ISSUES RELATING TO ELECTRONIC AND DIGITAL SIGNATURES

Manirani Dasgupta*

ABSTRACT

The documents, records as well as information or data should be retained for a specific period to be accessible and usable for a subsequent reference. The retention of electronic records must be in original form as generated, sent or received indicating the identification of origin, destination, date and time of dispatch or receipt of such records except such e-records as are automatically generated solely to enable to be dispatched or received as e-record, for example, format of e-mail must be received or dispatched in the form of e-record or information which are solely generated for this purpose and therefore question of retention in original format of the same is not disputable. The e-record will be treated as original format as generated, sent or received when it will indicate details of its creation, sending and receipt. Creation in this context is not necessarily typing by the user rather on behalf of user any one can type or create the document. Digital Signature is the use of electronic and statutory method to authenticate electronic record by anyone who subscribes it through digital signature certificate issued by appropriate authority appointed for this purpose by the Central Government. It is very difficult to define the term digital signature in precise form. Article 2 (a) of the United Nations Model Law on Electronic Commerce, 85th plenary meeting on digital signature, 12th Dec' 2001, defines the term 'Electronic Signature'. In India, according to section 2(p) of the Information Technology Act, 2000 '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 of the Act. Section 2 sub-sections (ta) and (tb) were inserted by the Information Technology (Amendment) Act, 2009 which defines 'Electronic Signature' and 'Electronic Signature Certificate' respectively to authenticate electronic record in electronic technique not to supplant but to supplement the Digital Signature and the Digital Signature Certificate. Authentication of electronic records and electronic signature must be following procedure prescribed under sections 3 and section 3A of the Information Technology Act, 2000 in India. The procedure is called affixing electronic signature or digital signature. That is adoption of specific method or procedure by means of electronic signature for its authentication. Any person can affix digital signature or electronic signature on his electronic record. Authentication shall be effected by use of asymmetric crypto system and hash function which envelop and transform initial electronic record into another electronic record which are reliable and according to second schedule. This function has to be completed by Key pair. In key pair there are private key and public key. Keys are unique to the subscriber and constitute a functioning Key Pair. If corporate sectors, government and individuals use their own digital or electronic signatures on maintaining level of confidentiality and privacy then it will be definitely helpful to prevent and control unauthorized access to data and related acts and can hope for authenticity, integrity and non-concealment of e-data which are transferred.

Key words: Education, Philosophy, Value Education, Teacher.

Introduction

The documents, records as well as information or data should be *retained for a specific period to be accessible and usable for a subsequent reference*. The retention of electronic records must be in

*Associate professor, Department of Law, University of Calcutta.

original form as generated, sent or received indicating the identification of origin, destination, date and time of dispatch or receipt of such records except such e-records as are automatically generated solely to enable to be dispatched or received as e-record[1] for example, format of e-mail must be received or dispatched in the form of e-record or information which are solely generated for this purpose and therefore question of retention in original format of the same is not disputable. The e-record will be treated as original format as generated, sent or received when it will indicate details of its creation, sending and receipt. *Creation* in this context is not necessarily typing by the user rather on behalf of user any one can type or create the document. For example, in a cyber café or office on behalf of A, Y may type a document and A after verification of the same may save it or send it to X as e-mail attachment through A's e-mail address. Here generator of the record is A and original format is as verified, approved and sent by A to X. X is the recipient and the document as received by X in the original form without tampering or changing the format, style and so forth will be treated as original form. Here X must not convert e-document into *W* or MS word document format or should not make copy-past in any file or folder changing format, style, colour, font size or anything else rather he has to save it as it is in the original format sent by A and received by him. Then only it will be treated as primary evidence and original document.

However, where there is express law relating to retention of electronic documents, records or information, section 7(1) of the Information Technology Act, 2000 will not be applicable and that special provision will prevail. For example, section 5 of the Trade Mark Act, 1999 provides that in Trade Mark Registry Office the register must be kept in manual form and in electronic form such as in floppy disk or hard disk which must be circulated to all branch offices from head office and the Registrar shall take care of it. Not only that, rules, regulations, orders, bye-laws, notifications or other matters of the Government if published in official gazette or electronic gazette, the date of publication shall be deemed to be the date of the gazette or media in which it was first published in any form whether electronic or manual.[2] On the other hand, with reference to sections 6 to 8, though e-records and e-signature have legal sanctity but it is not a matter of right of any one to claim that any appropriate Government or Government authority should accept, issue, create, retain and preserve any document in electronic form or effect any monetary transaction in the electronic form.[3] Therefore, inspite of wide use e-records are not compulsory for every transaction and communication. So, e-publications of government records are subject to official secrecy and confidentiality.

