic record is possible with the help of public key and no alteration, modification, change or tampering is possible furthermore once it is transformed into hash result by applying private key. Both these keys are so related with each other that only the electronic record encrypted by private key can be open by its corresponding public key only. Thus use of this asymmetric pair of keys for encryption and decryption of electronic records serve following purposes:

For Originator

It helps the originator to encrypt the electronic record. Once originator encrypts any electronic record with the help of his private key, nobody [even originator] can modify the content of the electronic record. Thus private wrap the digital content and does not allow modifying, altering, changing or tampering the content of the electronic record. Thus after apply his private keys originator will assure himself that the electronic record cannot be bring to its original format and any change is almost impossible in the electronic record.

Once the electronic record is encrypted it get wrapped, and no further alteration by any means allowed to be made. Therefore originator remains assured that any electronic record he has created is safe. Such electronic record can be decrypted only with the corresponding public key of originator. Thus, if any alteration has been made to electronic record created with the help of originator's private key, the public key of originator will unable to open the electronic record. Therefore, public key of originator will works only in case when the electronic record created by encryption of private key of originator.

For recipient

As the document so created by private key of originator is unique one which can be opened only with the help of public key of originator, recipient can verify and get assured by decrypting the electronic record with public key of originator which is readily available. Once the electronic record is able to decrypt, it is evident that it was encrypted by the private key of originator. If the deception is possible, it is evident that it is not modified after its encryption.

Therefore, if the electronic record is capable to decrypt with the help of public key of originator, the originator cannot deny the authenticity of electronic record. But if electronic record is unable to be verified with the help of public key of originator, it is possible that originator had not created it or it has altered after its creation.

Because technically whenever private keys applies to the electronic record, hash function works upon it to transformed it by algorithm mapping into another electronic record called hash function, this hash function is only able to verify with the help of corresponding public key of the originator. This helps the originator that once he applies his private key to any electronic record, the resulting record [known as hash result] will neither be able to tamper nor any change is possible, and only can be verified with the help of his public key and not otherwise.

For the purpose of legal system

a. This system also helps to create authenticity and accuracy for electronic record. In case of any doubt and denial of authentication either by originator or recipient, the electronic record can be varied. Because hash function is such algorithm mapping system which generate the same hash result every time with same input.

Therefore, if the electronic record is capable to decrypt with the help of public key of originator, the originator cannot deny the authenticity of electronic record. But if electronic record is unable to be verified with the help of public key of originator, it is possible that originator had not created it or it has altered after its creation.

Verification can be made out in following ways. If the recipient has brought any electronic record in question before the court claiming that it is created by originator, and if originator denies its creation, it can be verified by applying public key of the originator. If the document gets decrypted with the public key of originator, the originator would not be in position to deny that he is a creator of the document. Because there is only one set of corresponding public and private key. It is highly impossible to decrypt the electronic record encrypted by one private key using public key of different originator.

This system in short is called affixing of digital signature. As the originator by using his private key create a electronic record in such a way that his private key act as his signature to the electronic record. The necessity of digital signatures is the essence to create authentic transaction, creating non-repudiation and integrity. It can be achieved by this process in following manner –

Authentication: As discussed above, authentication is achieved in the digital environment because this process ensure that no two sets of public and private key pair match with each other. Again the electronic record encrypted by private key of a pair is only decrypted by public key of the same pair. However, the electronic record once created by applying private key, get tampered, altered, modified or change, the public key will not able to decrypt it anyway.

Therefore, the parties, originator and recipient, can authenticate the genuineness and originality of electronic record. The Information Technology Act, 2000 has created a mechanism for affixing digital signature. The office of Controller of Certifying Authority has entrusted the responsibility for issuing, maintaining and taking all steps for safeguarding the digital signature. It issues the digital signature to subscriber, keep record and provide guidelines for its safeguards. Thus, in case of any dispute office of the Controller of Certifying Authority referred. As the record of the digital signature which constitution a key pair[ix] of private and public key is issues and maintained by the Controller of Certifying Authority, the subscriber [holding key pair] is not in position to deny its possession and authenticity.

Non-repudiation: The manner in which digital signature affixed to any electronic record can cerate authenticity of an originator, it also make is disable to repudiate any argument of its non-creation. Thus once the electronic record is created by any private key, the originator cannot deny its creation. He furthermore has to accept all the responsibilities and consequences arise by its creation. His authorship gets fixed to the electronic record and all the right and a liability oozes out automatically lies to the creator. This is important because most of the time, the creator deny the creation of the electronic record to overthrow the legal responsibility. In the eye of law this is called as non-repudiation. It is important to resolve the problems and solve the legal disputes.

