JICLT

Journal of International Commercial Law and Technology
Vol. 7, Issue 3 (2012)

Authentication of Electronic Records: Limitations of Indian Legal Approach

Farooq A. Mir
Department of Law, University of Kashmir
Srinagar, India
far_lwtr@rediffmail.com

M. Tariq Banday
Department of Electronics and Instrumentation Technology,
University of Kashmir, India
sgrmtb@yahoo.com

Abstract. *Paper based documents have inherent authenticity and high evidentiary value for obvious reasons. The documents are permanent record of the contractual relationship of the parties and their contents cannot be so easily altered, modified or changed and even if any change is effected that can be easily detected. This is the reason that the Indian Evidence Act, 1872 excludes oral evidence in presence of documentary evidence. The moot point is that can an electronic record be treated equivalent to paper based record? In other words, can an electronic record have all the properties of the physical document appended with the hand written signature? This is necessitated by the fact that there are different laws in India providing that a contract is not valid unless it is in writing and signed by the parties. An attempt is made in this paper to analyze the provisions prescribing authentication of electronic records in India to demonstrate inherent limitations in them. To overcome these limitations, a new model of authentication is proposed which is based on digital signature combined with time stamping service.*

1. Introduction

Generally, law does not favor any particular mode of execution of commercial transactions save in exceptional situations where it is expressly provided that a commercial transaction be in writing and signed by the parties so as to be enforceable. This document is the record of the parties to an agreement and the signature is the stamp of a person's identity and marks his intention to commit himself legally. The commercial community has found these two requirements convenient to create legal relationship and forms now a well-established mode of executing business transaction.

The legal systems across the globe do not exhibit uniform requirements of writing and signature and legal efficacy of these requirements also vary. For instance, a promise made on account of love and affection between the parties having near relations with each other or a promise to pay time barred debt or something already voluntarily done is only unenforceable and not invalid if the promise is not in writing, signed and registered as is required under the Indian Contract Act, 1872. The same is true for the English Statutes of Fraud, which makes a transaction unenforceable in court and not invalid for lack of writing and signature by the parties to be charged.[1]

The formal requirements of legal transactions witnessed a great transformation in the present century and consequences of failure to satisfy these requirements have been greatly diminished. Leaving aside this

[1] Arthur, I., 1950, Corbin, Corbin on Contracts, pp. 20-23.

transformation, a legal system that does not ensure reliability and enforceability will not be acceptable to business community because growth of business cannot be expected in an uncertain legal environment.[2]

The requirements of writing and signature perform a variety of functions. The parties documenting their commercial relationship have a confidence that a permanent record of their transaction has been created which would not be unilaterally altered and would facilitate reproduction so that each party has a copy of the original contract.

This document becomes a tangible evidence of existence and nature of the intention of the parties executing it which can be ascertained by any one called to resolve their differences and can be used against or in favor of the party trying to establish its claim on the basis of it. When a person puts a mark in the distinctive manner on a written document in the form of a signature, he establishes a link between himself and the document and thus authenticates it because writing becomes attributable to the signer. The signer by virtue of his signature is identified with the document.

The advantages of reducing promises to writing and signed by the parties are many and varied. The parties become aware of the consequences of their entering into the contract and thus prevent inconsiderate engagements. The intention to commit themselves legally becomes manifest once signature is put on a written document and calls signer’s attention to the legal significance of the act. This eliminates possibility of any casual relationship and takes parties by their words put in the document.[3]

The signature on a document is not only stamp of person’s identity but also implies approval on his part to contents of the document. The writing itself may not sometimes be sufficient to reflect assent of the party. The signature demonstrates willingness on the part of the signer to be part and parcel of the deal. The signature symbols the finality of the deal. It marks the *consensus ad idem* of the parties – *a sine qua non* for every commercial transaction. It brings certainty and clarity in the transaction and thus lessens the burden of inquirer, as there remains hardly anything to prove beyond the face of the document.[4]

Traditional methods of communication of information for executing a commercial transaction have considerably changed. The documents can be executed in electronic form without having any physical shape. But the plain electronic record is highly insecure and does not possess all the properties of the paper based document unless it is appended with digital or electronic signature created by any encryption procedure which will be functionally equivalent to the paper based document appended with a hand written signature.