Electronic money transaction without proper safeguard tends to create several problems, for example, ATM fraud and fraud in banking transactions, fraud in financial transactions, internet fraud, credit card fraud and so forth are increasing day by day. Criminals in cyberspace are very often misusing and abusing e-banking and e-financial transaction facilities. Hackers in cyberspace unauthorisedly access password and source code of the users and institutions to commit economic crimes and other cyber crimes e.g. theft, denial of service attack, flowing of virus, spamming and so forth. If separate machine is used only to keep e-record without internet or network connection, there will be 100% safety and security of data. For example, Calcutta University Law Department and Technology Department having their own network to exchange data within two departments and no computer of these two departments is connected with internet. There will be very little chance of data tampering, misuse or crime in respect of the records. But if one computer is connected with internet, there will be chance of direct as well as remote cyber

[1]. For detail see section 7(1) the Information Technology Act, 2000.
[2]. For detail see section 8 of the Information Technology Act, 2000.
[3]. For detail see section 9 of the Information Technology Act, 2000.

attack through *I-Way*. Therefore, nowhere is safe in cyberspace without standard security and control. On the other hand if we advocate use of separate machine only for keeping records without internet connection, it is a bar to advancement and sanctity of Information Communication Technology (ICT) and it will bring us back to the genesis of computer and development of ICT because without communication processing facilities a machine can be treated as a calculator but not a computer.

The Concept of Digital Signature

The concept of Digital Signature was first evolved by Whitfield Diffie and Martin Hellman in the year 1976 and thereafter Ronald Rivest, Adi Shamir and Len Adleman invented the RSA algorithm to be used for Digital Signature. The first widely marketed software package to offer digital signature by them was totus Notes I.O. released in the year 1989. Though, Silvio Micali Ronald Rivest and Shafi Gold Wasser fist thought about the security system of Digital Signature. Digital Signature is the use of electronic and statutory method to authenticate electronic record by any one who subscribes it through digital signature certificate issued by appropriate authority appointed for this purpose by the Central Government. It is very difficult to define the term digital signature in precise form. Article 2 (a) of the United Nations Model Law on Electronic Commerce, 85th plenary meeting on digital signature, 12th Dec' 2001, defines the term 'Electronic Signature'. It runs as follows: 'Electronic Signature' means data in electronic form affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message. Article 2(b) of the United Nations Model Law on Electronic Commerce states that a 'Certificate' means a data message or other record confirming the link between a signatory and signature creation data. According to section 2(p) 0f the Information Technology Act, 2000 (IT Act); 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 of the Act. Section 2 sub-sections (ta) and (tb) were inserted by the Information Technology (Amendment) Act, 2009 which defines 'Electronic Signature' and 'Electronic Signature Certificate' respectively to authenticate electronic record in electronic technique not to supplant but to supplement the Digital Signature and the Digital Signature Certificate.

Authentication of electronic records and electronic signature must be following procedure prescribed under sections 3 and section 3A of the Information Technology Act, 2000 in India. The procedure is called affixing electronic signature or digital signature. That is adoption of specific method or procedure by means of electronic signature for its authentication.4 Any person can affix digital signature or electronic signature on his electronic record.5 Authentication shall be effected by use of asymmetric

4. For detail see Section 2(ta) and (tb) of the Information Technology Act, 2000.

5.Section 2 (d) "Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature". (f) "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; (g) Certifying Authority" means a person who has been granted a license to issue a Electronic Signature Certificate under section 24; (h) "Certification Practice Statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Electronic Signature Certificates; (q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35; (t) "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(ta) (Inserted by proposed ITAA-2006) "electronic signature" means authentication of any electronic

crypto system and hash function which envelop and transform initial electronic record into another electronic record6 which are reliable and according to second schedule.7 This function has to be completed by Key pair. In key pair there are private key and public key. Keys are unique to the subscriber and constitute a functioning Key Pair.8 For the verification of the electronic record the subscriber needs to use his public key.9 The Central Government may prescribe the procedure10 and publish it in the official Gazette to add or omit such procedure for affixing digital signature from the second schedule11 depending on its reliability.12

Therefore, whosoever uses information technology to communicate, data exchange or transmit information for online contract, regular business affairs, to provide Government services or personal use must use electronic or digital signature in the electronic record by using *asymmetric crypto system* and *hash function,* to protect data in cyberspace and prevent misuse or abuse of information; to authenticate data and to prevent data from any abuse or misuse. Hash function envelops it and transforms original document and authenticates original document with secure digital signature. The document will be treated reliable if it contains digital signature under verification process. There will be very little chance of tampering or misuse of data. Specially, Government sectors while using e-records must always use secure electronic or digital signature for its authentication and reliability.

