The information technology Act

November, 2001

The Techology Law Team

Nishith Desai Associates
Legal & Tax Counseling Worldwide

Published by

**The Chamber of
Income Tax Consultants**

The information technology Act

The Techology Law Team

Nishith Desai Associates

Legal & Tax Counseling Worldwide

MUMBAI

93-B MITTAL COURT, NARIMAN POINT,
MUMBAI 400 021. INDIA.
TEL.: 91 (22) 2282 0609
FAX: 91 (22) 2287 5792

SILICON VALLEY

220 CALIFORNIA AVENUE, SUITE
201, PALO ALTO, CA 94306. USA.
TEL.: 1 (650) 325 7100
FAX: 1 (650) 325 7300

BANGALORE

DBS CENTER – SUTIE 217,
26, CUNNINGHAM ROAD,
BANGALORE 560052. INDIA.
TEL.: 91 (80) 2267272 / 2202440

Published by

The Chamber of
Income Tax Consultants

Introduction

India was one of the first few countries in the world to pass e-commerce enabling legislation, the Information Technology Act, 2000 ("**Act**"), with its formal notification on October 17, 2000. The Act facilitates e-commerce and the use of technology in the conduct of transactions.

Signed and written documents are traditionally used for commercial transactions (mainly because of their evidentiary value). Also, Indian law requires certain documents and contracts to be written and signed. The basic purpose of a signature is to authenticate a document and to identify and bind the person who signs the document. Where contracts are entered online and documents are sent via e-mail, it might not be possible for parties to actually “sign” the contract or document. Therefore, it is difficult to identify the originator of an online document and to verify its authenticity.

The concept of digital signatures has been devised to overcome this limitation and the Act has been enacted to give legal backing to such digital signatures and regulate hem.

The Act drew its inspiration from the Model law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) and pioneering e-commerce enabling legislations such as the Utah Digital Signatures Act, 1995, the Singapore Electronic Transactions Act, 1998 and the Malaysian Electronic Signatures Act.

Within India itself, the enthusiasm of the Government to enact such a legislation resulted in two draft Bills - one prepared by the Department of Electronics (now part of the Ministry of Information Technology) and another by the Ministry of Commerce. The drafts culminated in a 3rd draft, which was a result of the combined effort.

The essence of the Act is captured in the long title of the Act, which reads *inter alia* "*An act to provide for the legal recognition of transactions carried out by … alternatives to paper-based methods of communication and storage of information…*".

The Act seeks to address the two different aspects of the technological revolution. One, which is expressly, stated in the Preamble of the Act, being that of providing legal recognition to electronic transactions and use of alternatives to paper-based methods of communications, storage etc. The other aspect, though not clearly stated in the Preamble itself, which the Act seeks to address, is the regulation and control of cyber crimes and other related offences.

The Act seeks to define various offences arising out of the use of digital signatures and lay down guidelines for regulating them. Interestingly, unlike most other similar legislations, the Act also seeks to regulate the Internet in some form by making publication of obscene information in electronic form an offence.

It is also to the credit of the Indian legislature that the Act was one of the first legislations to be thrown open for public comment, prior to it being finalized. The response of the public in India was significant, that by itself indicating the immense need for the legislation.

FAQs

A) What is a Digital Signature and why do I need it?

Simplistically put, a digital signature is an electronic form of a physical world hand-written signature. Instead of applying to paper documents, digital signatures are applied to electronic documents.

A digital signature, like physical signature, has a dual function, being that of integrity and non-repudiation. Since the digital signature is unique and is only in the possession of its holder, the person cannot repudiate his digital signature on the electronic document. Since encryption technology is used in digital signatures, any tampering with the document immediately invalidates the digital signature, thus preserving integrity of the document.

B) What are Symmetric and Asymmetric encryptions?

Encryption algorithms can be broadly classified into two categories: symmetric and asymmetric. Symmetric algorithms use the same key to lock and unlock a document whereas,Asymmetric algorithms use two different keys: when one is used to lock a document only the other can be used to unlock it.

Symmetric keys are usually large random numbers. Asymmetric keys are usually generated in a set of pairs called key pairs. The best-known asymmetric encryption algorithm is the RSA algorithm. ("RSA" stands for a hashing algorithm after its inventors, Rivest, Shamia and Alderman)

C) What is a key pair and how is it used?

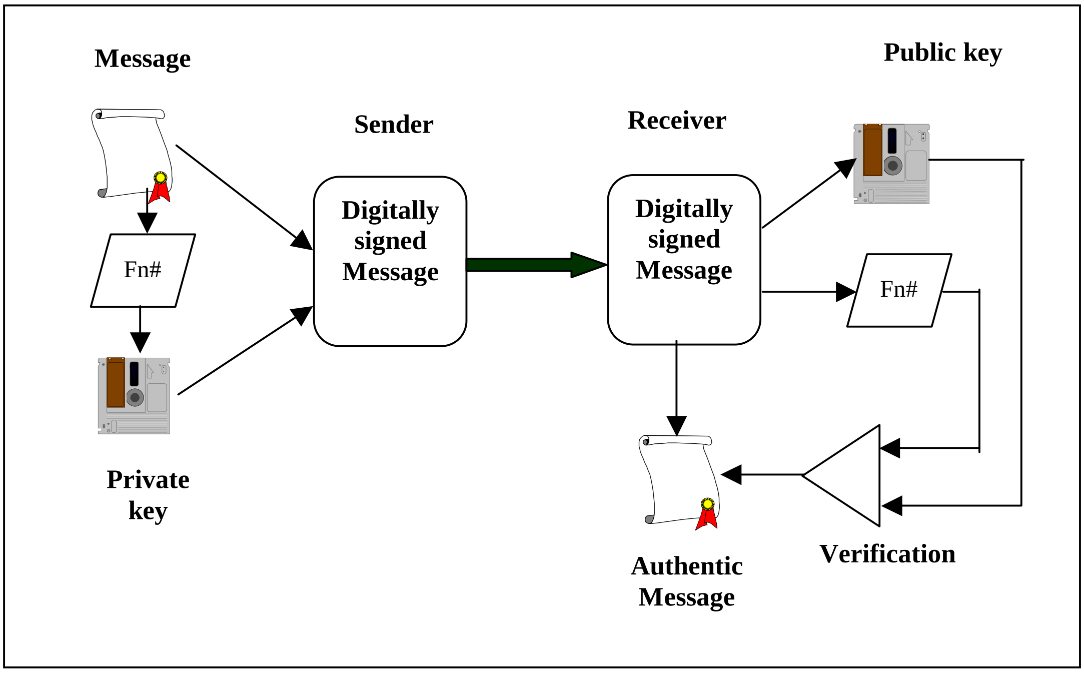
A key pair comprises of two keys.. Each key comprising of very large numbers, say 200 to 300 digits in length that are mathematically linked. The keys are named as “Private key” and “Public key”. However, the same key cannot be used to lock as well as unlock.

Rather than using the same key to both encrypt and decrypt the data, public key encryption uses a matched pair of encryption and decryption keys. Each key performs a one-way transformation on the data. Each key is the inverse function of the other; what one does, only the other can undo.

A Public Key is made publicly available by its owner, while the Private Key is kept secret. The key pair can also be used to send private/secret messages. To send a private message, an author scrambles the message (encrypts) with the intended recipient's Public Key. Once so encrypted, the message can only be decoded with the recipient's Private Key.

D) How does a digital signature replace a paper signature?

To begin with, a Digital Signature is not a handwritten signature that is scanned and pasted on a document. Neither is it a password nor a T-Pin number required for accessing a document. Digital Signature is, in fact, a result of applying an encryption process to specific information. The process is as follows :-



1. The message that is to be signed is first delineated. The delineated message is then processed using an algorithm called the 'hash function'[1]. The output obtained is called the 'hash result'[2]. The hash result is usually much smaller than the message, but nevertheless is unique to the message. If the message changes, the hash result also changes[3]. Thus if there is any tampering with the message, it can be found out by re-computing the hash result.

2. The hash result is then encrypted using the private key of the endorser. The encrypted hash result is actually the Digital Signature.

3. The Digital Signature is then affixed to the message and the message along with the digital signature is sent over the Internet. It is important to bear in mind that the message is not encrypted and if the message is intended to be confidential, it should be encrypted as explained above (using the public key of the receiver).

Once the intended receiver receives the message, he would like to examine the authenticity of the message as well as the integrity of the message. The authenticity can be verified by decrypting the digital signature using the public key of the sender. The fact that the digital signature could be decrypted using the sender's public key proves that the endorser of the message is the sender (i.e. a person who owns the corresponding private key).

[1] Hashing is a process by which a computer program arranges a body of information into table.

[2] It is computationally unfeasible to reconstruct the original message from the hash result

[3] It is extremely improbable that two messages will produce the same hash result. *See Kaufman, et al., Network Security pg. 102*

The integrity of the message can be verified by computing the hash result of the received message and comparing it to the output of the decrypted digital signature (which is actually the hash result of message initially). If both the hash results are same, it can be assumed that the message has not been tampered after digital signature has been affixed.

E) How do I check someone's signature?

First of all one needs a copy of the recipients public key, which should be freely available. A signature comprises of a private key, hence a public key is used to verify it. One can easily obtain the public key of the intended recipient of the encrypted message either from his Digital Signature Certificate ("**DSC**") or from the repository of the DSC, which is usually publicly available with the Certifying Authority ("**CA**").

F) What is a Digital Signature Certificate ("DSC")?

A DSC is simply a certificate signed by an independent and trusted third party (also known as a CA). This certificate has a standard format and is usually issued under the format called X.509.

A certificate consists of the following three elements:

i) Name and Other Extensions
This part of the certificate contains information about the entity to which the certificate is issued. Such information could include one's name, nationality and email address, details of ones work place etc. It could also include the DSC holders picture, a layout of his fingerprints, passport number etc.

ii) Public Key Information
The DSC also contains information about the public key of the holder. The certificate acts to bind the public key of the holder to him and attribute information described above. The public key is usually a part of the asymmetric key of the signature holder usually an RSA key.

iii) Certifying Authority (CA)
A CA is a relied-upon entity that issues, publishes, suspends and revokes digital certificates. The CA's role is to verify the identity of subscribers and provide certificate management services. A CA acts like a trusted electronic notary public, telling everyone who the valid users are and what their digital signatures should look like.

G) Which Digital Signatures are legally recognised?

There are various types of digital signatures available. However, not all digital signatures are legally recognised. For example the Act only recognises asymmetric cryptosystem and hash algorithm as methods of authentication of electronic records. Therefore, symmetric cryptosystem or other examples of electronic signatures will not be legally recognised digital signatures. Hence though there could be other forms of electronic signatures, which could be valid signatures, nonetheless would not be legally recognised. For the purposes of this book, unless the context otherwise requires, a digital signature would refer only to a legally recognised digital signature. The Act has further termed certain legally recognized digital signature as secure digital signature. (This has been explained later.)

H) What are the kinds of digital certificates?[4]

A certificate is a general term for a signed document containing name and public key information. Such a certificate can take many forms. However, the emerging certificate standard is the X.509 certificate format, which has been around for many years and form a part of the Open System Interconnection ("**OSI**") group of standards. X.509 certificates are very clearly defined using a notation called ASN.1 (Abstract Syntax Notation 1), which specifies the precise kinds of binary data that make up the certificate.