Most of the nation states have demonstrated unanimity in enacting that a signature, contract, or other record may not be denied legal effect, validity, or enforceability solely because it is in electronic form.[5] In effect, an electronic record has the same authority as other paper record provided it is appended with an appropriate electronic or digital signature that is i) under the control of the signer, ii) unique, iii) identifiable, iv) unalterable, and v) carry indication of the individual’s intent to sign.

The Information Technology Act 2000 (IT Act)[6] in India was initially technology specific in relation to authentication of electronic records. The authentication of electronic records was made possible only by digital signatures but now realizing the limitation of this technology specific legislation; the Indian Parliament has

[2] Braunstein Michael, 1989, Remedy, Reason and the Statute of Fraud: A Critical Economic Analysis, Utah L. Rev, Vol. 1989, pp. 383.
[3] Ian Lloyd, 1997, Legal Barriers to Electronic Contracts: Formal Requirements and Digital Signatures in Lilian Edwards and Cherlotte Waelde (Ed.), Law and the Internet Regulating Cyberspace, pp. 142.
[4] Landrock P. and Anderson M. B., 1996, Encryption and Interception, CLSR, Vol. 12, pp. 342.
[5] See for instance, US, Malaysia, and Singapore.
[6] IT ACT 2000, 2000, The Information Technology Act, 2000, Government of India, http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/itbill2000.pdf.

recently amended IT Act which has now, in addition to digital signatures, prescribed electronic signatures for authentication of electronic records. [7]

2. Digital Signature

The digital signature is an electronic analogue of a written signature; it can be used to provide assurance that the claimed signatory signed the information. In addition, a digital signature may be used to detect whether or not the information was modified after it was signed (i.e., to detect the integrity of the signed data). These assurances may be obtained irrespective of the fact whether the data was received in a transmission or retrieved from storage. A properly implemented digital signature algorithm that meets the requirements of this Standard can provide these services[8].

The IT Act defines digital signature as an authentication of an electronic record by a subscriber by applying asymmetric cryptosystem and hash function which envelop and transform initial electronic record into another electronic record[9]. The subscriber means a person in whose name the digital certificate is issued [10]. The electronic record means data, record, or data generated; image or sound stored, received or sent in an electronic form [11]. The term "electronic form", with reference to information means, any information generated, sent, received or stored in media, magnetic, optical, computer memory or similar device. [12] The word "data" and "record" in the definition of "electronic record" has to be interpreted liberally. Otherwise, the definition will be unnecessarily restrictive in scope, as it does not mention, for example, text, graphics, video or multimedia services. However, one may argue that the definition of "electronic form" provided in the IT Act widens the scope of the definition of the electronic record by including the words "any information". These two definitions have to be read conjunctively and the words "any information" used in the definition have to be construed with reference to the content provided in the definition of "electronic records".

A more flexible approach has been adopted in the proposed draft of Uniform Commercial Code (UCC),[13] which provides that a record means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. American Bar Association Guidelines[14] [14] have used the word "message" in the definition of digital signature and in its explanatory notes; it has made clear that the "expression message" is similar to the definition of "record" in proposed draft of UCC.

One of the procedures for authentication of the digital records prescribed under the IT Act is a combination of the asymmetric cryptosystem[15] and Hash function[16] . The asymmetric cryptosystem that is also known as public key cryptosystem uses two different but mathematically related keys. One key is called private key and another public key. Every person who wants to transmit his/her message over the Internet by using asymmetric cryptosystem must have two keys. The private key has to be kept secret and if one loses its control, which in