Security of E-records and E-signature

When electronic signature is under the process of verification of keys till verification completes, data is under the exclusive control of signatory during the time of affixing signature and it is stored, controlled and affixed in exclusive manner[13] using private key, then it will be treated as secure electronic

---

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

(tb) "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate"

(x) "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;

zc) "Private Key" means the key of a key pair used to create a digital signature;

(zd) "Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(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.

(t) Defines the term electronic record that.....

(p) defines the term Digital Signature that it means authentication of any electronic record by a subscriber by means of an electronic method or procedure according to section 3 of the IT Act, 2000 .

6. For detail see Section 3(1) of the Information Technology Act, 2000.

7. For detail see Section 3A(1) and (2) of the Information Technology Act, 2000.

8. For detail see Section 3(4) of the Information Technology Act, 2000.

9. For detail see Section 3(3) of the Information Technology Act, 2000.

10. For detail see Section 3A(3) of the Information Technology Act, 2000.

11. For detail see Section 3A(4) of the Information Technology Act, 2000.

12. For detail see Section 3A(4) proviso of the Information Technology Act, 2000.

13. For detail see Section 15 of the Information Technology Act, 2000.

signature. So, the security system starts from the time of application of security procedure[14] to the time of its verification in case of electronic records.[15] Then it will be treated as Secure Electronic Record. However, in case of digital signature, the signature creation data means the private key of the subscribers. For using the same the user needs to receive a certificate, which contains public key, from certifying authority authorised by the Controller and the Central Government. In e-governance use of secure digital signature must be compulsory in confidential and important data for authentication and reliability to citizens.

Legal Recognition of Digital Records, Electronic Signature and Digital Signature

Where law requires information or records compulsorily in writing or typewriting or printed form, such law recognises electronic records when such information or matters are (a) rendered or made available in an electronic form; and (b) accessible so as to be usable for a subsequent reference. Therefore, only availability in an electronic form is not enough rather for legal recognition it must be accessible and usable for any subsequent reference. Where it is legal compulsion to sign or bear electronic signature, it shall be deemed to have been satisfied where the requirements are fulfilled.[16] Where law requires that information or any matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature then that information or record must be authenticated by affixing electronic signature, earlier which was digital signature, according to the prescribed manner. However, explanation to section 5 of the I T Act, 2000 provides that 'signed' means affixing of his hand written signature or any mark on any document and the 'signature' shall also mean accordingly.[16a] Electronic records and electronic signatures are recognised and approved for the e-transaction in Government and its agencies according to format and fees prescribed by the Central Government.[17]

The United Nations 85th plenary meeting on Digital Signature, 12th Dec' 2001, Article I provides that e-signatures are applicable in the commercial activities without affecting rule of law for the protection of consumers. Article 3 deals with equal treatment of e-signatures, except article 5 where variation may be caused by valid agreement and in fulfillment of the requirements referred to in article 6, Para I and other applicable laws. Article 6 provides for recognition of electronic signature. Para 1 provides that where signature is legally compulsory for data message if an electronic signature is used that will be reliable and appropriate communication. It is applicable and reliable in every circumstances including relevant agreement. Therefore, Para 2 provides that electronic signature is applicable in case of legal obligation and where law provides consequence in absence of a signature.

Jurisdiction

E-record will be treated as attributed to the originator when it is proved that it was sent by originator himself or his authorised person or by information system programmed by or on his behalf to operate automatically.[18] For the date and time of dispatch and receipt of e-record we have to depend on the time when it enters the designated computer resource, when it is retrieved by addressee or when it enters into the computer resource of the addressee.[19] So for the jurisdiction or place of sent and receipt of records

---

14. For detail see Section 14 of the Information Technology Act, 2000.
15. For detail see Section 16 of the Information Technology Act, 2000.
16. For detail see Section 5 of the Information Technology Act, 2000.
16a. See also The IT (Security Procedure) Rules, 2004 rules 3 and 4.
17. For detail see Section 6 of the Information Technology Act, 2000.
18. For detail see Section 11 of the Information Technology Act, 2000.
19. For detail see Section 13(2) of the Information Technology Act, 2000.

are concerned, it is the place of their business[20] though location of computer resource and place of business of originator and addressee are different.[21] The principal business place will be treated as place of business where there are several business places of concerned person. And if either one has no business place thir usual place or residence will be treated as place of business. For a Corporate body, it is the place of registration.[22] For example, X enters into an agreement with Y. X is residing at Kolkata and Y is residing at London. X sent e-copy of agreement to Y while he visited Delhi through Delhi based Cyber café and Y received it while he was at Singapore. Here place of agreement will be Kolkata or London or residential address of either X or Y, or if they are registered Company, the place of business, in case of several branches principal place of business, if no such place of business then place of registration and where nothing is working then place of server. And under section 75 of the Information Technology Act, 2000 only reasonable and incidental link to Indian Computer is enough to settle jurisdictional issues. Therefore, Delhi and Singapore are also important to determine jurisdiction in cyberspace.