Integrity: This is another important objective achieve by the digital signature. By creating a mechanism solidifying authentication and non-repudiation, it develops the sense of integrity of both the parties to the transactions. Once the digital signature are involve, both the parties remain assured, and enter into the transactions, dealing with full sense of assurance that the transactions would capable to fix right and responsibilities oozing out of it. Furthermore, both the parties are having legal alternatives open for them in case of denial or allegations. If the electronic record carries the digital signature, parties are hardly in position to deny creation and participation in the transactions. Again, both parties also remained assured about the so called 'tampering' to the electronic record. If the electronic record gets tampered, it automatically loses its authentication and non-repudiation character and lose it legal genuineness. Thus the digital signature is also capable to achieve the object of 'integrity'.

Technological mechanism of Digital Signatures

It is essential to have brief look at the technological working of a 'digital signature' mechanism. As stated earlier, each user has a pair of private and public key. This can be graphically represented as follows:

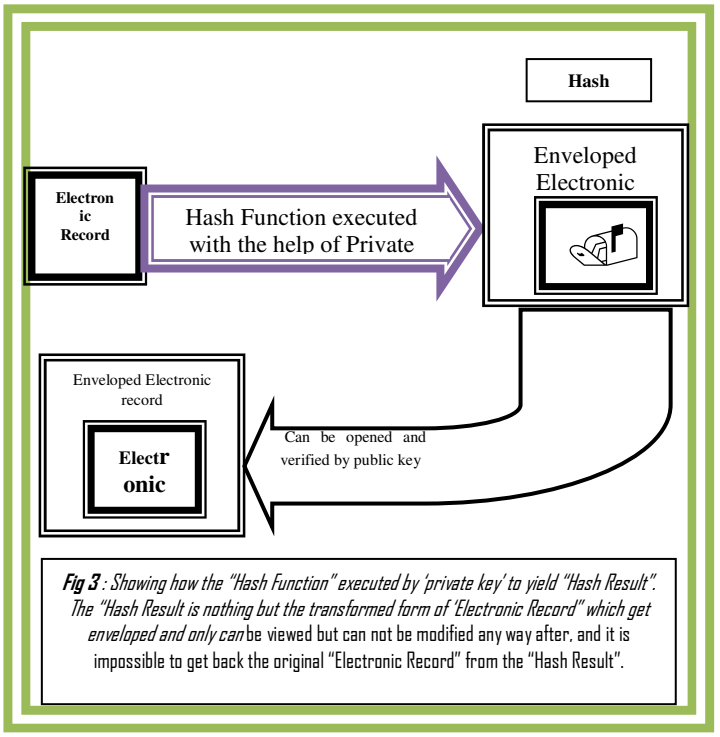

Fig 3 : Showing how the "Hash Function" executed by 'private key' to yield "Hash Result". The "Hash Result is nothing but the transformed form of 'Electronic Record" which get enveloped and only can be viewed but can not be modified any way after, and it is impossible to get back the original "Electronic Record" from the "Hash Result".

The private key remain secrete with the user and nobody is aware about it, while public key is freely distributed for the public which can be used to decrypt and verify the electronic records encrypted by person. While affixing the digital signature to any electronic record, the originator (subscriber of Digital Signature Certificate) applies his private key. When he applies his private key, an asymmetric crypto system and hash function transform the initial electronic record into another electronic record.

The "hash function" stands for an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known 'as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(i).	**to derive or reconstruct the original electronic record from the hash result produced by the algorithm;**
(ii).	Those two electronic records can produce the same hash result using the algorithm. And

This mechanism also ensure that the set of private key and the public key are unique to the subscriber and constitute a functioning key pair.[x] The keys (also) have the property that it is computationally not feasible to discover one of the key pairs merely by knowing the elements of the other key.[xi]

It can be understood from above that –

- Once the "hash function" works on electronic record, it yield "hash result". This process is such that the hash function yield as hash result each times it works upon.
- "Hash function" is an algorithm which makes it infeasible to derive or reconstruct the original electronic record from the hash result produced by the algorithm.
- The two electronic records cannot produce the same hash result using the algorithm.