[7] The IT (amendment) Act 2008, 2008, The Information Technology (Amendment) Act, 2000, Government of India, http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf
[8] Write, B., 1995, Eggs in Basket, Distributing the Risk of Electronic Signatures, Computers and Law, Vol. 6, pp. 30.
[9] Section 3(2) of IT Act.
[10] Section 2(zg) of IT Act.
[11] Section 2(t) of IT Act.
[12] Section 2(r) of IT Act.
[13] UCC, 1962, UNIFORM COMMERCIAL CODE Act 174 of 196, http://www.michigan.gov/documents/entireuccbook_18831_7.pdf
[14] American Bar Association, http://www.americanbar.org.
[15] Zheng. Y., Imai. H. and Imai, H. (Ed.). 2007. Public Key Cryptography, Springer, ISBN: 9783540656449.
[16] S. Lucks, 2005, A failure-friendly design principle for hash functions. In Proceeding of ASIACRYPT 2005, volume 3788 of LNCS, pages 474–494.

technical language is called compromise, it makes information vulnerable to interlopers. The public key has to be made available to public.

In Public Key Cryptography (PKC) encryption keys come in a pair, each key pair is different from the other key in the key pair, although the keys are mathematically related to each other. The mathematical relationship between the keys is such that the following holds true:

(1) Data encrypted with one encryption key can only be decrypted with the other key of the pair which means that data encrypted by private key will be decrypted by the public key and data encrypted by the public key can be decrypted by the private key. This is known as two directional function of public key algorithm or reversibility function.

(2) If the length of the encryption key (measured in bits) is sufficient, it will be practically impossible for anyone in possession of one key of the key pair to determine the other key.

Asymmetric crypto system is to be combined with hash function so as to create a digital signature. Hash function is a function which operates one sequence of characters to produce a result. It is defined as an algorithm mapping or translation of one sequence of bits into another, generally smaller set known as hash result which should yield the same hash result at every time when the algorithm is executed with the same electronic record as its input. Hash function must possess the following three characteristic features.

a) That a message yields the same hash result every time the algorithm is executed using the same message as input;

b) It is computationally infeasible that a message can be derived or reconstituted from the hash result produced by the algorithm;

c) It is computationally infeasible that two messages can be found that produce the same hash result using the algorithm.[17] .

2.1 Working of Digital Signature

The working of digital signature is shown in figure 1 . It demonstrates steps required for signing and encrypting a message by the sender and corresponding steps required for decrypting and signature verification by the receiver.

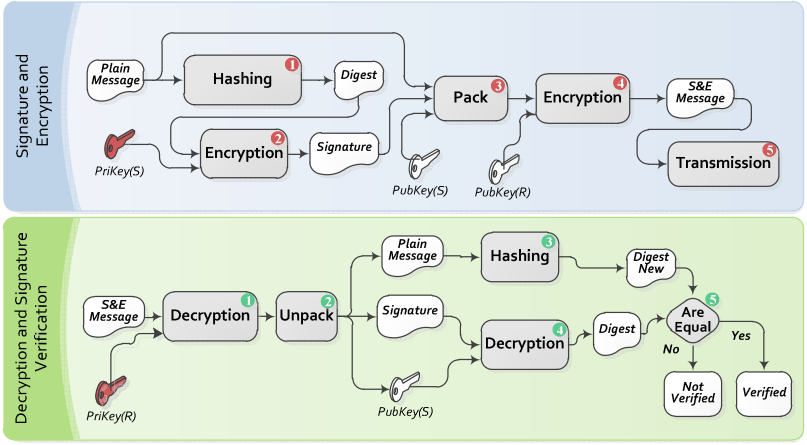

Figure 1: Working of Digital Signature

[17] Explanation to section 3 of IT Act.

The plain message to be sent is to be first identified. Hash function is then applied to this plain message to get its digest. This digest is encrypted by the private key of the sender (PriKey(S)) to get its signature. The plain message together with the encrypted signature and public key of the sender (PubKey(S)) is again encrypted but with the public key of the receiver (PubKey(R)) which is then sent to the sender.

The receiver will first use his private key (PriKey(R)) to decrypt the electronic record. This will give him plain message, encrypted signature and public key of the sender (PubKey(S)). The receiver will then apply the same hash function to the plain message and will get new digest. He will then decrypt the signature with the help of the public key of the sender (PubKey(S)) to get the digest back. If the two digests match, the signature is verified but not otherwise. If the two digests match, the assurance is that the message has not been changed in transmission and the message is original. The public key of the sender has successfully decrypted the signature; the assurance is that the message has come from the sender and not from any other person, thus authenticating the sender. The message has also remained confidential as it has been encrypted by the public key of the receiver who alone can decrypt it with the help of his private key. Thus, all the three critical features namely authenticity, integrity and confidentiality are achieved by applying asymmetric crypto system with hash function.