Certifying Authority

Central Government
Controller
Certifying Authorities
Subscribers
Users

The Central Government may by notification appoint the Controller and other officers who shall use office seal of the Controller.23 For the purpose of regulation and functions of Certifying Authority, the Controller may recognise any foreign Certifying Authority for the purpose of this Act with previous approval of the Central Government and by notification in the official gazette and their activities will be treated as valid until the Controller revokes such recognition.24 Article 12 of the UN Model Law on Digital Signature provides for recognition of foreign certificates and electronic signature and states that it will have similar legal effect as in one's own country if it has substantial and equivalent level of reliability according to international standards or parties may agree between themselves regarding the same. Any person, who is eligible under section 21(2) of the Information Technology Act, 2000 may make application to the Controller for a license to issue e-signature certificates. The essential requirements are qualifications, expertise, manpower, financial resources and other infrastructure facilities which are essential to issue such certificates as prescribed by the Central Government. This licence, once granted, shall be valid for the period as the Central Government may prescribe and shall not be transferable or heritable but subject to terms and conditions as may be specified by the regulations25 and subject to renewal of license in prescribed form and fees not exceeding five thousand rupees and not less than forty-five days before date of expiry of validity period as prescribed by the Central Government.26

[20]. For detail see Section 13(3) of the Information Technology Act, 2000.
[21]. For detail see Section 13(4) of the Information Technology Act, 2000.
[22]. For detail see section 13(5) of the Information Technology Act, 2000.
[23]. For detail see section 17 of the Information Technology Act, 2000.
[24]. For detail see section 19 of the Information Technology Act, 2000.
[25]. For detail see section 21(3) of the Information Technology Act, 2000.
[26]. For detail see section 23 of the Information Technology Act, 2000.

However, the controller may grant or reject the license and application after considering reasonable factors27 or suspend the license accordingly28 by notification through website or such electronic or other media as he may consider appropriate.29 So, Certifying authority means a person who has been granted a licence to issue electronic signature certificate under section 24 of the IT Act, 2000 as provided in section2(g). Every Certifying Authority shall follow appropriate procedures to provide reasonable level of reliability and security to ensure the secrecy and privacy of the electronic signature. Certifying Authority is the repository of all e-signature certificates and they publish information regarding its practices, e-signature certificates, current status of such certificate and observe other legal standards.[29a]

Electronic Signature Certificate

According to section 2(tb) of the IT Act, 2000 'electronic signature certificate' means an Electronic Signature Certificate issued under section 35 and includes digital signature certificate. Every electronic signature certificate application shall accompany with fees not exceeding Rs. 25,000/- to be paid to the Certifying Authority and a certification practice statement or particular statement to be considered by Certifying Authority. After due enquiries and reasonable opportunity given to the applicant,[30] the authority may grant or reject the application with recorded reasons[31] with or without conditions. [32] Before the Information Technology (Amendment) Act 2009, essential conditions were as follows**: i)** The applicant holds the private key corresponding the public key to be listed in the Digital Signature Certificate (DSC); ii**)** The applicant holds a private key, which is capable of creating a digital signature; iii**)** The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

However, the Electronic Signature Certificate may be suspended by the issuing authority on receipt of request from the subscriber or duly authorised person or if it is against the public interest for a period not exceeding 15 days without hearing the subscriber. But in such a situation the authority must communicate the same to the subscriber**.**[33] If it is proved that a material fact in the DSC is false or has been concealed; a requirement was not satisfied; the security system or Certifying authorities, private key was compromised to effect DSC's reliability[34] and so forth then after giving reasonable opportunity of being heard to the subscriber[35] or on request of the subscriber or duly authorised person; or on death of the subscriber; or on dissolution of the firm or winding up of the company where the subscriber is a firm or company,[36] the authority can revoke the DSC. Accordingly the Authority shall communicate the same to the subscriber and notify according to section 39 of this Act.