Therefore, every mechanism set forth must ensure all these standards. If the algorithm is unable to achieve all or any of the above objectives, the mechanism of digital signature would be futile and unable to ensure authenticity. This criterion is required by S. 3 of the Information Technology Act, 2000 and Controller of Certifying Authority has to ensure that the technological standards are capable to ensure these objectives. However, the different standards can be set forth for government and non-government entity by the Controller of Certifying Authority.[xii]

Jurisprudential and Legal aspects of Digital Signatures

If the preamble of the Information Technology Act, 2000 has given a close look, it is apparent that the act has enacted to provide 'legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication'.[xiii] The act has attempted to legally recognize the process in sum called 'electronic commerce'. The act is in furtherance of the resolution passed by United Nation on 30th January, 1997 to which India was signatory, where UNCITRAL [United Nation Commission on International Trade Law] has proposed a 'Model Law' and recommend to member states to give favourable consideration while bringing any enactments, amendments, or inceptions in the legislation relating to 'Electronic commerce'. In furtherance to promote the 'Electronic commerce' that is inter alia requires reliability of electronic documents,

it is essential to have mechanism that would ensure the trustworthiness of the electronic documents. The concept of 'Digital Signature' has brought into being with the sole purpose to develop mechanism for creating reliability and authenticity of electronic documents.

Legal Recognition of Digital signatures

The Act has set forth the objective to provide legal recognition for transactions carried out by means of electronic data interchange. At the same time, the authentication, integration and non-repudiation of electronic record is equally important. But more important than anything else is to provide a provision that would create a sense of responsible and assurance about the mechanism. The genuineness and of medium is equally important than creation of medium, and the information technology in general and digital signature in particular has attempted to bring authentication in this medium.[xiv]

Therefore, it was important that not only the affixing of 'digital signature' would make important, but it is also necessary to give equal force to the electronic record created by digital signature which in traditional medium has for attested and signed document. S. 5 of the Act fulfill this requirement which runs as under[xv] :

S. 5. Legal recognition of digital signatures.

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 anything 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 manner as may be prescribed by the Central Government.

Explanation.—For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

Thus the plain reading of S. 5 makes it clear that the electronic record to which the 'digital signature' has been affixed has equal binding force which in traditional system the signed document has. It has also expressly made it clear if any law require that any document must bear signature, the requirement will deem to be satisfied if the electronic record is authenticated by affixing digital signature.

The explanation clause clarifies the meaning of "signed" and "signature". The clause explain that as the word "signed" has the meaning and expression attached to it which is generally done by mean of affixing of his hand written signature or any mark on any document, and signature has its meaning, in the same way, the 'affixing of digital signature should be construed accordingly. One very important differentiation should be beard into mind that in India the Act has adopted "Digital Signature" which is created by hash function and pair of public and private key. In contrast, in most of the nation, it speak about "Electronic Signature". The basic different between "Digital Signature" and "Electronic Signature" is, the digital signature is in digital form contain may be alpha-numerical, where electronic signature may also contain sound, signature by digital pen, watermark, thumb impression, eye scan. Comparatively, 'Electronic Signature' provides more security. The proposed amendment in Sept 2005 which is still pending for want of enactment, which will provide the

mechanism for 'Electronic Signature' by replacing 'digital signature', if would take shape of legislation.

Digital Signature – Legal Definition and effectuation

The 'Digital Signature' has been defined by S. 2 (1) (p) of the Information Technology Act, 2000 [the Act] as follows :

> *2 (1) (p)* "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

Thus, what exactly the 'digital signature' stands for has not been defined by the Act. It simply point out that 'digital signature' means authentication of electronic record by subscriber by and in accordance of the procedure laid down by Chapter II, S. 3 of the Act. For reference it is essential to have a look to Section 3 of the Act which runs as under:

> **Section 3. Authentication of electronic records.**
>
> (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.
>
> (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.
>
> *Explanation.*—For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known 'as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—
>
> *(a)* to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
>
> *(b)* that two electronic records can produce the same hash result using the algorithm.
>
> (3) Any person by the use of a public key of the subscriber can verify the electronic record.
>
> (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Ss. 3 (1) of the Act explain the category of person who can authenticate the electronic record. It provides that the 'subscriber' can authentication any electronic record by affixing his digital signature to it. This sub section empowers only to the subscriber, *and not any general person*, the capacity to authenticate the electronic record. The Act also defined 'subscriber' vide S. 2 (1) (zg) as :

> "subscriber" means a person in whose name the Digital Signature Certificate is issued;