ASN.1 can be encoded in many ways but the emerging standard is a very simple encoding called DER (Distinguished Encoding Rules), which results in a compact binary certificate. For email exchange purposes the binary certificate will often be Base64 encoded, resulting in an ASCII text document that looks like this:

```
-----BEGIN CERTIFICATE-----

MIICWDCCAgICAQAwDQYJKoZIhvcNAQEEBQAwgbYxCzAJBgNVBAYTAlpBMRUwE
wYD
VQQIEwxXZXN0ZXJuIENhcGUxEjAQBgNVBAcTCUNhcGUgVG93bjEdMBsGA1UECh
MU
VGhhd3RlIENvbnN1bHRpbmcgY2MxHzAdBgNVBAsTFkNlcnRpZmljYXRpb24gU2Vy
dmljZXMxFzAVBgNVBAMTDnd3dy50aGF3dGUuY29tMSMwIQYJKoZIhvcNAQkBFhR3
ZWJtYXN0ZXJAdGhhd3RlLmNvbTAeFw05NjExMTQxNzE1MjVaFw05NjEyMTQxNzE1
MjVaMIG2MQswCQYDVQQGEwJaQTEVMBMGA1UECBMMV2VzdGVybiBDYXBlMRI
wEAYD
VQQHEwlDYXBlIFRvd24xHTAbBgNVBAoTFFRoYXd0ZSBDb25zdWx0aW5nIGNjMR8
w
HQYDVQQLExZDZXJ0aWZpY2F0aW9uIFNlcnZpY2VzMRcwFQYDVQQDEw53d3cudG
hh
d3RlLmNvbTEjMCEGCSqGSIb3DQEJARYUd2VibWFzdGVyQHRoYXd0ZS5jb20wXDA
N
BgkqhkiG9w0BAQEFAANLADBIAkEAmpIl7aR3aSPUUwUrHzpVMrsm3gpI2PzIwMh3
9l1h/RszI0/0qC2WRMlfwm5FapohoyjTJ6ZyGUUenICllKyKZwIDAQABMA0GCSqG
SIb3DQEBBAUAA0EAfI57WLkOKEyQqyCDYZ6reCukVDmAe7nZSbOyKv6KUvTCiQ5c
e5L4y3c/ViKdlou5BcQYAbxA7rwO/vz4m51w4w==

-----END CERTIFICATE-----
```

[4] Source: www.thawte.com. We acknowledge the efforts of the authors.

When you decode this certificate using an application like SSLeay you can see the components of the cert:

```
    Certificate:
    Data:
    Version: 0 (0x0)
    Serial Number: 0 (0x0)
    Signature Algorithm: md5withRSAEncryption
    Issuer: C=ZA, SP=Western Cape, L=Cape Town, O=Thawte Consulting cc,
   OU=Certification Services, CN=www.thawte.com,
   Email=webmaster@thawte.com

    Validity
    Not Before: Nov 14 17:15:25 1996 GMT
    Not After: Dec 14 17:15:25 1996 GMT
    Subject: C=ZA, SP=Western Cape, L=Cape Town, O=Thawte Consulting cc,
   OU=Certification Services, CN=www.thawte.com,
   Email=webmaster@thawte.com
    Subject Public Key Info:
    Public Key Algorithm: rsa Encryption
   Modulus:
       00:9a:92:25:ed:a4:77:69:23:d4:53:05:2b:1f:3a:
       55:32:bb:26:de:0a:48:d8:fc:c8:c0:c8:77:f6:5d:
       61:fd:1b:33:23:4f:f4:a8:2d:96:44:c9:5f:c2:6e:
       45:6a:9a:21:a3:28:d3:27:a6:72:19:45:1e:9c:80:
       a5:94:ac:8a:67
   Exponent: 65537 (0x10001)
    Signature Algorithm: md5withRSAEncryption
7c:8e:7b:58:b9:0e:28:4c:90:ab:20:83:61:9e:ab:78:2b:a4:
54:39:80:7b:b9:d9:49:b3:b2:2a:fe:8a:52:f4:c2:89:0e:5c:
7b:92:f8:cb:77:3f:56:22:9d:96:8b:b9:05:c4:18:01:bc:40:
ee:bc:0e:fe:fc:f8:9b:9d:70:e3
```

(Note: In this case the “Public Key” described is of the RSA variety.

I) Is it necessary to keep the DSC confidential?

One can freely distribute his DSC. In fact, it must be available to any person who wishes to send an encrypted message to you since the certificate would contain details of your public key corresponding to one’s private key. Such information would be required to send an encrypted message to you. However, the private key, which is used to decrypt the message sent to you, should be kept secret.

J) Does it matter which CA I choose?[5]

One could choose a CA based on the nature of the DSC so issued.. Hence, depending on whether the DSC would be used within the organization, nationally or worldwide, an appropriate choice of a CA could be made depending on the

[5] Source: supra

recognition and acceptability of the DSCs issued by that CA within the particular territory in which DSC would be used.

If the DSC is required for individual or corporate use, one should choose a CA who is most trusted among the parties with whom one transacts. The trust regarding the CA is generally created by reputation or by law. CAs, where trust is created by law, are preferred to CAs where trust is created by reputation. This is primarily because the evidentiary value of DSC in former case is greater.

K) Who issues Digital IDs and how?

DSCs are issued by a Certification Authority (CA), which usually are trusted bodies who vouch for the identities of those to whom they issue DSCs. A DSC could be issued to anyone from a student to an employee of a company or a citizen of a state.

A DSC is issued usually in the following manner: A person generates his own key pair and sends the public key to an appropriate CA with some proof of identification. The CA checks the identification and after assuring itself that the request really did come from the person seeking the DSC, sends a Digital ID attesting to the binding between the holder of the DSC and his public key. The holder can then present this DSC whenever desired in order to demonstrate the legitimacy of his public key.

Different CAs may issue DSCs with varying levels of identification requirements. Each CA publishes its own identification requirements and standards, so that verifiers can attach the appropriate level of confidence in the certified name-key bindings.

L) How are the keys associated with a DSC managed?

It is extremely important to adopt secure methods for the management of keys associated with DSC since most attacks on public-key systems could probably be aimed at the key management levels, rather than at the cryptographic algorithm itself.

A user should be in a position to securely obtain a key pair suited to his efficiency and security requirements. There must be a way to look up other people's public keys and to publicize one's own key. DSC provides the assurance of legitimacy of other’s public key. Therefore, it must be unforgettable, obtainable in a secure manner and processed in a way such that an intruder cannot misuse them.

If someone's private key is lost or compromised, others must be made aware of this so that they will no longer encrypt messages under the invalid public key nor accept messages signed with the invalid private key. Users must be able to store their private keys securely so that no intruder can find it, yet the keys must be readily accessible for legitimate use.

M) Where does my computer store my private key?

A private key is typically stored in encrypted format in a Preferences or Configuration file that can only be unlocked (decrypted) using your private key password. Different computer programs may store your private key in different places.

N) Who needs a key pair?

Anyone who wishes to sign messages or receive encrypted messages must have a key pair. Individuals might have more than one key. For example, one key for professional use and another for personal use. Also certain organisations like universities, large corporates have a single key to a group key associated with them.

O) For how long does a key stay valid?

Generally, a key remains valid until it is believed to have been compromised. However, usually a key is granted for a period of one year by a CA to limit the potential damage of key compromise.

Q) What happens when a key expires?

In order to guard against a long-term factoring attack, every key must have an expiration date after which it is no longer valid. The validity period must therefore be much shorter than the expected factoring time, or equivalently, the key length must be long enough to make the chance of factoring before expiration extremely small. The validity period for a key pair may also depend on the circumstances in which the key would be used, although there will also be a standard period. The validity period, together with the value of the key and the estimated strength of an expected attacker, then determines the appropriate key size.

After expiration, the user chooses a new key which should be longer than the old key, perhaps by several digits, to reflect both the performance increase of computer hardware and any recent improvements in factoring algorithms. Recommended key length schedules are likely be published. A user may re-certify a key that has expired, if it is sufficiently long and has not been compromised. The CA would then issue a new DSC for the same key, and all new signatures would point to the new DSC instead of the old. However, the fact that computer hardware continues to improve argues for replacing expired keys with new, longer keys every few years. Key replacement enables one to take advantage of the hardware improvements to increase the security of the cryptosystem. Faster hardware has the effect of increasing security, perhaps vastly, but only if key lengths are increased regularly.

R) How secure should the keys be?

Your digital private key is the critical portion of your online identity. Anybody who has access to your digital key can sign documents on your behalf and can decrypt messages addressed to you. If your key is compromised, you could well be held legally responsible for the actions of someone else. If you have a digital certificate containing a key that has been compromised you should notify your CA and revoke the certificate at once.

S) What if the CA's key is lost or compromised?

In the event of a loss or destruction of the CA's key DSCs signed with the old key remain valid, as long as the verifier can use the old public key to verify the DSC.

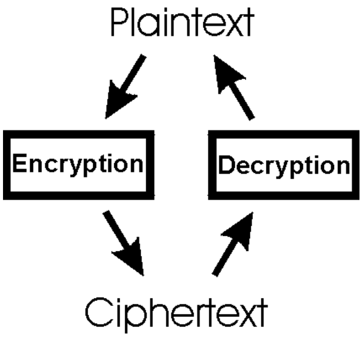
However, a compromised CA key is a much more dangerous situation. An attacker who discovers a CA's private key may be in a position to issue phony DSCs in the name of the CAthat would enable undetectable forgeries.

In such an event, the CA must immediately cease issuing DSC under its old key and change to a new key. If it is suspected that some phony DSCs were issued, all DSCs should be recalled, and reissued with a new CA key. These measures could be relaxed somewhat if DSCs were registered with a digital time-stamping service. Interestingly, a CA key does not invalidate users' keys, but only the DSCs that authenticate them. Compromise of a top-level CA's key should be considered catastrophic, since the key may be built into applications that verify DSCs.

T) How secure is modern cryptography?

Cryptography is the science of devising methods that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient.

The basic principle is this: A message being sent is known as **plaintext**. The message is then coded using a cryptographic algorithm. This process is called **encryption** (see Fig. 1). An encrypted message is known as **cipher text**, and is turned back into plaintext by the process of **decryption**. [6]



Modern cryptography is usually very secure. The higher the encryption level, the better is the security. Usually, 128-bit cryptography is used for

[6] Source: http://www.cs.bris.ac.uk/~cooper/Cryptography/crypto.html

asymmetric keys. These are considered to be sufficiently secure and it is believed that it would take a lifetime for someone to decrypt the same.

U) What is a hash function?

A hash function is a computation that takes a variable-size input and returns a fixed-size string which is called the hash value. One-way hash functions, hash functions that are hard to invert, are used to generate a message digest. Which is a hash output of a message so hashed. Examples of well-known hash functions are MD4, MD5, and SHS.

A hash function used for digital authentication must have certain properties that make it secure enough for cryptographic use. Specifically, it must be infeasible to find:

- A message that hashes to a given value
- Two distinct messages that hash to the same value

The ability to find a message hashing to a given value would enable an attacker to substitute a fake message for a real message that was signed. It would also enable someone to falsely disown a message by claiming that he or she actually signed a different message hashing to the same value, thus violating the non-repudiation property of digital signatures.

V) What makes a good Hashing Algorithm?[7]

A good hashing algorithm has the following properties:

1. A small change in the document will produce a large change in the hash. For example, the sentence "I owe Joe $100." has an MD5 hash of "yCHXVqL0fYV4VfJNajm8KA==", while the sentence "I owe Joe $1000." has a hash of "QHAwXFTxa3bHRH38IMMrSw==" (both of these hashes have been BASE64 encoded, so they look OK in a Web page). Note that a tiny change in the document has produced two totally different hashes.

2. Hashes should not be predictable. In other words, I should not be able to guess that changing the document by adding a "0" will have a specific effect on the hash.

3. Hashes should not collide and it should be computationally difficult to find collisions. In other words, two documents should have an extremely small chance of having the same hash, and it should be virtually impossible to find a document that has the same hash as a known document.

4. Hashing should be fast. Often we use hashes to check that large files have not changed. Instead of storing a complete copy of the large file we store a hash and then calculate a hash of the current file to see if it is the same. A different hash will indicate that the file has been changed - even if only slightly.

[7] Source: www.thwate.com.

There are many different hashing algorithms: MD2, SHA, SHA1 and MD5 are well known.

W) Why bother with Hashing?

If you have a hash of a large file you will know if that file has been changed even slightly by comparing the old hash with a current one. This is much more convenient in many cases than storing copies of large files. Also, sometimes you want to encrypt a reference to a document. Encryption is complex, so encrypting just a hash is much faster than encrypting the whole document. Note that the hash cannot be used to get the document back; it can only be used to refer to a particular version of that document.

X) What are MD2, MD4, and MD5?

MD2, MD4 and MD5 (MD stands for Message Digest) are widely used hash functions designed by Ron Rivest specifically for cryptographic use. They produce 128-bit digests and there is no known attack faster than exhaustive search.