Under article 9 of the United Nations Model Law on Electronic Commerce, Plenary meeting, the Certification Service Providers **(a)** must act according to its policies and practices. **(b)** They must exercise reasonable care to ensure the accuracy and completeness of all material representations which are relevant

---

27 . For detail see section 24 of the Information Technology Act, 2000.
28. For detail see section 25 of the Information Technology Act, 2000.
29. For detail see section 26 of the Information Technology Act, 2000.
29a. For detail see section 30 of the Information Technology Act, 2000.
30. For detail see section 35(4) proviso 2 of the Information Technology Act, 2000.
31. For detail see section 35 (2) to (4) of the Information Technology Act, 2000.
32. For detail see section 35 (4) proviso of the Information Technology Act, 2000.
33. For detail see section 35 (4) proviso of the Information Technology Act, 2000.
34. For detail see section 37(1) to (3) of the Information Technology Act, 2000.
35. For detail see section 38 (3) of the Information Technology Act, 2000.
36. For detail see section 38(1) of the Information Technology Act, 2000.

to the certificate or included in the certificate. **(c)** They must provide reasonable accessible means to enable relying party to ascertain from the certificate (i) the identity of the certification service provider, (ii) the signatory as identified in the certificate had control of the signature creation data at the time when the certificate was issued; and (iii) the signature creation data were valid at or before the time when the certificate was issued. **(d)** To ascertain relying party (i) the method used to identify the signatory (ii) about any limitation for the purpose of the use of the signature creation data or the certificate, (iii) That signature creation data are valid and have not been compromised. (iv) Any limitation on the scope or extent or liability stipulated by the certification service provider. (v) Signatory followed all means according to article 8; and (vi) whether a timely revocation service is offered. **(e)**To utilise trustworthy systems, procedures and human resources in performing its services, In case of failure to satisfy the requirements mentioned under Para 1, a certification service provider shall be responsible for the legal consequences. Article 10 provides that the trustworthiness of the Certificate Service Providers depends on **(a)** Financial and human resources, including existence of assets. **(b)** Quality of hardware and software systems. **(c)** Procedures for (i) processing, (ii) applications for certificate and (iii) retention of records. **(d)** Availability of information (i) signatories as identified in certificates and (ii) potential relying parties. **(e)** Regularity and extent of audit by an independent body. **(f)** Declaration by the state or authenticating authority about compliance with or existence of the fore- going; or **(g)** any other relevant factor.

Duties and Liabilities of Subscribers

Part VIII of the Information Technology Act, 2000 deals with duties of subscribers of Digital Signature Certificate and Electronic Signature Certificate. First and foremost duty of subscriber is generating key pair. If the subscriber accepts the public key of corresponding private key then he must generate that key pair by applying the security procedure[37] as prescribed by the Central Government. Therefore, generating key pair with signature must be following security standards, confidentiality and regulations. However, in respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.[37a]

Generation, Distribution and Security

Rule 18 of the Information Technology (Certifying Authorities) Rules, 2000 deals with key management for Digital Signature Certificate. Sub-Rule 1 of Rule 18 deals with Generation of Key. It provides that (a) the subscriber's key pair shall be generated by the subscriber or on a key generation system in the presence of the subscriber; (b) the key generation process shall be statistical random process which prevents possible cyber attack. Rule 18.2 provides that distribution of keys from key generation system to storage device must be using a secure mechanism that ensures confidentiality and integrity. However, it should be stored in tamper resistant devices and activated under strict control by the person other than who are related to Certifying Authority.[38] It can be stored under the custody of the key custodians in a tamper-resistant cryptographic module or split into sub-keys for split control.[39]

---

[37]. For detail See section 40 of the Information Technology Act, 2000.

37a. For detail see section 40A of the Information Technology Act, 2000.

[38]. Rule 18.3 (1) of the Information Technology (Certifying Authorities) Rules, 2000.

[39]. See supra note 38.

[40] . Rule 18.5 of the Information Technology (Certifying Authorities) Rules, 2000; in accordance with PKIX Certificate Management Protocol, or via an equally secure manner.

The Certifying Authority's public verification key must be delivered to the prospective Digital Signature Certificate holder in an online transaction following secure process.[40] Rule 19 provides for the private key protection and backup system as follows: (1) the Certifying authority must protect its private keys from disclosure. (2) The Certifying Authority must backup its private keys and store in encrypted form to protect at no lower than primary level; and (3) store in a secure storage facility away from where the original key is stored. After use the private key and all copies of it must be securely destroyed following the prescribed method.[41] The public and private key must be used for limited period with periodical change following key generation guidelines. There must be reasonable notice to subscriber's relying parties about any change to a new key pair with reliable process by showing generation of key interlocks such as signing a hash of the new key with the old key.[42] However, validity period for all keys is not more than five years and suggested validity of particular key lengths or period should be according to Threat-Risk Assessments of particular department.