3. Electronic Signature

The electronic signatures may be an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record[18] [18]. It can be in the form of simply typing one’s name, signing an electronic pad, or entering a Personal ID or password. No specific technology needs to be used in order to create a valid electronic signature.

The original IT Act was technology specific which would not have allowed the use of other technologies for authentication. This approach had inherent limitations. The IT related technologies are constantly evolving. The new technologies are more dependable, with added features, user friendly and cheaper. The benefits of new technology could not have been reaped by making the IT Act technology specific. This technology specific provision was also not in harmony with the laws of other jurisdictions and more particularly with the Model Law on Electronic Signatures[19] adopted by the United Nations Commission on International Trade Law (UNICITRAL) Vide its resolution No. 56/80 dated 12th December, 2001. This resolution recommended that all states accord favourable considerations to the said Model Law on electronic signatures. In order to harmonize the IT Act with the Model Law, it became necessary to provide for alternative technology of Electronic Signatures that was done through the IT (Amendment) Act, 2008.

The IT (Amendment) Act now gives an option to the subscriber to authenticate his electronic record by electronic signature or electronic authentication technique. The electronic documents can be now authenticated either by the digital signature or electronic signature. However, only such electronic signature or electronic authentication technique can be used for authentication of the electronic records which:

a) Is considered reliable; and
b) May be specified in the Second Schedule of the IT Act

Section 3-A of the IT Act provides that any electronic signature or electronic authentication technique shall be considered reliable if:

a) The signature creation data or authentication data are within the context in which they are used , linked to the signatory or as the case may be, the authenticator and to no other person;

[18] Electronic Signatures in Global and National Commerce Act 15 USC 700, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws &docid=f:publ229.106.pdf

[19] UNCITRAL. 2001, UNCITRAL Model Law on Electronic Signatures with Guide to Enactment, United Nations Publication, Sales No. E.02.V.8, ISBN 92-1-133653-8, http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf.

b) The signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and to no other person;
c) Any alteration to the electronic signature made after fixing such signature is detectable; and
d) Any alteration to the information made after its authentication by electronic signature is detectable; and
e) It fulfils such conditions which may be prescribed.

The electronic signatures, like hand written signatures, can be forged. It is to be verified whether the signature purported to be affixed by the subscriber really belongs to him. The Government of India may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated. The Government of India may, by notification in the official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule. Every such notification shall be laid before each house of Parliament. Provided that no electronic signature or authentication technique shall be specified in the second schedule unless such signature or technique is reliable. [20]

4. Secure Electronic Records and Secure Electronic Signature

A message sent over an open network like the Internet may pass through several computer systems; each owned and operated by different entities. At every stage, the message is vulnerable to attack. Similarly, an electronic record available on any computer system can be altered, modified or altogether changed at much greater ease than the information available on paper based document.

The authenticity, integrity and non -repudiation required in any legal system for a record to form basis of a claim be achieved either by secure system or secure data.

The IT Act provides that a secure system means computer hardware, software and procedure that:

a) Are reasonably secure from unauthorized access and misuse;
b) Provide a reasonable level of reliability and correct operation;
c) Are reasonably suited to perform the intended functions; and
d) *Adhere to generally accepted security procedure.* [21]

Further, section 14 provides that where any security procedure has been applied to an electronic record at a specified point of time, then such record shall be deemed to be secure electronic record from such point of time to the time of verification.

Similarly, section 15 provides that an electronic signature shall be deemed to be a secure electronic signature if:

a) The signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person;
b) The signature creation data was stored and affixed in such exclusive manner as may be prescribed.

The Government of India shall for the purposes of the Act prescribe the security procedure and practices. The Government of India, while providing such procedures and practices, shall have regard to:

a) The commercial circumstances
b) Nature of transactions and

[20] Section3-A (3) & (4) of IT Act.
[21] Section 2 (ze) of IT Act.

c) Such other related factors as it may consider appropriate.