Y) Why are there multiple trust hierarchies?

The level of hierarchy associated with a DSC is usually associated with the level of identification process involved in the issuance of a DSC. Usually, students or individuals who want to test DSC or use it for a minimum of purposes are issued DSC with minimum checks. Only some form of identification is checked. While the process of issuing fully secure DSC could involve personal checks, apart from checking the relevant documents. For example, a DSC used by a person only for sending emails may require minimal identification during issuance, whereas, a DSC used for execution of online contracts and entering into online transactions such as internet based stock trading may require a higher level of identification.

Z) What is a DSC revocation list?

A Certificate Revocation List (CRL) is a list of DSCs that have been revoked before their scheduled expiration date. There are several reasons why a key might need to be revoked and placed on a CRL. A key might have been compromised. When verifying a signature, one can check the relevant CRL to make sure the signatory’s key has not been revoked.

CAs maintain CRLs and provide information about revoked keys originally certified by the CA. CRLs only list current keys, because expired keys should not be accepted in any case; when a revoked key is past its original expiration date it is removed from the CRL. Although CRLs are maintained in a distributed manner, there may be central repositories for CRLs, that is, sites on networks containing the latest CRLs from many organizations.

Chapter -I

Overview

The division of powers between the Parliament and various State Legislatures is contained in Schedule VII of the Constitution of India, 1950. The Parliament has power to legislate on issues relating to post and telegraphs, telephones, wireless broadcasting and other like forms as per entry 31 of List 1 of Schedule VII aforesaid.

In pursuance of its powers, the Indian Parliament enacted the Information Technology Act, 2000 ("**Act**"). The Act, comprises of three significant aspects:

- Legal recognition of electronic records and communications - contractual framework, evidentiary aspects, digital signatures as the method of authentication, rules for determining time and place of dispatch and receipt of electronic records, etc.

- Regulation of Certification Authorities ("**CAs**") - appointment of a Controller of CAs, grant of licenses to CAs, duties vis-à-vis subscribers of digital signature certificates, recognition of foreign CAs, etc.

- Cyber contraventions - civil and criminal violations, penalties, establishment of the Adjudicating Authority and the Cyber Regulatory Appellate Tribunal, etc.

Further, the Act amends provisions of existing laws such as the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. The main purpose of these amendments is to address the related issues of electronic crimes and evidence, and to enable further regulation as regards electronic funds transfers.

Chapter I describes the scope and applicability of the Act and contains the definitions clause.

The Act extends to the whole of India and also seeks to implement extraterritorial operations, as regards criminal violations. The scope of the Act extends to all types of transactions and records, barring a few. However, the Act would not be applicable to[8] (a) a negotiable instrument[9] (b) a power of attorney (c) a trust (d) a will or any

[8] Section 1(4)

[9] Section 13 of Negotiable Instruments Act , 1881

(1) A negotiable instrument" means promissory note, bill of exchange or cheque payable either to order or to bearer.

Explanation (i) A promissory note, bill of exchange or cheque is payable to order which is expressed to be so payable or which is expressed to be payable to a particular person, and does not contain words prohibiting transfer or indicating an intention that it shall not be transferable. Explanation (ii) A promissory note, bill of exchange or cheque is payable to bearer which is expressed to be so payable or on which the only or last endorsement is an endorsement in blank. Explanation (iii) Where a promissory note, bill of exchange or cheque, either originally or by endorsement, is expressed to be payable to the order of a specified person, and not to him or his order, it is nevertheless payable to him or his order at his option.

testamentary disposition (e) any contract for sale or conveyance of immovable property; and (f) any document as may be notified by the Government of India in the Official Gazette.

Given the wide variety of real-life situations, there could be certain borderline cases where the applicability of the Act may not be clear. One example is of an employment agreement, if it contains a clause by the employee granting a power-of-attorney to the employer (for filing applications with respect to intellectual property protection). Here, it is unclear on whether the Agreement would be governed by the Act or not. There could be other examples as well. But, there are two likely approaches - one which states that an entire transaction cannot be conducted as per the provisions of the Act because a small portion falls outside the scope of the Act; the other which states that, a transaction falls outside the scope of the Act only if the main purpose of such transaction is outside its scope.

Section 2 of the Act is the definitions clause, which contain about 30 definitions, several of which relate to technical terms. Some of the terms that have been defined include "access", "computer", "computer resource", "data", "information", "function", "addressee", "originator", "intermediary". However, there are certain definitions, which are inter-related and often go about in circles, creating ambiguity and uncertainty about the terms so defined.[10]

Chapter II of the Act prescribes that electronic records may be authenticated using digital signatures and proceeds to detail what an asymmetric cryptosystem is.

Chapter III of the Act contains the sections, which provide for the legal recognition of electronic records and digital signatures. Digital signatures are given equivalence to the handwritten signatures. This Chapter further provides for the use of electronic records and digital signatures in Government records and communications. However, the efforts to establish electronic governance are limited by Section 9 (which provides that no person would have the right to confer a right upon any person to insist that the Government should accept electronic records).

Chapter IV of the Act deals with contractual aspects of use of electronic records, such as attribution, acknowledgement, time and place of dispatch and receipt. The basic law

A negotiable instrument may be made payable to two or more payees jointly, or it may be made payable in the alternative to one of two, or one or some of several payees.

[10] For instance, the lines of distinction between the set of computer - related definitions (i.e computer, computer network, computer resource, computer system [see Box 1]) are amorphous. In a highly networked environment involving several components (which perform logical, processing functions) the end of a "computer" and the beginning of a "computer network", may be very difficult to identify. Let us consider a typical scenario where usually computers are networked with each other within a department or an organisation by means of a LAN (Local Area Network). Or another situation wherein computers of an organisation in various branches are connected by means of a WAN (Wide Area Network). Furthermore, all the computers could be connected to a central server, which stores data of all the computers. Also, the computers are connected to a public network to enable the access of Internet. In absence of a clear definition, it is often unclear and ambiguous as to where to draw a line to differentiate between a computer, computer network, public network etc.

governing contracts in India is the Indian Contract Act, 1872 ("**Contracts Act**") which stipulates the rules regarding offer and acceptance, promise and consideration, performance and breach, etc. As such, the Contract Act does not mandate that contracts should be written. However, prior to the passing of the Act, there was some doubt on the enforceability of online contracts. The Act now provides that all requirements for a matter to be in writing are satisfied if such matter is in electronic form and accessible so as to be usable for a subsequent reference.

Chapter V of the Act provides for certain presumptions that are available to secure electronic records and secure digital signatures. Section 3 of the Act gives validity to digital signatures. It states that where "any law provides that information or any other matter shall be authenticated by affixing the signature, or any document should 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 a digital signature affixed in such manner as may be prescribed by the Government".

Chapters VI, VII and VIII of the Act broadly lay down the legal framework within which digital signatures can be issued and used. Apart from the regulatory framework, the Act also prescribes a framework for certain contractual rights and duties of a CA vis-à-vis a subscriber. Digital signatures operate on the foundation of a CA who would certify the digital signatures as that of a certain person. Any entity wishing to operate as a CA in India is required to obtain a license from the Controller of CAs (appointed by and under the general control and direction of the Central Government) for its operations.[11] The license would be a non-transferable license and subject to terms and conditions as may be specified in the future.

The Central Government is empowered to make rules and regulations regarding several operational aspects of the business of CAs, including the recognition of foreign CAs.

Chapters IX, X and XI deal with contraventions, offences and penalties. These Chapters also deal with the establishment of the office of an Adjudicating Officer and the Cyber Regulations Appellate Tribunal (“**CRAT**”).

Chapter XII consists of a single provision that is directed towards addressing the issue of network service provider liability

Lastly, **Chapter XIII** deals with miscellaneous provisions such as the overriding effect of the Act, controversial Section 80 i.e. the powers of police etc.

Box 1

[11] The Controller has the discretionto grant the license or reject the application. The Controller may however, not reject an application without giving the applicant CA an opportunity to present its case.

"Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer, software or communication facilities which are connected or related to the computer in a computer system or computer network.

"Computer Network" means the interconnection of one or more computers through (I) the use of satellite, microwave, terrestrial line or other communication media; and, (ii) terminals or a complex consisting of two or more interconnected computers, whether or not the interconnection is continuously maintained.

"Computer resource" means computer, computer system, computer network, data, computer data base or software.

"Computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data, and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

Chapter 2

Electronic Transactions

The advent of the Internet has facilitated all kinds of new businesses using faster and cheaper means of communication. Various services such as information services, online ordering services, online payment services, broadcasting services, search and recovery services and any other service, which can be facilitated through the Internet.

The growing popularity of these services has also contributed to the increasing conduct of electronic transactions. Transactions have been concluded using the popular e-mail where parties exchange commitments, instead of traditional paper-based orders and acceptances. Web-based orders, automated processing systems are also being widely used.

"Transaction" has been broadly defined to mean "an action or a set of actions occurring between two or more persons relating to the conduct of business, commercial or governmental affairs"[12]. In fact, the manifold possibilities of the electronic transactions are demonstrated in the Uniform Electronic Transactions Act, which defines "automated transactions" to mean "*a transaction conducted or performed, in whole or in part, by electronic means or electronic records in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course of forming a contract, performing under an existing contract or fulfilling an obligation required by the transaction*".[13]

Traditionally, transactions were concluded on the basis of oral or written communications. Concluded transactions were legally enforceable, since well-established rules determined the commitments made by one person to another, through the various modes of communications. In India, the Contracts Act essentially governs the conduct of transactions. Formation of any contract (through any mode of communication) would involve three main ingredients:

(a) There has to be an offer,
(b) There has to be an acceptance of the said offer without modification, and
(c) There has to be some consideration for the contract.

The anonymous and borderless nature of the Internet has challenged the rules of traditional contract law on various fronts - identity of person (or attribution of a particular communication to a person), time of dispatch and receipt of communication, place of communication, etc. The Contract Act is limited in adopting itself to suit the Internet, and taking into account the authentication technologies that are necessary for attribution purposes. Instead, the Act has been enacted to precisely address the peculiar issues raised by the new technology. As explained earlier, the Act is only an enabling one and does not introduce anything new to the existing principles of contract law. The Act has to be read in conjunction with the existing provisions of law, including the Contract Act.

[12] Section 46-4-102 (16) of the Uniform Electronic Transaction Act 1999, USA, (a federal law drafted by the National Conference of Commissioners on Uniform State Laws). This has been adopted in several states. c.f. www.law.upenn.edu.

[13] Section 46-4-102 (2) of the Uniform Electronic Transactions Act, 1999.

Some of the key aspects addressed by the Act in the conduct of transactions through electronic modes of communication are summarized below.

Attribution

The Act provides that an electronic record shall be attributed to the originator if it was sent (a) by originator, or (b) by a person who had the authority to act on behalf of the originator in respect of that electronic record, or (c) by an information system programmed by or on behalf of the originator to operate automatically.[14]

The Section seems to be redundant in one respect: if X sends a message, it restates that the message sent by X would be deemed as that sent by X. However, the scope of the section is very limited when it comes to attribution in relation to a person's own actions. The section presupposes that the electronic record would be "sent" by the originator. This assumes communications between two parties and does not address the attribution of electronic records, where no communication is involved. It excludes the possibility where attribution requires to be made to the originator (acting by himself) although it does not involve any "sending": - i.e., how is a saved file containing details keyed in by a person attributable to him though not sent to anyone? This is similar to a situation where a person signs a letter and retains it in a cupboard, and the letter is discovered later by a third party (either accidentally or intentionally). What would be the motive attributable to the author of the letter?

But more importantly, the Section relies on the principle of agency to attribute an electronic record to an originator, when certain action has been taken by a person other than him.

Another issue arising out of Section 11(b) would be to determine how much authority does the other person have with respect to the electronic record. For example, if some person has the authority to alter contents of the message before sending it, would the message be still attributed to the original originator? It seems that the intention of the Act is that electronic record should be attributed to the originator if sent by some other person, provided the sender acted like a postman and did not have authority to alter the contents. However, the Act is a little ambiguous and requires clarification. Otherwise, the interpretation of the scope of the authority could be tricky as in routine operations the scope of authority may be actually defined from time to time and not clearly documented.