Confidentiality of Subscriber's Information

Rule 22 deals with the implementation of privacy, confidential and secure procedure to protect subscribers' data from third party. However, there may be discloser of subscribers' data with his consent and according to Law. These are as follows: (i) procedures and security controls to protect the privacy and confidentiality of the subscriber's data under the Certifying Authority's custody shall be implemented and confidential information of the subscriber must not be disclosed to a third party without his consent unless it is required according to law or a court order. (ii) Subscriber's information during its operation shall be protected to ensure his privacy. (iii) There must be a secure communication channel between Certifying Authority and its subscribers to ensure the authenticity, integrity and confidentiality of the exchange e.g., transmission of Digital Signature Certificate, password, private key during the certificate issuance process.

Control of Key Pairs

Section 42 of the Act, 2000 deals with control of private key. It provides that every subscriber shall exercise reasonable care to retain control of the private key of key pairs as listed in the Digital Signature Certificate and take steps to prevent its disclosure.[43] If it is compromised, then, the subscriber shall immediately communicate the same to the Certifying Authority. Till he informs the Certifying Authority about such compromise, he shall be liable.[43a] The Certifying Authority then following Rule 21.3[43b] shall immediately revoke all affected subscribers, subscribers key, subscribers' certificates and public keys of Authority along with keys useful for audit and investigation purposes. However, this public key again must be protected by the Certifying Authority from unauthorised modification.

Use of secure medium

The subscribers have to use key pairs that are of 1024 bits long generated on a secure medium for signing.[43c] A subscriber shall be deemed to have accepted a certificate if he publishes or authorises the publication of a Digital Signature Certificate (a) to one or more person; or (b) in a repository or demonstrates his approval in any manner.[44] For example, when X represents or publishes himself or

---

41 . For detail see Rule 20 and Rule 21.1 of the IT(Certifying Authorities) Rules, 2000.
42. For detail see Rule 21.1 of the IT(Certifying Authorities) Rules, 2000.
43. For detail see section 42(1) of the Information Technology Act, 2000.
43a. For detail see section 42, Explanation of the Information Technology Act, 2000..
43b. For detail see Rule 21.3 of the IT(Certifying Authorities) Rules, 2000.

authorizes his agent y to publish any Digital Signature Certificate to A or advertises his authority through any media then the Certifying Authority shall deem that X has accepted his authority as the subscriber to use key pair following standard confidentiality, reliability and privacy. Subscriber certifies to all who reasonably rely on the information of the Digital Signature Certificate issued to the subscriber by the Certifying Authority that (a) the signature holds the private key corresponding public key listed in the Digital Signature Certificate and is entitled to hold the same; (b) all representations and relevant information to the Certifying Authority by subscriber and in Digital Signature Certificates are true. (c) And subscriber knew all information as true.[45]

Subscriber's Liabilities

However, in case of failure to protect data subscribers may be responsible for compensation to the person affected. While it is a body corporate and negligently hold, possessed or it deals with any sensitive or personal data in a computer resource where reasonable security practice and procedures were to follow and which causes wrongful loss or wrongful gain to any person.[46] Where no specific provisions are mentioned for contravention of any rules or regulations made under this Act, the wrongdoer shall be liable to pay a compensations not exceeding Rs. 25,000/- to the affected person.[46a]

Cyber Appellate Tribunal

To deal with the disputes and to adjudicate the matters the Act provides for the establishment of Cyber Appellate Tribunal.[46b] However, section 64 of the Act empowers the appropriate authority under Cyber Appellate Tribunal to recover the penalty or compensation as an arrear of land revenue and the licence or the Electronic Signature Certificate where penalty or compensation is not paid and to suspend these till the penalty is paid.

Subscriber's Criminal Liability

Penalty for Misrepresentation of Material Fact Relating to Electronic Signature

If anyone misrepresents or suppresses any material fact from the Controller or Certifying Authority relating to licence or electronic signature certificate, he shall be punished with upto two years imprisonment or upto one lakh rupees fine or with both.[46c]

Liability for Breach of Confidentiality And privacy by any Authorised Person

Section 72 prohibits disclosure of electronic record, book, register, correspondence, information, document or other material by any authorised person who has access to those information to third person and impose punishment with upto 2 years imprisonment or up to one lakh rupees fine or with both. However, section 72A, was inserted vide IT(Amendment) Act, 2009, prescribes punishment for disclosure of information in breach of lawful contract with up to three years imprisonment, or upto five lakh rupees

---

43c. For detail see The Information Technology (CA) Regulation, 2001, R.4 (1) (i) that the minimum key length for Asymmetric cryptosystem (RSA Algorithm) shall be 2048 for the Certifying Authority's key pairs and 1024 for the key pairs used by subscribers.