Thus the person having Digital Signature Certificate is only empowered to authenticate (any) electronic record by affixing his 'digital signature'. The Act does prescribe that subscriber can authenticate electronic record by affixing his 'digital signature'. Therefore it is not required by the Act that subscriber can authenticate only 'his' electronic record. It is clear from the language of the S. 3 (1) that subscriber can authenticate any of the electronic record whether created by himself or by any other person by affixing his 'digital signature'. It is apparently clear that though only the subscriber can authenticate the electronic record by affixing his 'digital signature', but no

limitation has been put on the subscriber to authenticate only his electronic record. He can authenticate the electronic record of other's also, but subject to provision of the Act, and only electronic record bearing valid 'digital signature' is treated reliable and authenticate in the eye of law. The general public using Internet for the purpose of E-mails, Chatting, sharing files, surfing, downloading for educational or any other purpose or even taking information from the WebPages, or government institutions, offices, companies having their Webpage cannot be treated as authenticate electronic record unless the creator of these electronic record has not holding 'digital signature certificate' and even if holding it, he has not authenticated his electronic record by using his 'digital signature'. Therefore, it should be noted down that all those electronic records which exists in digital environment are neither reliable nor authenticated. The authentication process is deliberate attempt by subscriber holding 'digital signature' and an option for him to affix his 'digital signature' to the electronic record. However, once the subscriber opted to authenticate the electronic record, and in this attempt, affix his 'digital signature' to any electronic record, it will be treated authenticate by world at large against the subscriber and subscriber cannot afterward repudiate its authenticity. Anyone can verify the authenticity by applying 'public key' of creator as the mechanism of 'digital signature' is capable to verify[xvi] the authenticity of electronic record created using 'digital signature' and this mechanism is recognized by means provided by law.

The electronic record bearing 'digital signature' thus presumed to be authenticates and can be relied upon for the purpose of commercial and other transactional business. Subject to other provisions of the Act, the electronic record bearing 'digital signature' carries evidential value and can be used against subscriber if denied or alleged to be non-authenticated.

Ss. 3 (2) prescribe the procedure of affixing of 'digital signature' to the electronic record. It stipulates that the authentication of the electronic record shall be effectuated by use of the asymmetric crypto system and hash function. The Asymmetric Crypto System' is a cryptographic process in which two different asymmetric key pair has been used to secure the record. These two key are private key and public key in which private key is used for creating a digital signature and corresponding public key to verify the digital signature.[xvii] S. 3 (4) of the Information Technology Act, 2000 states that the private key and the public key are unique to the subscriber and constitute a functioning key pair.[xviii] These two keys are related and correspond to each other in such a way that the electronic record created by a private key can only verify by public key related and corresponds to it.[xix]

Though traditionally, only one key pair use to encrypt the record and same key pair use to decrypt it. But for securing the record and unable its reversibility, two different key pairs are used in which one key pair modify the record and other key pair can only verify it, but does not able to alter, change its content.

When the private key is used to effectuate the 'digital signature' to the electronic record, hash function which is a kind of algorithm mapping use to envelop and translate one sequence of bits into another work on it to generate "hash result". The hash function is one which whenever works upon the same electronic record yield the same hash result every time.

However, the legal provision prescribe with regard to hash function that –

(i)	**The hash function is one which is used to envelop and transform the electronic record into another electronic record which is called hash result**
(ii)	The hash function is to yield same hash result every time whenever executed with same electronic record as it input
(iii)	This hash function must bear the feature that deriving or reconstruction of original record from hash result shall not be possible
(iv)	No two electronic records yield same hash result with hash function

These four conditions are mandatory to ensure that nobody able to get the original electronic record back from hash result. The first condition will ensure that hash result shall envelop and transform the electronic record into another electronic record. This process blocks the content and wraps it so that the content of the electronic record get block from any change or modification.

The second condition is to safeguard the interest of subscriber. The quality of hash function to yield same hash result every time whenever executed upon the same input will help the subscriber to verify any latter moment tampering or change into the electronic record. Thus if subscriber is doubtful about the authenticity of the electronic record, he can execute hash function to verify that the result is same or not. If the result remains unchanged each time, he can ensure that the document is one which he had created. But if two hash results differ, he can very well take plea that the input is different. The same methodology can be used by forensic lab to verify that whether the same hash result yield second time or not. They can check it with the alleged electronic record by comparison.

The third condition laid down by the Act is due to the reasons that once the digital signature affixed to the electronic record, it get enveloped and wrapped by the hash function. Now it is only possible that one can only verify it but cannot modify. Once the system ensure this feature, it give a legal presumption that once the electronic record bears digital signature, it is neither modified, changed, altered or tampered by anybody. Even the subscriber cannot able to get original record by any means. Therefore, reliability of electronic record can be ensured.