This is similar to the principles contained in the UNCITRAL Model Law. Article 13 is the closest that the UNCITRAL Model Law comes to establishing a rule of liability. The intention is to give maximum legal weight to the authentication procedures established by the parties. Thus, under paragraph (3), if the addressee applies a procedure previously accepted by the originator and thereby obtains confirmation that the message originated from the latter, the originator is presumed to be the author of the message. This provision addresses not only the case where an authentication procedure has been agreed upon between the originator and the addressee, but also the case where the originator unilaterally or by agreement with the intermediary, has accepted a procedure

[14] Section 11 of the Act

and consented to be bound by a message, which meets the conditions laid down in that procedure.

Acknowledgement of receipt

In addition to principles of attribution, the rules of law concerning acknowledgement are also critical, as the acknowledgement of receipt would complete the communication process.

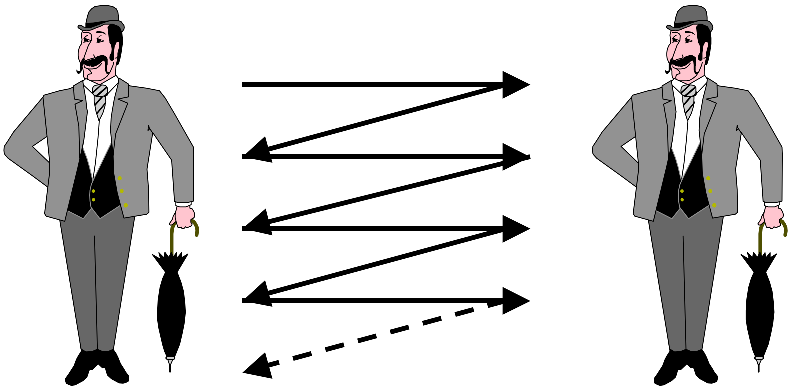
Section 12 of the Act provides for a default acknowledgement process, if the originator and the addressee have not agreed upon the particular method of acknowledgement. It is provided that an acknowledgement may be given by (i) any communication by the addressee (automated or otherwise) or (ii) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

For example, Y can expressly communicate that he has received the message sent by Y, in any manner, oral or written.

Alternately, if Y acts upon the message received from X, Y would be implied to have received the message. Assume that X has sent a message telling Y to meet him at a particular place at a particular time. If Y goes to that place at that time, he communicates by conduct that he has received the message. Even if Y calls X to say that he cannot be at that place at that time, it is implied by his conduct that he had received the communication from X.

Subsection 12(2) stipulates further that "*where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then, unless acknowledgement has been so received, the electronic record shall be deemed to have never been sent by the originator*".

While this provision *prima facie* appears reasonable, the legal fiction can lead to some unrealistic situations. To illustrate, if A sends a message and insists on an acknowledgement and B responds with an acknowledgement, but with a rider that that acknowledgement must be acknowledged, then A and B may be constantly acknowledging each other's message and may never be able to complete the loop. If one of them does not acknowledge the receipt of the other's message, then the other's message will be deemed as never sent. This may result in the previous message being deemed as never sent which would affect the earlier message and so on! Thus such legal fiction can create issues that lead to ridiculous situations.



It must be noted however, that messages under the Act are different from the concepts of "offer" and "acceptance" under the Contract Act. Depending on the facts, a message may contain an "offer", "acceptance" or a "revocation" for purposes of the Contract Act.

In addition, the Contract Act contains provisions regarding the manner in which offers and acceptances are communicated and revoked. The rules of the Contracts Act are applicable to contracts, which are concluded electronically.

Time of dispatch and receipt

The time and place of a communication are relevant to the issue whether a contract has been concluded or not. The time of the contract indicates the time from which the parties are bound to act in accordance with the contract. This is also relevant in cases where actions are time-critical. The place of contract, on the other hand, plays an important role in establishing the jurisdiction for any cause of action due to breach. Further, the time and place may be also relevant to determine whether an obligation or a condition has been performed. The rules that determine the time and place of conclusion of contracts have been keeping pace with the changing technology.

Under the Contract Act, the modes of determination of the time of formation of contracts through various means of communication have been laid down in several cases.

As regards postal contracts, a variety of theories have been propounded. They include (a) the theory that the contract is complete as soon as the offeree has made a declaration of his acceptance, (b) the theory that the contract is formed when a letter or telegram has been dispatched accepting the offer, and (c) the theory that communication of the acceptance must be received by the offeror.

When the proposal and acceptance are made by letters, the contract is made at the time when and at the place where the letter of acceptance is posted.[15] The rule with regard to telegraphs is the same as in the case of letters by post i.e. the acceptance is complete when the letter is put in the post or the telegram is handed for dispatch to the telegraph office.[16]

If a letter of acceptance is misdirected by the acceptors fault, it cannot be deemed to have been effectually put in a course of transmission to the proposer[17]. Where the intimation of acceptance does not reach the offeror, it has to be shown that the letter or telegram of acceptance was correctly addressed to the offeror otherwise it could not,

[15] Kamisetti Subbiah V. Katha Venkataswamy (1903) 27 Mad. 355; Protap Chandra V. Kali Charan, AIR1952 Cal32; Manilal V. Venkatachalapathy (1944) Mad.95; Baroda Oil Cakes V. Parshottam, AIR 1954 Bom 491 & American Pipe Co. V. State of U.P., AIR 1983 Cal. 186 at 192

[16] Bhagwandas V. Girdhari Lal & Co. 91966) A.S.C. 543; (1966) 1 S.C.R. 656
Cowan V. O'Connor, 20 Q.B.D 640 (Telegraph); Tinn V. Hoffman & Co., 29 L.T. 271, 274, 278

[17] Ram Das V. Official Liquidator, Cotton Ginning Co. (1887) 9 All. 366, 385

although posted or dispatched, be said to have been put in a course of transmission to him.[18]

In *Bhagwandas* V. *Girdhari Lal & Co.*[19], the Supreme Court held that in the case of oral communication or communication by telex or telephone, an acceptance is communicated when it is actually received by the offeror. In another landmark case in the United Kingdom, *Entores Ltd.* v *Miles Far East Corporation*[20], it was held that the rule of instantaneous communications between the parties is different from the rule of post.

In the case of communications by post, an acceptance is complete as soon as it is put in the post box and that is the place where the contract is made. In the case of instantaneous communications, the contract is made when the acceptance is received. Telephone and telex are instantaneous and direct methods of communication. The theory that the contract is formed at the time of the dispatch of the acceptance does not apply to these methods of communication - the contract is completed only at the time when the acceptance is received[21].

The question now remains whether in the case of electronic contracts, a contract is concluded when the acceptance is dispatched from the sender or when the acceptance is actually received by the offeror. To provide clarity to above ambiguity, the Act[22] provides the rules regarding time and place for electronic contracts. It must be mentioned once again that these rules are applicable to a "message" and not necessarily with respect to an "offer" or "acceptance", as understood under the Contracts Act.

The Act provides that the dispatch of an electronic record occurs when it enters an information system outside the control of the person who sent the record, unless otherwise agreed.

The time for receipt of an electronic record is determined by the time when the electronic record enters the computer resource designated by the addressee or if the electronic record is sent to a computer resource not designated by the addressee, it occurs at the time when the addressee retrieves the electronic record. Alternatively, if no computer resource has been designated, then receipt occurs when the electronic record enters the "computer resource of the addressee".

[18] Kulluram Kesharvani V. State of Madhya Pradesh & Ors. AIR 1986 M.P. 204, 206

[19] (1966) A.S.C. 543; (1966) 1 S.C.R. 656

[20] (1955) 2 Q.B. 327; All E.R. 493; (1955) 3 W.L.R. 48.

[21] The Brimnes - Tenax Steamship Co. Ltd, v. Owners of MV Brimnes, (1974) 3 All E. R. 88, 100: "*A message sent by telex is taken to have been received by the addressee when the message is received by the telex machine and not when the addressee's attention is drawn to it.*"

[22] Section 13 of the Act

The above provision, combined with the ambiguous definition of "computer resource", may pose practical problems in the real world of communication, where timing is often critical (e.g. closing of bids, last time for receiving acceptances, etc). If A were to instruct B to send an acknowledgement to A's email address XYZ@hotmail.com then, would A have designated a computer resource for receipt? If it is not construed as a designation of a computer resource, then would the alternative section apply (i.e. that receipt occurs when the electronic record enters the computer resource of the addressee)? What exactly would be the computer resource of the addressee? Will the message deemed to be received when the message reaches A's designated hotmail inbox at a remote server, or when A actually logs on to his hotmail service and retrieves the mail? What if A is notified that A has received a new message but A does not open his hotmail inbox and read the message? These are some questions, which need to be examined.

If the addressee's e-mail capability is operated on the server of a third party service provider, it could be said that e-mail is received when it arrives on that server. It would be fair to the addressee that receipt should be when the e-mail is received in the local mailbox of the addressee, or even when the addressee is notified that the e-mail has arrived or when she has also read it. Other complicating factors relate to whether the addressee's system has an open line to a remote server or a periodic dial-up access, and whether the remote server or the local server initiates transfer of data.

The rules for answering some of the questions above seem similar to those in the case of a person designating an offline postbox, where he would receive all communications. In such a case, it could be said that once the mail has been delivered into the postbox, it would bedeemed to be delivered to the addressee. The addressee would bear the consequences of his actions - of retrieving or not retrieving. However, the question becomes tricky when the issue is when the addressee cannot access the post box for reasons beyond his control. Whether a computer resource is outside or within a user's control is best decided on the basis of an assessment of the prevailing facts and factors, which could permit and those, which could prevent control, by the user. It appears that the factors, which suggest that a web-based email address is a computer resource within the control of the addressee, outweigh those, which suggest otherwise.

However, as mentioned earlier, the rules for time of dispatch and receipt of electronic messages will necessarily interact with the rules for communications of offers, acceptances and revocations under the Contract Act.

Article 14 of the UNICTRAL Model Law, places emphasis on whether the message has been received, and not whether it has been read. Singapore law[23] provides that an electronic record is dispatched when it enters an information system outside the control of the originator or the person who sent the electronic record on behalf of the originator. However, the Malaysian Digital Signatures Act is silent on this point. Therefore, the rules seem to be only those found in the Malaysian Contract Act, 1950.

These are some of the issues that need to be clarified with respect to the Act, in order to facilitate rigid principles for time of formation of online contracts.

[23] Article 15 of the Electronics Transactions Act

Place of business

The general rule under the Contracts Act, with regards to place of formation of contract in the case of instantaneous communications has been laid down in *Entores Ltd v Miles Far East Corporation,* where it was stated that "The ordinary rule of law to which, the special considerations governing contracts by post or exceptions apply is that the acceptance of an offer must be communicated to the offerer, and *the place where the contract is made is the place where the offeror receives the notification of the acceptance by the offeree*". The rule laid down in this case has been accepted in India by the majority judgment of the Supreme Court of India in Bhagwandas V. Ghirdhari Lal & Co[24].

The IT Act also sets default rules for the place of dispatch and receipt of documents. The electronic records are deemed to have been dispatched at the place the originator of the message has his principal place of business and received at the place where the addressee has his principal place of business.

These rules as regards "place of business" are in consonance with the rules in this regard under the UNCITRAL Model Law, and are identical to those under the Singapore legislation.

These rules have deeming provisions for place of dispatch and receipt, which may not be the same place where the person was while sending/receiving the electronic record. This is primarily because as newer and newer forms of technology, including Internet Protocol (where a message is broken into several bits, and sent through several routes, before being assembled back together at the receiver end) are put into use, the determination of a physical place of dispatch or receipt may be difficult.

It is in this context, that it appears most practical to equate the place of dispatch with the place of business of the sender and the place of receipt with that of the addressee. This may be also more useful to clarify determinations of place for the purposes of jurisdiction and conflicts of law rules, rather than add further confusing dimensions.

As can be seen, the provisions made above are in respect of "electronic records", regardless of the nature of their contents. The Contracts Act governs the position as regards communications, which are in the nature of a "proposal" or an "acceptance". The Contracts Act also governs the time when a contract is deemed to have concluded. Thus the rules relating to dispatch and receipt of messages under the IT Act read along with the principles of proposal, acceptance, etc under the Contract Act would determine the interpretation of an electronic contract.