44. For detail see section 40(1) of the Information Technology Act, 2000.

45. For detail see section 41(2) of the Information Technology Act, 2000.

fine or with both. For subscribers always section 72A will be applicable because subscription of certificate always requires fulfilling some terms and conditions according to agreement between the Certifying Authority and the subscriber. Only after valid contract subscribers get authority to publish or authorise to publish or issue certificates. Therefore, fine for subscriber is five lakh i.e. more than for breach of confidentiality and privacy without contract.[46d]

Penalty for publishing false Digital Signature Certificate

Section 73 is applicable not only to subscribers but also every person who publishes false particulars of certificate. Under section 73(1) no person shall publish it or make it available to any other person knowingly that (a) the Certifying Authority has not issued the same certificate, (b) the subscriber listed in the certificate has no Authority immediately and till then he should have responsibility to maintain confidentiality and privacy as accepted. It can be done by the Certifying Authority or any other person including the subscriber. (c) The certificate has been revoked or suspended. For example, in case of private key compromise it is the prime duty of the subscriber to inform the Certifying Authority.

Revocation and suspension

The Certifying Authority if comes to know about misuse or abuse of certificate then he may revoke affected keys and certificates. During this revocation period if the subscriber certifies and uses the certificate as valid then it will be treated as criminal offence unless such publication is for the purpose of verifying a electronic signature created prior to such revocation or suspension of certificate. There may be temporary revocation or suspension of certificate for the purpose of periodical change of key pairs and in such case the authority should immediately inform about new key pairs to the subscribers. But during this suspended period no one should publish certificate to other person with knowledge. Therefore, here mens-rea is very important factor. If knowledge is absent, it is not a crime because there are two elements of crime actus reus and mens-rea. Except exceptional cases, if both are present then only the human conduct will be treated as crime. Here exceptional situation is, if *such publication is for the purpose of verifying a electronic signature created prior to such suspension or revocation.* Section 73(2) prescribes punishment for the contravention of the provisions of section 73(1) with upto two years imprisonment or upto one lakh rupees fine or with both. Under sections 25 and 26 the Controller may suspend licence or revoke it with due notification.

Fraudulent Publication of Electronic Signature Certificate

Fraudulent Publication of Electronic Signature Certificate or making available of it knowingly for fraudulent or unlawful purpose is offence punishable with upto two years imprisonment or upto one lakh rupees fine or with both.

Examiner of Electronic Evidence:

Chapter XXA was inserted by the Information Technology (Amendment) Act, 2009 after Chapter XII and section 79A is the only section of this new chapter. It empowers the Central Government to notify the examiner of electronic evidence about related matters. According to this section the Central Government may specify by notification in the official gazette any department, agency of the Central Government or a State Government as an examiner of electronic evidence for the purpose of providing expert opinion on electronic evidence. This provision is in conformity with the Indian Evidence Law.

Conclusion and Suggestions

In the new communication era, to regulate digital world there is need to adopt effective, specific and proper law worldwide. Jurisdiction in cyberspace is very complex problem. The concepts of territorial nature of law and territorial application of law are not applicable in cyberspace. Therefore, world has to

adopt uniform legal system and co-operation so far substantive as well as procedural laws are concerned. To control cyber-crimes, cyber contraventions and for good governance through electronic governance and mobile governance, we must adopt specific procedure to be followed by specific court in national and international level. Issues relating to evidence are contributory factors for proliferation of cybercrimes and its growing menace. Wrongdoers in cyberspace are confident that it is very difficult to catch them and even if it has been done then procedure to impose punishments will be a great problem because evidence in cyberspace is the practical problem.

The Information Technology Act, 2000 provides several provisions for recognition of electronic records, digital evidences, digital signature, electronic signature, certificates authenticating digital and electronic signatures, to maintain confidentiality and privacy of electronic transactions as well as electronic data and the like. If Corporate sectors such as banks, industries, institutions, organisations; government departments and individuals use their own digital or electronic signatures on electronic record during transactions maintaining level of confidentiality and privacy then it will be definitely helpful to prevent and control unauthorised access to data, cyber fraud, cyber hacking, cyber theft and the like. Then we can hope for authenticity, integrity and non-concealment of e-data which are transferred. The Information and Communication Technology will become much dependable and alternative to paper transaction. But here Public Key Infrastructure and the Controllers responsibility and accountability as well as duties of the Certifying Authorities and the subscribers are vital. They must maintain standards as provided under the rules and regulations by Central Government time to time. Government has to reform rules and regulations time to time to meet dynamic world standards. Therefore, for data protection, protection of the value of information, prevention and control of cyber crimes as well as cyber contraventions, misuse and abuse of data and like, electronic signature and digital signature system with world standard security measures will be very effective.