The last condition ensures that no two results from two different inputs shall yield after execution by hash function. This is because if the two hash result will be identical despite the inputs were different, its authenticity will at stake. Thus for different input, different hash result must be yield and no two hash result shall be identical if the input is different. These conditions can ensure and strengthen the reliability of mechanism and chances of creeping up of loopholes.

Creation and maintenance of Digital Signature

The Information Technology Act, 2000 has also set up the mechanism for creation and maintenance of 'Digital Signatures'. The office of the Controller has been created for the purpose. The Controller grants the licences to the 'Certifying Authority' which further issue 'digital signature' to the subscriber. Thus, Controller does not directly issue 'digital signature', but issues licences to the 'Certifying Authority'. The Certifying Authority issues the 'Digital Signature Certificate' to the subscribers. These can be represented graphically in following manner :

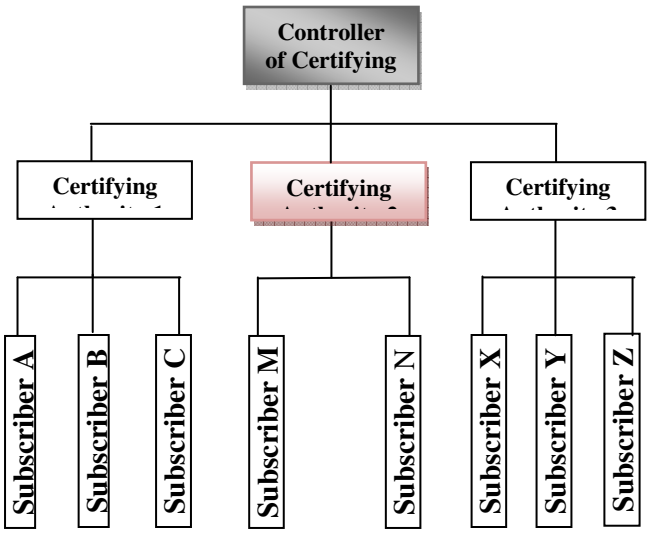

Fig 4 : Showing hierarchical set up of Controller of CA

Note : Subscribers are not the constituent part of the office of CCA

The Controller of Certifying Authority [CCA] is appointed by Central Government by notification in Official Gazette in accordance with S. 17 of the Act. by the Central Government. The Controller shall discharge his functions under the Act subject to the general control and directions of the Central Government.[xx] The functions of the Controller are prescribed by S. 18 of the Act which following major functions:

- exercising supervision over the activities of the Certifying Authorities
- certifying public keys of the Certifying Authorities
- laying down the standards to be maintained by the Certifying Authorities
- specifying the qualifications and experience which employees of the Certifying Authorities should possess
- specifying the conditions subject to which the Certifying Authorities shall conduct their business
- specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key
- specifying the form and content of a Digital Signature Certificate and the key,
- specifying the form and manner in which accounts shall be maintained by the Certifying Authorities
- specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them
- facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems
- specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers
- resolving any conflict of interests between the Certifying Authorities and the subscribers
- laying down the duties of the Certifying Authorities
- Maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.[xxi]

If the above functions of the Controller of Certifying Authority are scrutinized closely, it can be averted that Controller enjoys great control over the Certifying Authority. The Controller exercises greater control with regards to the activities of Certifying Authorities as he supervises activities of Certifying Authorities, laying

down the standards to be maintained by the Certifying Authorities, specify the qualifications and experience of employees of the Certifying Authorities should employ, specify the conditions of business carried by Certifying Authorities, specify the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key, specify the form and content of a Digital Signature Certificate and the key, specify the form and manner in which accounts shall be maintained by the Certifying Authorities, facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems, specify the manner in which the Certifying Authorities shall conduct their dealings with the subscribers, resolve any conflict of interests between the Certifying Authorities and the subscribers, lay down the duties of the Certifying Authorities and maintain a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public. Therefore, even though Controller does not directly play the role of distribution of 'digital signature' to the subscriber, he enjoy almost all the power in which manner the 'digital signature' shall be issued and maintained by 'Certifying Authorities'. In practices, the Controller of Certifying Authority issue licence to Certifying Authorities who in fact give digital signature to the subscriber.[xxii]