International transactions

International transactions are essentially transactions, where nationals of more than one country enter into an arrangement to perform some work. The contract may pertain to work carried out in one of the countries where the parties are resident or in an entirely different third country.

[24] (1966) A.S.C. 543

The national of each country is bound by the laws of his country. Furthermore, the laws of the country where the obligations are to be performed would govern certain aspects of the transaction. So, an international transaction involves interaction between at least a minimum of 2 to 3 national legal systems. The issues arising therein are examined in the context of an example.

In a transaction involving an Indian resident in India and a United States national resident in the US A, let us assume that the Indian national has relied on the digital signature of the US national, as certified by a trusted third party in the US, Verisign. The class of the certificate provided by Verisign is Class 3.

The contract relates to a simple sale of a movable property, e.g. a stock of second-hand rare books. The sale price is fixed in US currency and the delivery is to be made at the residence of the US national.

If the parties have agreed that the contract shall be governed by US law, then, the rules of contract would be determined by the US rules of contract including time, mode and place of communication. If no law is chosen, then private international law takes over. The law of the nation having the most substantial connection would most probably be applied to the transaction.

Indian law recognizes only "digital signatures"[25] However, under other laws, eg. the Electronic Signatures in Global and National Commerce Act of the United States, no such restriction applies and a wide variety of electronic signatures are recognized as valid in law[26].

Therefore, the transaction could be made legally valid or invalid, depending on the choice of law between the contracting persons.

The above points are only a few key considerations that would affect the conclusion of electronic transactions. The principles of attribution are sought to be strengthened using appropriate identification technology. The next chapter discusses the Indian law in relation to "digital signatures", the technology recognized by Indian law.

[25] Please refer to Chapter 3: Issue and Use of Digital Signatures

[26] Section 101 and 102.

Chapter 3

Issue and Use of Digital Signatures

The Act seeks to establish "digital signatures" as the system for authentication of electronic records. Section 2(p) read with Section 3 clearly indicates that the method of authentication shall be the public key infrastructure ("PKI") which uses hash functions and asymmetric cryptosystems[27].

Section 3 provides that a "subscriber" may use a digital signature to authenticate an electronic record. A "subscriber" means a person in whose name the DSC has been issued[28]. A DSC means one which is issued by a Certifying Authority ("**CA**")[29]. A CA means a person who has been granted a licence to issue a DSC[30].

The Act provides a licensing regime for CAs, which includes recognition of foreign Certificates[31]. The regulation of CAs is primarily done by the Controller of Certification Authorities ("**Controller**"), who is vested with the functions of licensing, certifying, monitoring and overseeing the activities of CAs[32]. The Controller's functions extend to the entire spectrum of activities including:

- the standards to be maintained,
- the qualifications and experience of employees of CAs,
- the form and content in which accounts shall be maintained by CAs,
- the form and content of a digital signature certificate and the key, and,
- resolving any conflict of interests between the CA's and the subscribers.

Further, the Central Government[33] has notified the Certifying AuthorityRules **("CA Rules"**) on October 17, 2000, which prescribe the conditions under which CA's can apply for a license in India, and carry on their operations. The CA Rules contain within their purview, provisions as regards various aspects such as:

- Composition of applicant company or partnership firm;
- Networth requirements;
- PKI technology to be used for digital signatures;
- Certificate Standard;

[27] Please refer to the FAQs for further details on the same.

[28] Section 2(zg) of the Act.

[29] Section 2(q) of the Act.

[30] Section 2(g) of the Act.

[31] Chapters VI, VII and VIII of the Act.

[32] Sections 17 and 18

[33] In exercise of its powers under Section 87(2) of the Act

- Location of facilities;
- Cross-certification standards;
- Database standards;
- Period of license, subscriber's private key, subscriber's public key, CA private key, CA public key; and,
- Process of generation, issue, verification, archival, etc of DSCs.

The Rules also contain Schedules II and III, which prescribe detailed Security Guidelines that any CA has to comply with.

At this point, it would be relevant to examine some issues, which surround the legal status of a "digital signature".

Section 5 is the main provision, which provides for the legal recognition of digital signatures as a substitute for handwritten signatures. Section 5 provides also that this would be available to digital signatures, which are affixed in the manner prescribed by the Central Government. Further, Section 10 empowers the Central Government to prescribe rules regarding certain aspects of digital signatures.

On the other hand, Section 15 provides that a digital signature is a "secure digital signature" if it can be verified using a security procedure applied by the parties concerned. A secure digital signature enjoys the benefit of certain favourable presumptions under the Indian Evidence Act, 1872 ("**Evidence Act**")[34].

Section 16 goes on to provide that the Central Government shall prescribe "the security procedure", after taking into account certain prevailing commercial circumstances.

As mentioned earlier, one interpretation of Section 3 indicates that a digital signature is one, which is issued by a licenced CA. The support for this interpretation is drawn from the usage of the word "subscriber", instead of the word "person". This interpretation would necessarily mean that digital signatures, which are not issued by a licenced CA, are not recognized under the Act.

However, the language of Section 15 which refers to a security procedure 'agreed between the parties', as distinct from one 'prescribed by the Central Government', leaves some room for doubt, as regards the status of digital signatures not issued by a licenced CA. However, clearly, a digital signature, which is supported by a DSC issued by a licenced CA, has additional favourable presumptions[35].

As mentioned above, the Central Government has prescribed the CA Rules. Apparently, as suggested by the title of the CA Rules, they are primarily in respect of regulation of CAs. This would raise the question whether these CA Rules are the rules issued by Central Government under Section 5, 10 and 16 in respect of digital signatures and security procedures. However, there are certain provisions under the Rules[36], where the language seems to imply that they apply to digital signatures in

[34] Please refer to Chapter 4 : Evidentiary value of Digital Signatures and Electronic Records

[35] Please refer to Chapter 4 : Evidentiary value of digital signatures and electronic records.

general. Therefore, it may be interpreted that all digital signatures would have to comply with the CA Rules[37].

In any event, the Act along with the CA Rules is very detailed as regards the standards and regulations to be followed by CAs for the issue of digital signatures. Some of the issues relevant to the CA industry and business are summarized below:

Foreign Investment

Rule 8 of the CA Rules provides the requirements for an applicant of a CA licence. A company registered in India, having its paid-up capital and networth, each atleast Rs. 50 Million, is eligible to apply for a license. However, no company wishing to apply a license shall have more than 49% of its capital held by non-resident Indians or foreigners.

Technology

As mentioned earlier, the Act has laid down very specific criteria as regards the technology to be used with regard to authentication systems. Section 3 of the Act prescribes that "*the authentication of the electronic record shall be effected by the use of the asymmetric cryptosystem and hash function …*".

Further, Rules 6 and 7 of the CA Rules prescribe detailed technical standards to be adopted as regards the digital signatures to be issued under Indian law. Within the framework of the Act, the Rules have prescribed that all DSCs are required to conform to the ITU X.509 v(3) standard. [See Box 2 on pg 53].

This is similar to the provisions under Singapore and Malaysian Laws, which have also built their e-commerce promotion around the public key infrastructure. On the other hand, the federal Electronic Signatures in Global and National Commerce Act of the United States of America is technology neutral, where it promotes any technology having the ability to logically associate a person with an electronic record.

As mentioned earlier, there are several other technologies that provide authentication mechanisms. A technology-neutral provision would validate new technologies on the principle of being able to reliably and logically associate a communication with an individual.

Under the present Indian regime, stronger and more reliable authentication technologies would not be recognized as giving rise to digital signatures valid under the Act.

Types of Certificates

[36] Rules 3, 4 and 5

[37] This assumes that the CA Rules issued by Central Government under Sections 5, 10 and 16.

The Act recognizes a digital signature as one which authenticates the creation of an electronic record by a subscriber[38]. Further, under Section 2(zg), a subscriber is defined as any person in whose name the DSC is issued.

Chapters VI, VII and VIII of the Act, establish the framework of the relationship between the subscriber and the CA. The key obligations of the CA vis-à-vis subscriber[39], are prescribed under the Act. These are minimum obligations, which a CA has to comply with, when it issues a DSC.

World over, the digital signature industry typically offers various classes of signatures, with reference to individual subscribers. One class of the certificate is differentiated from the other based *inter alia* on (a) security level (b) price (c) period of validity, and (d) restrictions on the use of DSC.

Section 10 of the Act provides powers to the Central Government to make rules in respect of digital signatures including "the types of digital signatures". Section 15 also suggests a concept of "secure digital signatures" as distinct from ordinary digital signatures. As mentioned earlier, the "secure" status is based upon the application of a security procedure "agreed between the parties concerned". While one interpretation of provisions of the Act and the Rules[40], seems to suggest that any and all DSCs under the Act provide the same rights and impose the same liabilities on the subscribers, the distinction caused by Section 15 in favour of secure digital signatures creates some doubt.

Given the present situation, distinctions based on security level and restrictions on use of the DCS may not possible. As mentioned above, every CA has to comply with certain mimimum security levels under the Act while issuing a DSC. Any DSC which has a level below the minimum required levels would not be considered a DSC. Moreover, any digital signature, which has higher than required security levels, is not offered any advantage under the Act in terms of its status as a substitute for a signature[41]. Hence, the value proposition to a consumer as regards the legal status of a digital signature may not be clearly available.

Similarly, as regards restrictions on the use of the DSC also, the Act is very clear under Section 5 that a digital signature affixed in the means prescribed by the Central Government shall be deemed to be a signature of the person, notwithstanding any other law to the contrary. The only exceptions to this are the documents to which the Act does not apply, as referred to in Section 1(4) of the Act. Hence, any classification based on the usability or restrictions of use may not be legally sustainable, in the Indian context.

As specified in Section 36, every CA must make certain minimum representations with regard to every DSC that it issues. Over and above these minimum representations, the

[38] Section 2(p).

[39] Please refer to subsequent discussion on page.

[40] Sections 3, 5, 15, 30, 35 and 36 amongst other provisions

[41] The only exception to this is the favourable presumption under Section 15.

Act does not prohibit higher assurance levels than these levels. The assurance levels may also be used to assure differing levels of certification.

Section 10 of the Act provides that the Central Government may make rules as regards types of DSCs. But, the present CA Rules do not elaborate on the types of DSCs.

However, regardless of higher levels of assurances, a CA would require to guarantee the minimum representations as regards the identity of the subscriber, and cannot prescribe limitations. Section 5 of the Act equates the digital signature to a regular signature where required by law.

For instance, a DSC issued specifically to members for use in online trading processes could be used by members to conduct some other transactions e.g. purchase orders for consumer goods. A relying party who relies on such DSC issued by a CA authenticating the signature for the member, may have a valid claim on that CA if the identity of the member is discovered to be false, even though the DSC has been used for purposes other than online trading.

To take another instance, a DSC from a CA limited to validating that an electronic record is from a particular email identity, without any corroboration of the person's identity, may not be treated as a digital signature recognizable in Indian courts. Alternatively, if such a DSC were treated as a digital signature, then the CA would be in breach of its obligations to carry on authentication functions before issuing such a DSC or take on the liability as if it had authenticated the person’s identity.

Hence, the CA and the subscriber would have to find a meeting point on differing values of the DSCs, given that the Act and the Rules place severe limitations on a CA in product diversity.

Group certificates

In another scenario, provision of DSCs to corporates or groups of persons, also poses challenges within the framework of the Act. Section 2 (zg) defines "subscriber" to mean a person in whose name the DSC is issued.

According to Rule 2 (i), "person" shall include an individual or a company or association or a body of individuals, whether incorporated or not; or Central Government or a State government or any of the ministries or departments, agencies or authorities of such governments. Therefore, the Act seems to contemplate the issuance of DSCs to associations of persons or juristic persons like companies. Thus, it is like combining the Company seal and the signature of the authorized representative in the physical world without revealing who the authorized representative were. However, the Act is unclear on how the identity and acts of these entities or associations would interact with their legal status and legal capacity under other laws in force.

When issuing a DSC to a juristic person, the choice as to who would be the "Named Entity"[42] and who the "subscriber" is, to say the least, challenging. The relation between the Named Entity and the Subscriber becomes very complex. This involves

[42] Please refer to FAQs

establishing details as regards when an individual can act on behalf of a juristic person, which is governed by various other laws as well as rules and regulations of the juristic person itself.