These electronic records are prone to unauthorized modification or alteration and even can altogether be changed. In order to prevent an electronic record from such unwanted changes, it has to be “secured”. It becomes secured electronic record only when security procedure is applied to it. This security procedure enables to identify whether the electronic record is that of the purported sender, detects any alteration or errors in the communication, contents or storage of the electronic record since the time it was applied. The essential feature of a secured record is that it has not been altered in the course of storage. If it has been signed by a secure electronic signature, it will have that characteristic.

Electronic signatures can be forged also. Anyone having access to the electronic signatures of others can impersonate them. To prevent such obnoxious activities, various security procedures can be applied to an electronic signature such that it can be verified that (a) the signature is the same which it was at the time it was affixed, (b) it is unique to the subscriber affixing it, and (c) it is capable of identifying such subscriber as the signatory who is under the exclusive control of the means enabling to create signature.

3.1 Limitations of the IT Act

The IT Act provides two procedures for authentication of electronic records and then creates rebuttable presumption under section 85B of the Indian Evidence Act like Section 18 of the Electronic Transactions Act of Singapore for secure electronic record and secure electronic signatures. The presumption is that the secure electronic record or signature has not been altered since the specific point of time to which the secure status relates and the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record. The authenticity and integrity of the electronic record or any electronic signature shall be presumed unless proved otherwise.

The question to be answered is: is digital signature created by asymmetric cryptosystem and Hash Function per se secure? Or still it has to pass tests laid down under section 14.The provisions relating to secured electronic record and signature have been borrowed from the Singapore Electronic Transactions Act. However, this Act is technology neutral and quite rightly provides that electronic record and electronic signature shall be deemed to be secure if they have the prescribed properties. As against this, the IT Act prescribes digital signatures and electronic signatures for authentication of electronic records. A particular procedure has been prescribed for creating digital signature but obviously no such procedure has been laid down for creating Electronic signature instead certain properties have been prescribed which an electronic signature must satisfy in order to be legal valid. If an electronic record has been authenticated by digital signature, it will have all those properties that have been prescribed for electronic signature. This means that an electronic record authenticated by digital signature shall be per se secure but an electronic record authenticated by an electronic signature has to satisfy the requirements laid down under section 14. However, IT has not recognized this fundamental difference between Digital and electronic signatures.

4. Legal Validity of Authenticated Electronic Records

The IT Act has accorded legal recognition to electronic signatures. It has been provided that where there is a legal requirement that any 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 electronic signature affixed in such manner as may be prescribed by the Central Government. [22].

[22] Section 5 of IT Act.

As mentioned above, authentication of the electronic records is possible by the digital or electronic signature but surprisingly the IT Act gives legal recognition to the electronic signatures only. This in fact is a drafting mistake because prior to the amendments in the IT Act in 2008, legal recognition was accorded to the digital signatures by the above provision. The amendment Act has now recognized electronic signatures also for authentication purposes. The term digital signature was replaced by the term electronic signature without realizing that digital signatures, in addition to electronic signatures, can still be used for authentication of the documents. There is a separate definition of the digital signature and it is not being used interchangeably with electronic signature. The IT Act should have expressly accorded recognition to both Electronic as well as Digital signatures.

5. Limitation of Authentication Procedure

The Indian Contract Act (IC Act) allows the parties to a contract to revoke the offer or acceptance as the case may be. This revocation is possible only within a certain period of time and not afterwards[23]. Thus the date and time for communication or receiving of an offer or acceptance becomes crucial.

Similarly, the law of limitation in India prescribes different timings for filing various suites. If a suite is filed beyond the prescribed time limit, it can be dismissed because the remedy is barred by time. Thus the date on which the cause of action arose and the date when the actual suit was filed becomes crucial as the outcome of the suite at the initial stage hinges on the question whether it has been filed within the prescribed time period or not. The time is equally crucial in all those situations where electronic communications are substituted for conventional methods of communications.