The Act has also specified the scope for the recognition of foreign Certifying Authorities. For this purpose, the act has prescribed that Controller may with prior approval of Central Government and subject to such conditions and restrictions as may be specified by regulations, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of the Act. In this case, if the foreign Certifying Authority would given recognition, the 'Digital Signature Certificate' issued by such Certifying Authority either to any citizens having any nationality, any company or institution incorporated in India or any foreign person, company or institution will be treated recognized for the purpose of the Act and will have the same effect and force as if the 'digital signature' is issued by the Certifying Authority having licence by Controller for all purposes laid down by the Act. [xxiii]

Digital Signature – Safeguard and functional mechanism

The Acts prescribe vide various provisions to safeguards and functional mechanism for 'Digital signature'. These safeguards can be put in following ways:

Provisions to safeguard the 'Digital Signature' mechanism

- The Controller acts as the repository of all Digital Signature Certificates and also maintains the computerized data base of all public keys.[xxiv] This ensures the availability of public key to any member of public and verification of data is possible
- The Controller has responsibility to ensure from any intrusion and misuse of any hardware, software and procedures to safeguards 'Digital Signature mechanism' and
- Shall observe such other standards as may be prescribed by the Central Government.[xxv]
- The Controller is empowered to investigate any contravention of any of the provisions of the Act either by himself or through authorized officer[xxvi]

- S. 30 of the Act provide the procedure which Certifying Authority should follow. This section laid down the responsibility on Certifying Authority with regard to hardware, software and procedures that are secure from intrusion and misuse. It also laid down that Certifying Authority should provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions. In addition to it, Certifying Authority should also adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and observe such other standards as may be specified by regulations. This is because to ensure the security measures for 'Digital Signature' and prevents it from any intrusion and misuse.[xxvii]

Provisions with regards to functional aspects of 'Digital Signature'

- The Controller is empowered to issue the licence to issue Digital Signature Certificates any person only after fulfillment of requirement laid down by the Act.[xxviii] The **Terms and conditions of licence to issue Digital Signature Certificate have been provided vide rule 3 of** the Information Technology (Certifying Authority) Regulations, 2001.
- The licence to Certifying Authority is issued only subject to satisfaction of qualification, expertise, manpower, financial resources and infrastructure facilities. This shows that person must comply with the requirement laid down by the Act and corresponding rules from time to time. Therefore, while granting the licence to any Certifying Authority to issue 'Digital Signature' the ability of the Certifying Authority will be tested upon and comply with, otherwise Controller will not issue licence to Certifying Authority.
- Though the provision laid down the liberty for Certifying Authorities to set norms and standards for issue 'Digital Signature Certificate'[xxix] to the subscribers, they must observe the rules and regulation laid down by the Act and instruction given by the Controller from time to time.[xxx]
- The Certifying Authority may charge the fees for issuing 'Digital Signature' to subscriber not exceeding Rs. 25000/- [or as may be prescribed by Central Government].
- The licence issued to the Certifying Authority also has expiry date. However the provision for renewal of licence also been prescribed by the Act. [xxxi]
- The Act also prescribed the provision for issuance and suspension of licence for which Controller has been empowered by the Act. The grounds for the suspension of licences are

Providing any incorrect information asked by any statement
Failed to comply with any term and condition on the basis of which the licence has been granted
Failed to maintain standard or contravened the provision of the Act

However, Controller will give the Certifying Authority an 'opportunity of being heard' to put his stand before revocation of licence[xxxii]

Thus, as stated in the beginning of this part of research writing, the mechanism of digital signature functions to achieve authentication, non-repudiation and verification of electronic record. It provides the sense of security in the electronic environment and facilitates the electronic transaction.

Sum up

The above analysis show that 'digital signature' under the Information Technology Act, 2000, that this is not only essential aspect for creating secure environment for electronic transactions, but it create a sense of authentication and non-repudiation and thus ultimately achieve its objectives of facilitating e-commerce. Thus in its application, digital signature has not only proved an essential techno-legal requirement, but it has made the e-commerce meaningful.

However, looking to the present development across the world, it is essential to reconsider the importation of 'electronic signature' in the legal books as it ensures greater level of safety and security in electronic environment. Beside the same, the need for cross-border recognition of digital/electronic signature is already overdue which cannot be delayed further.