It is possible that an entity having no legal status or capacity to contract under existing laws, may be able to obtain an identity (and ability to authenticate documents) under the Act. Thus, though a DSC may be validly issued to such an entity, the DSC may be not be used in a manner inconsistent with other laws which govern the capacity to contract.

An instance of Identity vis-à-vis capacity

1. Company has independent *identity* under the Companies Act, 1956.
2. Company can *act* only through individuals acting on behalf of the Company.
3. Such authorisation or individuals acting would depend on specific provisions of the Companies Act
4. DSC may be issued to company under the Act/Rules.
5. The use of DSC though valid under the Act would be governed and be subject to the Companies Act, 1956.

The Act provides for the issuance of DSC to a company. However, there are no guidelines or Rules that indicate the manner of use of such DSC. Consequently, a DSC may be used in a manner that is invalid under the Companies Act, 1956, although validly issued. The CA should therefore, carefully determine the scope of use of the DSC. Moreover, the CA should also ensure that its exposure to unauthorised acts is limited by deeming clauses in its Certification Practise Statement or other agreements.

Equipment signatures

In the new era, it is quite common to have automated replies from various web service providers. These can be provided from different kinds of servers, using various kinds of software. Typical automated replies (such as online order confirmations) may actually amount to acceptance of contracts.

Given that web-based communication systems are not foolproof from external interference, it becomes critical to ensure that the order confirmations actually are from the web service provider. In such cases, it would become necessary to determine whether the signature is to be attributed to equipment or if it should be attributed to the person who is in control of the equipment.

Logically, the signature cannot be attributed to a piece of equipment in entirety because a piece of equipment is not a legal entity and cannot make decisions. Therefore, it appears that signatures can be issued to a person only. However, the person who relies on such certificate should be made aware of the relationship between the person (i.e. subscriber), the CA and the equipment. This would require careful documentation of the extent of risks / liabilities and the limitations thereon.

However, given the reality and the high proliferation of programmable equipment which can be instructed to act in a particular manner, there would be many permutations and combinations with regard to the attributions of an equipment's actions to the person who is in control of the equipment. This is likely to be more interesting because of concerns of the person who owns / controls the equipment about the "tamper-proof" nature of the equipment, in an age where remote hacking incidents seem to become commonplace.

Identification

Under Section 36(e), the CA, while issuing a DSC is required to represent the information contained in the DSC as accurate. As per Rule 10, the information contained in the Certificate includes the name of the subscriber whose public key is identified by the particular DSC.

Further, Rules 25(2) requires the CA to comply with the procedure defined in the CPS for verification of identification (i.e. the "subscriber identity verification method" defined under Rule 2(k) as a method used to verify and authenticate the identity of a subscriber). This subscriber identity verification method would require to be approved by the Controller[43].

Neither the Act nor the CA Rules prescribe guidelines as regards such verification procedures. It seems that, since the subscriber verification method would be vetted by the Controller, the Controller would have discretion in determining the methods employed by the CA. In any event, approval by the Controller might not relieve the CA of the responsibility to ensure such verification and authentication of the identity of the subscriber.

Neither the Act nor the CA Rules contain any express provision as to whether such identification processes can be outsourced. It appears that there would be no bar on such outsourcing to specific registration authorities. However, such registration authorities are likely to be construed as trusted persons and the CA would bear consequent liability for such actions of the registration authorities.

Conditions relating to issuance of Certificates

Rule 24 provides that the issuance of a DSC shall *inter alia* involves binding the key pair associated with the DSC, with the owner of the DSC.

As a pre-condition to issue of a DSC, Rule 25 requires that a CA, prior to issuance of DSC, confirms that the subscriber name does not appear in its list of compromised users and obtain consent from the user that the details of such DSC can be published on a directory service. The Rule further goes on to provide that the CA "shall comply with all privacy requirements". The scope of this provision is uncertain and may involve liabilities.

The exact events of generation / issue of a DSC are described under Rule 24. Any CA would require to be in compliance with these technical requirements.

Upon the issue of a DSC, Section 36 provides that: "The Certifying Authority shall represent the following, inter alia at the time of issuance:

[43] As provided under Rules 10(ii)(b) & 23(e)

- It has published the DSC or otherwise made it available to such person relying on it;
- Subscriber holds the private key corresponding to the public key listed in the DSC;
- The subscriber's public key and private key constitute a functioning key pair;
- The information contained in the DSC is accurate; and,
- It has no knowledge of any material fact, which would adversely affect the reliability of the above representations.

All DSCs are required to be issued with a designated expiry date (as per Rule 26). Guideline 21 of Schedule III provides that the expiry date under the CA Rules should not exceed 5 years from the date of issue. However, the recommended period for subscriber's DSC is 3 years. Upon the expiry of the Certificate, the CA is required to archive the DSCs. The details of the archival obligations of a CA are provided below.

It is relevant to mention at this point that Section 73 provides for a prohibition on publication or making available a DSC with the knowledge that the CA listed in the DSC has not issued it or that the subscriber has not accepted it or the DSC has been suspended or revoked.

Suspension and Revocation

The Act (Section 37) prescribes certain situations where a CA may suspend a DSC:

- Upon request by the subscriber or any person authorised, or
- In public interest

However, the Act also provides that no DSC may be suspended for period exceeding 15 days, without providing an opportunity to the subscriber.

The Act (Section 38) and the CA Rules also prescribe certain situations where a CA may revoke a DSC:

- Upon request by the subscriber or any person authorised, or
- On death of the subscriber, or
- Upon dissolution of the firm or winding up of the company.

Although the above provisions provide situations where the CA "is authorized" to suspend or revoke, this discretion would carry with `it an obligation to ensure that appropriate revocation or suspension occurs.

Apart from the above situations where the CA has discretionary power, the CA has definite obligations to revoke a DSC under Rule 29 in case of a compromise of the DSC, misuse of the DSC, misrepresentation or errors in the DSC and where the DSC is no longer required.

Rule 28 states that "compromise" *inter alia* means where the private key associated with the DSC is in doubt. The terms "misuse" of the Certificate and "where the DSC is no longer required" are ambiguous.

In practical terms, the CA would require to clearly delimit what would amount to "misuse" or "expiry of requirement". This would not only require a detailed assessment of what are the practical situations, but also involve careful documentation of the understanding between the CA and all parties.

CA is also required to take best efforts to be immediately notified upon the occurrence of such events and can revoke the Certificate. Upon revocation, the CA is required to publish DSC details in its Certificate Revocation List.

Location of facilities

Rule 9 requires that infrastructure associated with all functions of generation, issue and management of DSCs as well as maintenance of directories shall be located in India. Several Indian players were looking to establish collaborations with foreign CAs, where they could obtain licenses in India to issue DSCs while outsourcing their back-end or technology support functions. There is some debate on what the exact extent of this provision is (certificate server, directory server, key recovery server, etc). As and when, these kinds of collaborations are established, Controller would have to decide on their legality. It would be appropriate for the controller to clarify these issues upfront so as to avoid any confusion.

Ownership of facilities

Neither the Act nor the CA Rules lay down express conditions or restrictions relating to ownership of the infrastructure by the CA. Hence, it appears that the direction of regulation is on the service as provided by the licensed CA regardless of who owns the infrastructure. However, it must be kept in mind that location restrictions, as enumerated earlier, would apply to such infrastructure.

Audit of operations

Rules 31 and 32 require that the CA ensures that an independent auditor audits its operations. Further, the CA is required to conduct a half-yearly audit of its security policy, physical security, planning of its operations and a quarterly audit of its operations. Under Rule 20, the Certifying Authority can commence operations, among other things, only after the audit of its operations.

Root Certificates

There are no provisions of the Act/CA Rules that expressly require a CA to generate its own DSC. However, Guideline 18.3 of the Schedule III prescribes storage requirements of the CA keys.

Guideline 21.1.4 requires the CA to define key change process that ensures reliability of the process by showing how the generation of key interlocks - such as signing a hash of the new key with the old key. Further, there is a distinction made between CA’s private signing keys, root keys and associated DSCs for certain periods of validity.

Cross-certification

Rules 12 and 20 require that a CA cannot commence operations until it has made arrangements for cross-certification with other licensed CA's.

This provision in one sense can be seen as forcing the CA Industry to come forth and establish common standards to promote use of digital signatures. However, because of this provision, it is logically not possible for any one CA to start operations unilaterally. This provision on cross-certification makes it a very high level integration. This is because most Indian CAs would be trusted by or trust other foreign CAs. Hence, cross-certification in India would mean the establishment of a certification chain between the different foreign entities as well.

Interestingly, the two draft versions of the CA Rules did not contain any such provision and the final CA Rules caught the industry by surprise. While the objective to provide for seamless authentication services is laudable, the mechanism of achieving it in this manner appears myopic. As of now, no one entity can start issuing DSCs unless there exists another entity licenced by a CA and they both see eye-to-eye on the certification services.

Moreover, the reason for insistence on cross-certification is not clear. Typically, cross-certification is required in an environment where there is no assurance of trust except by interdependence or where there are several trust levels (types of certificates). However, in the Indian context, the trust is guaranteed by statute and does not require contractual agreement. Moreover, it appears that there cannot be several types of certificates, under the Act. Hence, it remains to be seen what this provision will achieve.

Lifetime of DSC

The Security Guidelines (Schedule III annexed to the CA Rules) provide recommendations as regards the operational period of the certificate. Under Para 21 of the Security Guidelines, the suggested period for a subscribers private key is three years[44]. The suggested period for the CA's root keys and associated certificates is five years; although the suggested period for CA's private signing key is two years.

Archives and records

The CA Rules also provide that all DSCs must be archived for a period of seven years or the period of legal requirement. What constitutes "the period of legal requirement" is highly ambiguous, and open to different interpretations. In certain cases, for instance, copyright assignment (the period of validity is life of author + 60 years), the signature on the assignment document may be required to be maintained for more than a 100 years. Imagine then the situation! This ambiguity would leave every CA doubtful if it has fulfilled its obligations.

Rule 27 requires the Certifying Authority to maintain archives of:

- Applications for issue of DSCs;
- Registration and verification documents of DSCs;
- DSC;

[44] Para 21.1(4)

- Notices of suspension;
- Information of suspended DSC;
- Information of revoked DSC;
- Expired DSC.

for a minimum period of 7 years or as per the legal requirement.

Guideline 9 of Schedule II requires the CA to maintain back-ups of a number of critical items including encryption keys, datafiles, databases. Specifically, Guideline 6 provides that offsite backup shall be secure and located within India.

Section 30 (b) provides a general obligation that the Certifying Authority ensures a reasonable level of reliability of its services. Guideline 9 and 10 of Schedule III govern the maintenance of audit trails for verification of transaction patterns and adequate back-ups.

Recognition of foreign CAs

Section 19 of the Act provides that the Controller can make recognize certificates issued by Foreign CAs (subject to specified regulations and prior approval of the Central Government).

As of date, no regulations have been issued as regards the recognition of foreign CA's except Rule 12(2) of the CA Rules. Rule 12(2) provides that any arrangement for cross-certification between an Indian CA and a foreign CA, must be specifically approved by the Controller, prior to commencement of such cross-certification operations.

If any DSCs were recognized under Section 19 of the Act, a person in India would then be able to use such DSC. It appears that such use would be restricted i.e., that Indian residents would be able to rely only on such DSC which is provided by the resident of another country. However, it appears unlikely that an Indian resident would be able to obtain certificates from foreign CAs, which can then be issued to other transactions. If not, then there would be no necessity for CAs to establish a commercial presence on ground in India, as all certifications can be applied for and issued online. Also, the 49% foreign investment restriction would be bypassed.

In the absence of any such recognition, it appears that a person in India cannot contend that he validly relied on a DSC issued by a foreign CA.

The Singapore law prescribes reasonably similar guidelines. Section 42 of the Singapore Act (based on Chapter III of the draft UNCITRAL Rules) provides that signatures issued under foreign laws which are equivalent to the laws of Singapore. The Singapore law further provides guidelines, which establish the criteria for judging the equivalence. The determination of equivalence may be made by the Controller (based on the above criteria and published in the Official Gazette) or through bilateral or multilateral agreements with other countries. The Controller is also authorized to specify that a particular class of certificates, or a particular CA, be used in relation to particular messages.