The procedure prescribed for authentication of electronic records under the IT Act does not authenticate time. There are many techniques available that can spoof or sniff data as well as time. Sniffing [24] and spoofing [25] are security threats that target the lower layers of networking infrastructure supporting applications that use the Internet. Users do not interact directly with these lower layers and are completely unaware of their existence. Spoofing is an active security attack in which one machine on the network masquerades as a different machine. As an active attack, it disrupts the normal flow of data and may involve injecting data into the communication links between other machines. This masquerade aims to fool other machines on the network into accepting the impostor as an original, either to lure the other machines into sending it data or to allow it to alter data. The word “spoof” means deception or intended to trick one into accepting as genuine something that is actually false. Such deception can have grave consequences because notions of trust are central to many networking systems. Sniffing may seem innocuous depending on just how sensitive and confidential you consider the information on your network. Some network security attacks use sniffing as a prelude to spoofing. Sniffing gathers sufficient information to make the deception believable.

The different legal requirements cannot be met simply by providing authentication procedure for electronic records; it is to be blended with the time stamping service which would authenticate time for receipt and dispatch of electronic records.

[23] Sections 4 & 5 of IC Act.

[24] Derek Atkins, Paul Buis, Chris Hare, Robert Kelley, Carey Nachenberg, Anthony B. Nelson, Paul Phillips, Tim Ritchey, and William Steen, 1996, Internet Security Professional Reference, New Riders Publishing, pp. 257.

[25] John Peter Jesan, 2006, Information Security, Ubiquity, DOI: 10.1145/1117693.1117695, http://ubiquity.acm.org/article.cfm?id=1117695.

6. Time Stamping

A time-stamping service supports assertions of proof that a datum existed before a particular time [26] . In order to associate a datum with a particular point in time, a Time Stamp Authority (TSA) may need to be used. This Trusted Third Party provides a proof-of-existence of a particular datum at a given time. The TSA can also be used to indicate the time of submission when a deadline is critical, or to indicate the time of transaction for entries in a log. A Digital Time Stamping Service (DTS) issues timestamps which associate a data and time with a digital document in a cryptographically strong way. The Digital Time Stamp can be used at a later date to prove that an electronic document existed at the time stated on its time stamp.

When a time stamp is added to a signature then there is an external witness. The process of adding a time stamp to a signature does not send the document outside one's computer. Time stamping does not compromise the privacy of one's document - only a hash of the signature is sent to Time Stamping Authority to create the timestamp.

6.1 Model for Time Stamping Digital Signature

One of the major uses of time-stamping is to time stamp a digital signature to prove that the digital signature was created before a given time[27] . This enables a person to know whether the digital signature was affixed on the electronic record before it was time stamped and whether the digital signature was created before or after the revocation of digital signature certificate. Figure 2 demonstrates the use of time stamping appended to the digital signature for ensuring the correctness of date and time of the signature.