The study of electronic environment from legal point of view would be incomplete without scrutinizing the 'criminality' and its various dimensions. The previous and this chapter of this research writing had focused its attention on legal framework prescribe by law. However, this would be incomplete without having glance to the 'crime' being committed in cyberspace. The study of crime committed in cyberspace will provide a platform to activate the study in proper direction, as the one of the basic role of legal framework is to regulate the 'criminality' and set law and order. Thus this makes it essential to have a glance to 'criminality in cyberspace'. Therefore, next chapter of this investigative writing turn its attention towards this aspect.

References

[i] This list is not exhaustive. For e.g. Restatement (Second) of Contracts notes another function, termed the "deterrent function", which seeks to "Discourage transactions of doubtful utility." Restatement (Second) of Contracts 72 Comment c(1981). Professor Perillo notes earmarking of intent, clarification, managerial efficiency, publicity, education, as well as taxation and regulation as functions served by the statute of frauds. Joseph M. Perillo, the Statute of Frauds in the Light of the Functions and Dysfunctions of Form, 43 Fordham L. Rev. 39, 48-64.

[ii] See, Restatement (Second) of Contracts, statutory note preceding S. 110 (1982) (Summarizing purpose of the statute of frauds, which includes a signature requirement): Lon L. Fuller, Consideration and Form, 41 Colum. L. Rev. 799, 800 (1941); 6 Jeremy Bentham, The Works of Jeremy Bentham 508-85 (Bowring Ed. 1962) (1839) (Bentham called forms serving evidentiary functions "preappointed [i.e., made in advance] evidence"). A handwritten signature creates probative evidence in part because of the chemical properties of ink that make it adhere to paper, and because handwriting style is quite unique to the signer. Signed includes any symbol executed or adopted by a party with present intention to authenticate a writing.

[iii] John Austin, Lectures on jurisprudence 939-44 (44th Ed. 1873); Restatement (Second) of Contracts S. 72 comment c (1982) and statutory note preceding S. 110 (1982) (what is here termed a "Ceremonial" function is termed a "cautionary" function in the Restatement);

[iv] See, Model law on Electronic Commerce, United National Commission on International Trade Law (UNCITRAL), 29th Session, Art. 7 (1) at 3, Doc., A/CN.9/XXIX.CRP.1/Add. 13 (1996) ("Where a law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message…."); Draft Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Data Communication, United Nationals Commission on International Trade Law (UNCITRAL), 28th Session, Art. 6, at 44, U.N. Doc. A/CN./9/406 (1994). For example, a signature on a written contract customarily indicates the signer's assent. A signature on the back of a check is customarily taken s an endorsement. See U.C.C. S. 3-204 (1990).

[v] Analogizing the form of a legal transaction to minting of coins, which serves to make their metal content and weight apparent without further examination. The notion of clarity and finality provide by a form are largely predicated on the fact that the form provides good evidence. The basic premise of the efficiency and logistical function is that a signed, written document is such a good indicator of what the transaction is, that the transaction should be considered to be as the signed document says. The moment of signing the document thus becomes decision.

[vi] See, e.g. U.C.C. S. 3-401 (1990) (A Person is not liable on an instrument unless the person signed it); See generally U.C.C. S. 3-104 (1990) (requirements for negotiability).

[vii] See for details, S 20 of the Information Technology Act, 2000 which runs as under

S. 20. : **Controller to act as repository.**

(1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall—

(a) make use of hardware, software and procedures that are secure its {correct after verification} intrusion and misuse;

(b) observe such other standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.

(3) The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

[viii] Of course, the holder of the private key may choose to divulge it, or may lose control of it (often called 'compromise'), and thereby make forgery possible. The Guidelines seek to address this problem in two ways, (1) by requiring the subscriber, who holds the private key, to use a degree of care in its safekeeping, and (2) enabling the subscriber to disassociate himself from the key by temporarily suspending or permanently revoking his certificate and publishing these actions in a "certificate revocation list." or "CRL". A verity of methods is available for securing the private key. The safer methods store the private key in a "cryptographic token" (one example is a "smart card") which executes the signature programme within an internal micro processing chip, so that the private key is never divulged outside the token and does not pass into the main memory or processor of the signer's computer. The signer must typically present to the token some authenticating information, such as a password, pass phrase, or personal identification number, for the token to run a process requiring access to the private key. In addition, this token must be physically produced, and biometric authentication such as fingerprints or retinal scan can assure the physical presence of the token's authorized holder. There are also software-based schemes for protecting the security of the private key, generally less secure than hardware schemes, but providing adequate security for many types of applications.