Malaysian law also establishes criteria for recognition of a foreign CA. Central to the concept of recognition is that an international treaty, agreement or convention concerning the recognition of foreign certificates has been concluded to which Malaysia is a party. However, the certificate issued by the foreign CA must demonstrate a level of security equal to or more stringent than the level of security of a certificate issued by a licensed CA of Malaysia.

Application process and checklist

The basic requirements for an application for a CA licence are provided under Section 22 of the Act and Rule 10 of the CA Rules. The form of application has also been provided as Schedule 1 to the CA Rules.

Box 2 Technical Standards under Rule 6 in respect of CAs

Product	Standard
Public key infrastructure	PKIX
DSCs and Digital signature revocation list	X.509 version 3 certificates specified in ITU RFC 1422
Directory (DAP and LDAP)	X500 for publication of certificates and revocation lists
Database management operations	use of generic SQL
Public key algorithm	DSA and RSA
Digital hash function	MD5 and SHA-1
RSA public key technology	PKCS#1 RSA encryption standard (512, 1024, 2048 bit) PKCS#5 password based encryption standard PKCS#7 cryptographic message syntax standard PKCS#9 selected attribute types PKCS#10 RSA certification request PKCS#8 private key information syntax standard PKCS#12 portable format for storing / transporting a user's private keys and certificates
Distinguished name	X.520
Digital encryption and digital signature	PKCS#7
Digital signature request format	PKCS#10

Chapter 4

Evidentiary Value Of Electronic Records And Digital Signatures

Chapter V of the Act is exclusively dedicated to "security". Titled as *Secure Electronic Records and Secure Digital Signatures*, this Chapter consists of 3 Sections which describe when an electronic record and a digital signature would be deemed "secure" and a provision enabling the Central Government to make rules prescribing the security procedure. Secure electronic records and digital signatures are granted certain evidentiary value. These are provided by way of amendments to Evidence Act, which are contained in Schedule 2 to the Act.

Secure Electronic Records

Section 14 of the Act provides that an electronic record would be deemed "secure", if "any security procedure" has been applied to an electronic record. It shall be deemed secure from the time the security procedure was applied upto the point in time of verification. It is not clear what could amount to a "security procedure" valid under this Section, though the scope seems to be very wide.

Section 16 provides that the Central Government shall prescribe the security procedure for the purposes of the Act, having regard to prevailing commercial circumstances such as

- The nature of the transaction
- The level of sophistication of the parties
- The volume of similar transactions
- The cost and availability of alternatives
- The procedures used generally in comparable transactions

Section 15 provides that parties can agree on the security procedures to be applied, whereas Section 16 provides that the Government will decide on security procedures to be applied. Section 15 is not subject to Section 16 nor is Section 16 subject to Section 15. They seem to be operating independently of each other, and validly.

This raises a question as regards how to resolve any inconsistencies between the parties as regards, the security procedures.

While one interpretation could mean that parties could adopt any security procedures under Section 15 of the Act, there could also be the other proposition that by necessary implication, Section 15 is subject to Section 16. Also, at the present moment, the Government has not notified any procedures under Section 16 (although security procedures have been notified for CA). Hence, in the absence of procedures notified under Section 16, it appears that parties would choose their own security procedures.

A secure electronic record and a secure digital signature can avail of beneficial provisions in the amended Evidence Act

Section 67A of the Evidence Act requires that any person wishing to rely on the fact that an electronic record has been digitally signed by a particular person must prove such a fact, unless the digital signature is a secure digital signature.

Section 85B of the Evidence Act raises a presumption that a secure record has not been altered until the point in time when such secure record was verified, which otherwise would have required specific proof. Further, the Section provides that the Court would presume in any proceedings involving a secure digital signature that the secure digital signature is affixed by the subscriber with the intent of signing or approving the electronic record and that the information listed in a DSC is correct (except specific non-verified subscriber information).

These presumptions have a far-reaching impact in the conduct of business, as these provide the required impetus to persons who would seek to rely on another's ostensible statements of intent.

The definition of "evidence" has been expanded to expressly include electronic records. Further, Section 17A has been introduced to include statements in electronic formats also as "admissions" if they suggest any inference to any fact in issue or relevant fact.

The Evidence Act contained a provision (Section 22) that oral admissions as regards any document are not relevant unless and until the party proposing them show that (a) he is entitled to give secondary evidence of the contents of such document, or, (b) the genuineness of the document produced is in question. Further, Section 65 prescribes that situations which secondary evidence relating to documents may be given. The amendment made by the Act now introduces Section 22A by which the same rule as regards oral admissions is extended to electronic documents as well.

Sections 65A and 65B relate to conditions of admissibility of electronic records. Section 65B in particular provides that information contained in an electronic record (which is stored or printed) would also be considered as a document and shall be admissible if certain conditions are satisfied

a. the computer output containing the information was produced by the computer during the period over which the lawful person was having control over that computer regularly;
b. there has been input generally into the computer which would generate the kind of information contained in the output;
c. the computer was operating properly or if not, then the period in which it was out of operation or did not operate properly did not affect the electronic record or the accuracy of the contents; and,
d. the information contained in the electronic record reproduces or is derived from the information fed into the computer in the ordinary course of activities.

From a plain reading of the Section, it appears that the person adducing electronic records requires to demonstrate that the above conditions are satisfied before he / she can rely on a particular electronic record. And imagine the plight of one who wishes to rely on an e-mail received at his hotmail.com or usa.net id. How many computers would he have to show as working properly before he can rely on a printed version of that e-mail?

In addition to the above sections, Sections 85A, 85B, 88A and 90A have been introduced in the Evidence Act. These sections offer various presumptions in favour of electronic agreements, secure electronic records, electronic messages and electronic records over 5 years old.

It may be particularly interesting to note that Section 88A provides that any message sent through an email server will be presumed by a Court to have been fed into a computer for transmission. But the Court is barred from making any presumption as regards the person who fed in the message. The evaluation of the person who sent the message can be made only on an examination of facts, and not on a presumption.

In general, this is consistent with the provisions of the UNCITRAL Model law. The Singapore law also similarly provides for security procedures between parties. Procedures agreed between parties are granted the greatest weight. When, an addressee applies an agreed procedure and determines that the originator has sent the message, then the originator is presumed to be the author of the message. This provision addresses not only the case where an authentication procedure has been agreed between the originator and the addressee, but also the case where the originator unilaterally, or by agreement with the intermediary, has accepted a procedure and consented to be bound by a message which meets the conditions laid down in that procedure.

Although it may be appropriate to place emphasis upon agreement between the parties, it may not be appropriate to establish a presumption of attribution in favour of any authentication procedures, as the security and reliability of such procedures vary so markedly that there is no factual basis for establishing such a presumption.

Secure Digital Signatures

Section 15 provides that a digital signature would be deemed "secure" if, after application of the security procedure, it is established that the digital signature (a) was unique to the subscriber affixing it (b) was capable of identifying such subscriber (c) was created in a manner or using a means under the exclusive control of the subscriber, and (d) is invalidated if the electronic record is tampered with. While this section read by itself seems very wide, the definition of digital signature limits the technology to only asymmetric cryptosystems. The conditions of uniqueness and logical association are captured in Section 3 itself and hence, are redundant. The additional conditions in Section 15 which are not present in Section 3 are exclusive control and tamper-proof nature.

Section 85B of the Evidence Act provides a favourable presumption of the "intention" in respect of "secure digital signatures". The Court is required to presume that the secure digital signature is affixed by the subscriber with "the intention of signing or approving the electronic record".

However, a digital signature supported by a DSC, has certain additional advantages.

To begin with, Section 85C provides a very important presumption as regards "identity" of the subscriber. This Section requires the Court to presume that the information listed in DSC is correct, except for information, which has not been verified. This presumption is perhaps at the root of the evidentiary value of a digital signature and contributes

Further, Section 47A has been inserted in the Evidence Act which provides that when the Court has to form any opinion about the digital signature of any person, the opinion of the CA is a relevant fact.

Section 67A provides that except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record, then the fact that such digital signature is the digital signature of the subscriber must be proved. Further, in order to make such an assessment, the Court may order that person or the CA or the Controller to produce the digital signature certificate. This seems to indicate that the CA is capable of issuing digital signatures, which are not secure. However, when one views the entire framework of the Act, and in particular Section 15 (which defines a "secure digital signature"), it appears redundant to have such provisions since all digital signatures would be secure.

As can be seen, a very important consideration in legal proceedings is the evidentiary value of each party's contention. Much of the enforceability of an electronic transaction or an electronic record would depend on the evidence produced in Court and its sustainability. Therefore, while deciding upon the issue or use of a digital signature, it would be critical to make sure that the final choice provides maximum evidentiary value.

Chapter 5

Electronic Governance

The purpose of the Act is to promote the use of electronic records and establish equality between the paper records and electronic records. The language of the Act (Section 4 and 5) leaves no room for doubt that electronic records and digital signatures are valid substitutes for written records and signatures.

However, the Act is not only in respect of private transactions. In fact, Chapter III of the Act is entirely dedicated to the use of electronic records in the course of dealings with and within the Government.

Sections 6, 7 and 8 further clarify the use of the electronic records in the Government.

The various uses envisaged for citizens are:

- filing of forms, applications like tax returns, etc.;
- payment of money; and,
- retention of records required by law.

The various uses envisaged for the Government are:

- issue of sanctions, permits, licences, etc.; and,
- publications of rules, regulations, etc. in an Electronic Gazette.

Interestingly, Section 9 of the Act provides an exemption to the Government from complying with the provisions of Section 6, 7 and 8 as regards accepting, retaining and publishing electronic records. Though, there are no express words that the Government agencies are exempted from complying with Sections 4 and Section 5 as regards electronic records, the reality remains that this provision leaves room for favourable interpretation, by the Government agencies to refuse to accept electronic filings. (For example, income tax returns, applications, etc.)

The exemption afforded to Government bodies, is a popular exemption. Many countries having similar legislation have made provisions for recognition of electronic records. Such a provision is made essentially to provide the Government bodies a window to organize the infrastructure necessary to maintain the various kinds of records is put into place. Considering the varied nature of records and documents maintained by the Government along with the huge volumes of such records, it appears that this provision providing time to the Government to work out adequate mechanisms to incorporate the use of electronic records and digital signatures into its working, is justified.

Another issue, which the Govt. would have to address, would be that of the payment of stamp duty for electronic documents. New modalities of stamping of the documents and payment of stamp duty would have to be worked out. For example, the stamp duty payable on a general agreement is Rs. 100. The exact procedure for making payment for such agreements entered online would have to be addressed.

Chapter 6

Penalties and Offences

Though the Internet has made the world a smaller place to live in, it has also made it unsafe. Moreover, it is relatively more difficult and sometimes practically impossible to locate and stalk the guilty party.

The Act has broadly categorized contraventions of two types - those, which are loosely of a criminal nature i.e., bear consequences of imprisonment and other contraventions.

Chapter IX of the Act describes several contraventions such as making unauthorised copies, unauthorised access to records, introduction of 'computer contaminants', denial of access, etc. A violation of such nature would result in monetary penalty and/or compensation to be paid to the affected party.