The business enterprises while perform their transactions and authenticate confidential activities or in Government sectors or individual transactions and the like, formalities can be completed only just putting signature or signing the document and carry on further affairs; but where these activities are performed online, it requires personal identity or confidential information to complete the procedure by affixing digital or electronic signature on electronic documents. In cyberspace the mode or procedure of signing electronic records are different from manual signatures. Affixing signature on electronic documents is digital signature as well as electronic signature to confirm the authenticity, integrity and efficiency of e-records.

After above discussion we can conclude that the utility of digital as well as electronic signature are as follows:

- **Evidential value:** When the digital signature is affixed on electronic records then it gives recipient reason to believe that message or document was created by known sender and not altered during transaction and it is to be treated authenticate. Therefore, it makes the electronic record authenticate documentary evidence.
- **Proof of attached document:** While affixing digital signature or electronic signature on electronic records is only to prove legality of certain other document's then affixing digital signature or electronic signature perform as proof of attached document/s.
- **Authentic execution of document:** While performance of business transaction requires approval by using or affixing digital or electronic signature, then to make the document legally approved and authentic for execution the digital or electronic signature is important.

- **Efficiency:** Digital signature as well as electronic signature make a document much efficient showing originators/senders and recipients and that the document has finality. Therefore, it can be executed immediately. As affixing signature only requires use of several click and hash function it is time saving too.
- **Integrity:** The sender and receiver will be confident that the message has not been altered during transmission, because any alteration to document after signature will invalidate the signature.

The private key can be used by storing it on a user's computer which will be protected by a local password. But while user has to sign through that particular computer then security of the private key may be a question because in such case security of computer is related to security of local password which may affect on security of private key. (ii) Another way is to store the private key on smart card which is very often tamper resistant and requires Personal Identification Number Code or PIN Code of smart card user to activate it. Any third person unauthorizedly accessed the smart card will require PIN Code to make it active and to generate a digital signature. Not only that, it is difficult to copy any information from smart card because to activate it, requires a numeric keypad or card reader. Therefore, the user of smart card needs to carry and deal with the card very carefully as loss of it will mean loss of private key which may cause, even revocation of certificate. (iii) There is need of procedure against attacks on public keys and private keys. The private keys of user or owner must use properly to maintain security, authenticity, integrity of Digital Signature and procedure to use and verify keys. (iv) In case of Electronic Signature also the private keys or password of user owner has to use properly, carry with due care and keep secrecy to maintain security and authenticity. For example, maintaining secrecy is essential for ATM Cards, Credit Cards and the like. (v)In the European Union and the USA digital signatures are legally recognised. But, Law is not clear about cryptographical signatures and electronic signatures. Asymmetric cryptography is to be used for Digital Signature which makes it more authentic and mostly equal to handwritten signature because it is very difficult to forge properly implemented digital signatures. Here signer or sender cannot repudiate or claim subsequently that the message was not signed by him and at the same time senders private key will remain secret. However, sometimes there may be time stamp during which digital signature will be treated as valid even if the private key of the sender is exposed after signing the message.

Digital Signatures and Electronic Signatures must be used following proper methods or procedures and with due care and caution for several purposes such as: i) To prevent any abuse or misuse of documents by criminals or wrongdoers. ii) To maintain integrity of document and of signature. iii) To satisfy legal requirements for the documents. iv) To maintain authenticity and efficiency of documents and of signature. v) To prevent cyber piracy and other cyber crimes by use of digital or electronic signatures and such authentic information or documents. vi) To maintain law and order in society and smooth functioning of business enterprises and their activities in superhighway in the contemporary era of information communication technology, liberalisation and globalisation. vii)To maintain social security and security of nation while digital signature or electronic signature are used by Electronic Governance system whether for E-Health, E-Agriculture, E-Security, E-Administration, E-Learning, E-Education, E-contract, E-Banking, E-Services or the like. viii)To maintain security integrity, efficiency and authenticity of information or document and digital or electronic signature even while used between private individuals in their private affairs which may lead to social insecurity and disorder as well as violation of private and public laws too. ix) User of digital signature cannot see his sign as he only use hush code, public key and private key. While the private key and PIN codes are stored in a particular computer if that particular computer is controlled by unauthorised user he can succeed to control over every personal information

along with private key and thereby he can replace original document with his own documents, can tamper any information, can crack or hack any information, can commit any other cyber crimes relating to such information or document. Even he can contaminate any kind of virus or bug to destroy document or information as well as whole computer system and network. Though, unauthorised use of information or document is punishable offence under the I T Act, 2000 and also civil wrong under section 43 of the said Act. x) For any business transaction or any authentic action any one can just sign the document and proceed further. Therefore, online transactions required confidential identifications.