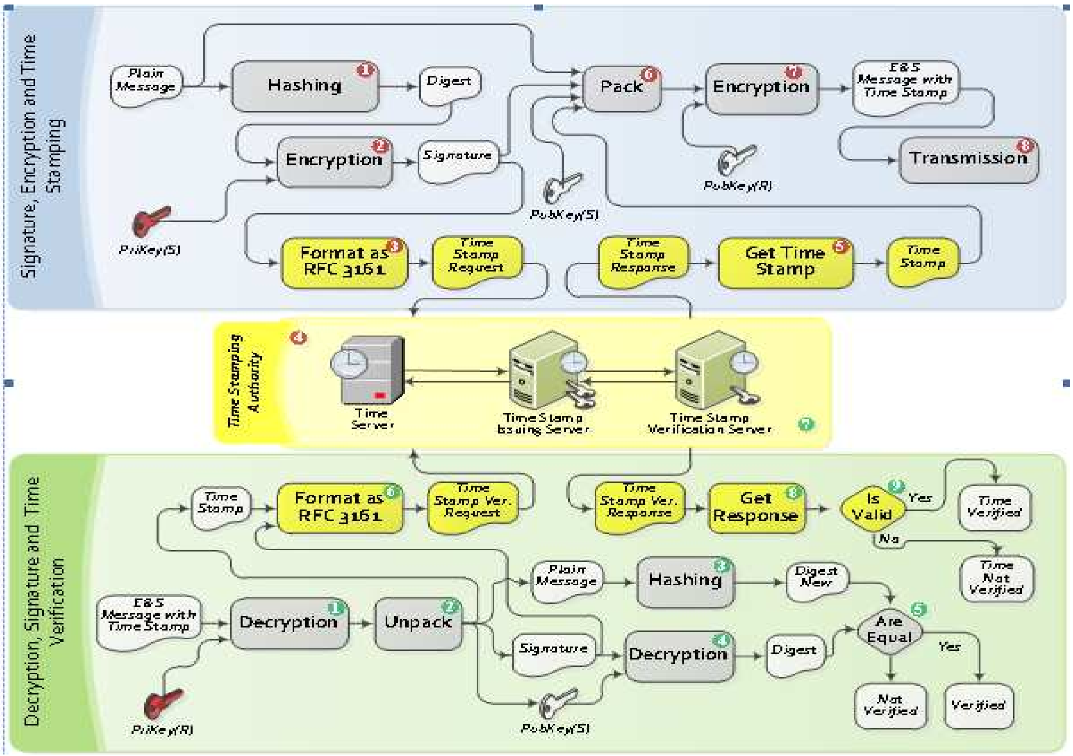

Figure 2 : **Use of time stamping to time stamp digital signature**

[26] Adams., et al (2001), Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC 3161, p. 17.
[27] Id.

As shown in figure 2 above the message digest is computed in step 1 and in step 2 the signature is generated which is formatted as RFC 3161 time stamp request in step 3. It is submitted to a trusted time stamping authority in step 4, which generates a time stamp response containing the time stamp in step 5. The time stamp is packed with the plain message, signature and public key in step 6 to form a packed message which is encrypted in step 7 using the public key of the receiver and the resultant encrypted and signed message containing time stamp is transmitted to the receiver in step 8. The above process is to be reversed by the receiver in the following steps.

The encrypted and signed message along with time stamp is decrypted by the receiver by using his private key in step 1 which is unpacked into the individual components (time stamp, plain message, signature, public key of sender (*PubKey(S)*) in step 2. The signature is verified as discussed in section 2 above (steps 3 to 5). The time stamp and the signature are formatted as RFC 3161 format in step 6 to produce a time stamp verification request which is submitted to the trusted time stamping authority for verification in step 7. The time stamping server replies with a time stamping verification response containing the time validation in step 8. The date and time of digital signature is verified in step 9 as correct in case the time validation response is positive and not otherwise.

The Government of India has recently issued interoperability guidelines,[28] which have created sub-CAs. It has been made mandatory that a CA with sub-CA must necessarily issue end entity certificates only through its sub-CAs. The only exception is for code signing and time stamping certificates which may directly be issued by CAs. These guidelines however, not made affixing of time stamp mandatory.

7. Conclusion

The IT Act in India is the only legislation that governs electronic transactions and for that purpose prescribes procedure for authentication of electronic records and signatures. Initially, the IT Act was technology specific and had prescribed a particular procedure for authentication of the electronic records. This procedure has its own limitations. This legal position now stands changed after the amendments in the IT Act. The IT Act has now, in addition to digital signature, provided electronic signatures for authentication of the electronic records. However, necessary fine tuning has not been done in other provisions so as to remove inconsistency in them.

The procedure prescribed for authentication of electronic records cannot be helpful in those transactions where time is crucial and determinant of the rights and obligations of the parties. This is the reason that it is suggested that time stamping service may also be made mandatory for authentication of the electronic records.

* * * *

Cite as: Farooq A.Mir & M. Tariq Banday, *Authentication of Electronic Records :Limitation of Indian Legal Approach* , Journal of International Commercial Law and Technology, vol.7 Issue 3 (July, 2012)

[28] CCA. 2009. Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act, CCA India, version 2.4 updated on 14th June 2011, http://cca.gov.in/rw/resource/dsc _guidelines_r2_4.pdf.