[ix] See, the information Technology (Certifying Authorities) Rules, 2000 Schedule V [Glossary] which define key pair as, 'KEY PAIR – In an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

[x] See, for detail, S.3 of the Information Technology Act, 2000 (21 of 2000)

[xi] http://www.state.co.us/gov_dir/gss/cec3/colo_rules.htm visited on 20.10.2006

[xii] In the first phase of its operation the services being offered are government to government. NIC offers four distinct classes of digital certification services, classes 0-3 for NICNET users within the government. For all its subscribers it issues class 2 digital IDs. These digital IDs are used to identify the subscriber on the net and are legally valid as they are backed by the Information Technology Act, 2000.

[xiii] Preamble of the Information Technology Act, 2000 runs as follows :

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 involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends inter alia that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.

[xiv] See, State of Punjab and Ors. Vs. Amritsar Beverages Ltd. and Ors. Civil Appeal No. 3419 of 2006 (Arising out of SLP (Civil) Nos. 10371-10374 of 2004) Decided On: 08.08.2006 [para 7] p. 3488. The Supreme Court observed,

> We may notice some recent amendments in this behalf Section 464 of the Indian Penal Code deals with the inclusion of the digital signatures. Sections 29, 167, 172, 192 and 463 of the Indian Penal Code have been amended to include electronics documents within the definition of Page 3489 'documents'. Section 63 of the Evidence Act has been amended to include admissibility of computer outputs in the media, paper, optical or magnetic form. Section 73A prescribes procedures for verification of digital signatures. Sections 85A and 85B of the Evidence Act raise a presumption as regards electronic contracts, electronic records, digital signature certificates and electronic messages.
>
> [para 8]

[xv] This shall be borne in mind that the amendment brought into effect by the Information Technology Act, 2000 in Evidence Act, 1882 has also create strong presumption in favour of electronic contracts, electronic records, digital signature certificates and electronic messages.

[xvi] Therefore, the term 'verify' has also been defined by the Act which prescribed the meaning and scope as follows :

S. 2 (1) (zh) "verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

[xvii] S. 2 (1) (f) of the Information Technology Act, 2000 which define "asymmetric crypto system" as follows:

> "asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

[xviii] S. 3 (4) of the Information Technology Act, 2000. See also, Duggal Pavan, Cyber Law – The Indian Perspective, Saakshar Law Publications New Delhi, 2nd Ed. 2004, pg. 65

[xix] S. 2 (1) (x) of the Information Technology Act, 2000 which define "Key pair" as follows :

> "key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

[xx] See S. 17 of the Information Technology Act, 2000 which runs as under

> 17. **Appointment of Controller and other officers**.
>
> (1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.
>
> (2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
>
> (3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
>
> (4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.
>
> (5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
>
> (6) There shall be a seal of the Office of the Controller.

[xxi] Id. S. 18

[xxii] For e.g. First digital Contract Note authenticated by digital signature had been issued by Mr. K.N. Gupta, the first Controller of Certifying Authorities, Government of India, has issued the first licence to "Safe Script" to act as a Certifying Authority. Another persons who were in line for the issue of licence were (1) RBI Affiliate, Hyderabad (2) Institution of Development Research and Banking Technology and, (3) National Informatics Centre et. The "Safe Script" had issued a digital signature certificate in the name of "ICICIDIRECT.COM", Mumbai. On March 27, 2002 the subscriber "ICICIDIRECT.COM", became the first firm to issue a Digitally Signed Contract Note (DSCN) to its clients [The Economic Times, Delhi Ed. 29.03.2002 Pg. 5]. The ICICIDIRECT.COM used to issue contract notes for about 22,000 transactions carried out per day. They are physically mailed to the investors. With the introduction of the new system, the investors will investors will instantly receive a legally valid contract note electronically. A report says that the new service is expected to save around Rs. 6 crores which were payable to the brokers.

[xxiii] See S. 19 of the Information Technology Act, 2000 which runs as under :

> 19. Recognition of foreign Certifying Authorities.
>
> (1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
>
> (2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
>
> (3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under subsection (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

[xxiv] See S. 20 of the Information Technology Act, 2000

[xxv] Ibid.

[xxvi] Id. S. 68

[xxvii] Id. S. 30

[xxviii] Id. S. 21

[xxix] Rule 4 of the Information Technology (Certifying Authority) Regulations, 2001 has prescribed the standards followed by the Certifying Authority for carrying out its functions.

[xxx] See, S. 21 of the Information Technology Act, 2000

[xxxi] Id. S. 23

[xxxii] Id. S. 25