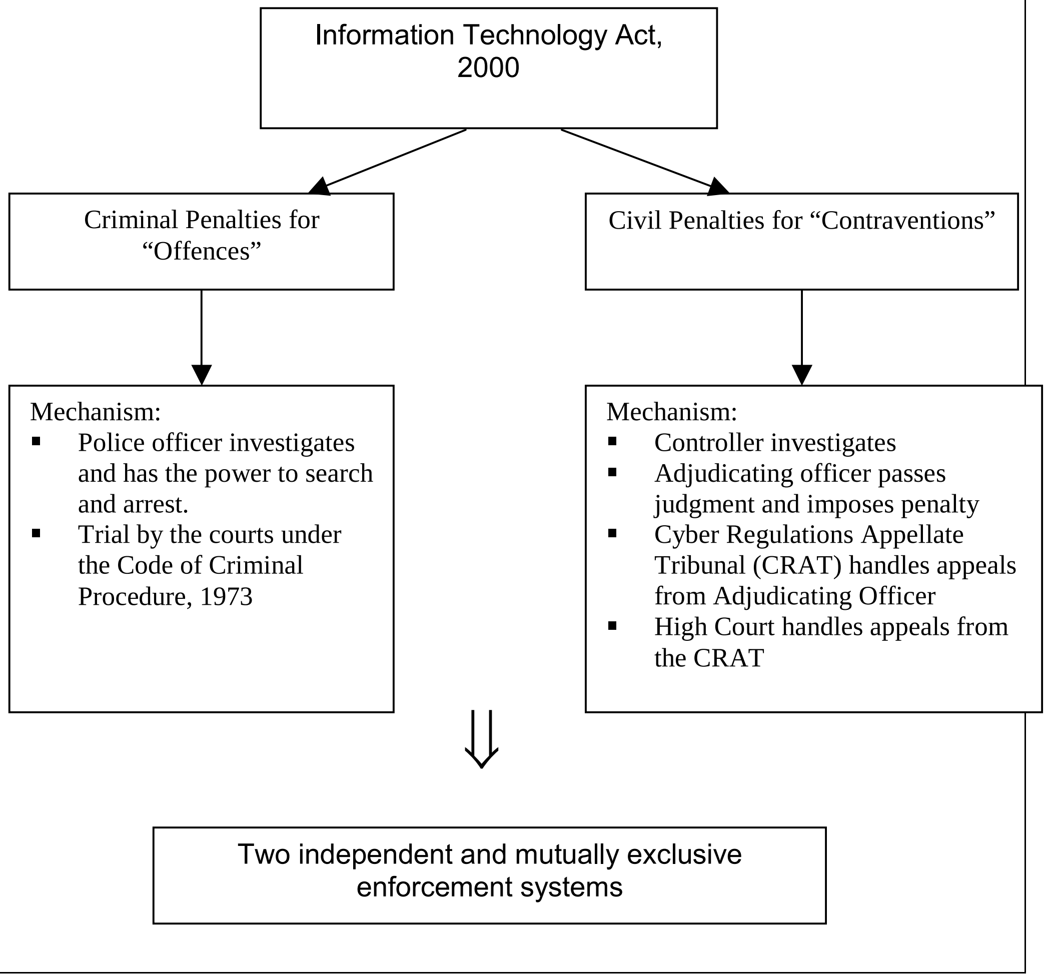
Chapter XI of the Act describes several offences such as tampering with source codes, hacking, publication or transmission of obscene information; misrepresentation of facts for obtaining DSC, publication of a false DSC, etc. These are punishable with imprisonment as well as monetary penalty.

Some of these offences and contraventions are based on criminal intent or knowledge of the person perpetrating the crime (e.g. tampering with computer source documents, hacking, publication of digital signatures for fraudulent purpose). On the other hand, there are some others, which are purely based on the commission of certain acts, even if unintentionally or unknowingly (damage to computer systems, publication of obscene information in electronic form, misrepresentation, breach of confidentiality, publication of false DSC). Although there is no specific element of *mens rea* in certain offences, it appears from the traditions of criminal jurisprudence, which the Courtsare likely to look at the criminal intent behind a particular action.

Chapter IX of the Act (“Penalties and Adjudication”) includes civil violations carrying only monetary penalties, while Chapter XI (“Offences”) relates to criminal offences punishable by fine or imprisonment, or both. However, neither of these chapters is titled in a manner that explains such a distinction. Furthermore, references to both civil and criminal violations are included in both chapters, and the terms “offence” and “contravention” are used transposably in Chapter XI.

The Act attempts to introduce two separate and distinct mechanisms for dealing with misfeasance - one apparently for civil misfeasance and the other for criminal misfeasance.

Box 3: Enforcement mechanisms



Information Technology Act, 2000

Criminal Penalties for "Offences"

Civil Penalties for "Contraventions"

Mechanism:
- Police officer investigates and has the power to search and arrest.
- Trial by the courts under the Code of Criminal Procedure, 1973

Mechanism:
- Controller investigates
- Adjudicating officer passes judgment and imposes penalty
- Cyber Regulations Appellate Tribunal (CRAT) handles appeals from Adjudicating Officer
- High Court handles appeals from the CRAT

Two independent and mutually exclusive enforcement systems

The civil mechanism broadly provides for the following:

- The Controller (appointed under Section 17) shall investigate any contraventions of the provisions of the Act under Section 28.

- Section 46 provides for the appointment of an Adjudicating Officer who has the powers of a civil court. The Adjudicating Officer's responsibilities include:
  - offering the accused person the opportunity to make a representation in the matter,
  - deciding whether that person has in fact committed the contravention, and
  - imposing the proper compensation and penalties.

- The CRAT consists of one person, and handles appeals from orders made by an adjudicating officer. After providing a hearing for the parties, the CRAT may confirm, modify, or set aside the adjudicating officer's order. The CRAT also has the powers of a civil court.

- Section 62 of the Act establishes that appeals from the CRAT on any question of fact or law may be filed with the High Court.

- Section 61 confers exclusive jurisdiction upon the adjudicating authority and the CRAT, stating that no court has the authority to hear any proceeding that falls under the command of either body.

The criminal mechanism broadly deals with the following:

Sections 78 and 80 enable a police officer to investigate any criminal offence under the Act, and allows such an officer to search and arrest any person in a public place without a warrant, if that person is reasonably suspected of having committed an offence under the Act. Criminal cases are then tried in regular courts in accordance with the Code of Criminal Procedure, 1973.

Though these mechanisms may seem clearly distinct, the language of the Act fails to clearly distinguish the types of violations under the two mechanisms, leaving open the possibility for an overlap of powers. The terms “contravention” and “offence” have been used interchangeably in an ambiguous and confusing manner. These terms ought to have been defined in the Act such that it is clear that “contravention” applies strictly to civil violations and “offence” applies only to criminal infringements. As it stands now, interpretation of the Act may be problematic because the Act is not otherwise organized in a way that clearly differentiates civil from criminal violations and vice versa.

We have briefly set out illustrative examples wherein the Act uses the terms "offences" and "contravention" interchangeably thereby creating ambiguity and overlap of powers.

- Sections 28, 29, 43(g), 45, 46, 63 use the term “contravention” in a civil context and relate to the powers of the Controller and envisage only monetary penalties instead of imprisonment.

- Further, Sections 33, 68, 78, & 80 apply the term “offence” in the criminal context and deal with the powers of the police and impose criminal punishment.

- However, Sections 69, 70, 76, & 85 use the terms “offence” and “contravention” interchangeably and ambiguously, for example:

    - Section 69(1), under the “Offences” chapter, allows the Controller to intercept information “for preventing incitement to the commission of any cognizable “offence” It is unclear whether the term “offence applies to civil &/or criminal violations, but one could reasonably guess that it would apply to both since the Controller would want to prevent the commission of either violation.
    - Section 70, also under the ‘Offences’ chapter, uses the term “contravention” in a criminal rather than civil context. It states that a person who accesses a protected system “in contravention of the provisions of this section shall be punished with imprisonment….”Granted, the phrase used is “in contravention” as opposed to using the term “contravention” as a noun, but similar wording is used civilly in Section 43(g).
    - Section 76 uses the term “contravention” in a very general manner. It is also in the “Offences” chapter, but it seems like it should apply in both criminal and civil contexts because confiscation may be necessary in either case.

- Section 85 is particularly confusing because it is entitled "*Offences* by companies" and yet the body of the section uses the term "contravention" multiple times while making *no mention* of "offences." This section seems to use the terms interchangeably, and it is unclear whether it applies to civil or criminal violations, or both.

The Act, aims to create individual civil and criminal adjudication mechanisms for dealing with infractions under its governance. It is apparent that the creation of a separation of powers between the two mechanisms was intended. However, the Act fails to meet its objective because of an ambiguity in its terms. Since the terms "offence" and "contravention" have been used interchangeably, there could be an overlap between the civil and criminal mechanisms of the Act.

The power to investigate "contraventions" is given to the Controller under Section 28 of the Act, while the authority to investigate "offences" is given to police officers under Section 78. Without clear and distinct definitions of the terms "offence" and "contravention," the Act does not appropriately serve its purpose of establishing two separate machinery for dealing with violations of the Act thereby creating an ambiguity and overlap of powers. If the two mechanisms outlined in the Act are to operate free from questions of interpretation, then the terms of those mechanisms ought to be plainly distinguished.

Extra territorial application

The applicability of the Act extends to any offence or contravention committed even outside India (and to any person irrespective of nationality) if the offence involves a computer, computer system or computer network located in India[45]. Undoubtedly, Internet crime is characterized by complexity due to the multitude of jurisdictions affected, the anonymous perpetrators. The complexities are bound to increase as corporate entities play the roles of perpetrators and victims of Internet related crime.

In such a scenario, the actual enforcement of such an extraterritorial provision of the Act would depend on critical international co-operation. As has been experienced in the case of the Lovebug virus, although there were damages worth millions of dollars - the prime suspects located in Philippines could not be extradited to other countries, since the national law of Philippines did not recognize such behaviour as criminal[46]. Depending on the magnitude of the damage, it may be expected that several international jurisdictional issues would be raised. What if there are several countries that are affected? Would the Indian statute be applicable even if only a very few computers are affected? What if although only few computers are affected, the damage runs into several millions?

Further, certain issues arise out of the requirements prescribed in the Act that a computer, computer network, and computer system should be located in India for the Indian courts to try offences or contraventions. For example, if the website of an Indian company which is hosted outside India (which is most likely the case), is hacked by a

[45] Section 75 of the Act

[46] Source: www.mb.com.ph/MAIN/2000-05/MN050903.asp

person outside India, there could be no contravention of the Act (unless the internet is treated as computer network). Moreover, if an offence (say hacking) is committed by a person from a country A on a website of a company situated in country B, then as per the Act, the Indian courts would have jurisdiction to try the offense even though the offender and the damage caused have no connection with India. Such jurisdiction would be conferred on the Indian courts merely on the ground that the server, which was used in the process of hacking, is situated in India.

Chapter 7

Network Service Provider Immunity

The Act contains provisions dealing with the liability of Network Service Providers (**NSPs**)[47]. A NSP has been defined under the Act to mean "an intermediary"[48]. An "intermediary", with respect to any particular electronic message, means any person who on behalf of another person, receives, stores or transmits that message or provides any service with respect to that message.

The Act stipulates that every NSP is given general immunity as regards any offence under or in contravention of the Act or the provisions made thereunder, if such NSP proves that (i) such offence or contravention was committed without its knowledge or (ii) that it had exercised all due diligence to prevent the commission of such offence or contravention.

There are two issues that arise with respect to this provision.

- Who would be considered to be a NSP?
- Under what circumstances would the NSP be liable?

Who would be considered to be NSP?

As per the definition under the Act, a NSP is restricted to a person who on behalf of another person, receives, stores or transmits a message or provides any service with respect to that message. However, it is not clear as to who would be considered to be an intermediary / a NSP outside the context of the message.

For example, it is not clear whether a website that provides hyperlinks could be considered as a NSP and could be held liable for any damage due to the hyperlinking.

Under what circumstances would the NSP be liable?

It appears that the lawmakers have intended to hold the NSP responsible only if an offence is committed using its network with its knowledge and it fails to exercise all due diligence.

So, in the event that the offence or contravention is committed with the knowledge of the NSP, but the NSP has exercised all due diligence to prevent the offence or contravention, it would not be held liable.

Certain difficulties may arise while determining the liability of a NSP. Firstly, the Internet is a dynamic phenomenon, and it would be virtually impossible to prove that the NSP had knowledge of the contravention or offence that was taking place on its network. Secondly, in the absence of well-defined standards, it may be problematic to assess as to what amounts to “due diligence”.

Imagine an online retailer, who acts as a selling agent to various software manufacturers. One of the software manufacturers specifically sells hacker software

[47] Section 79

[48] Section 2 (w)

(Superscan, Attack, Leaktest, to name a few) along with express statements that this could be used to break firewalls, and set up watch dogs at ports / network points. Presumably, the target market is a legitimate one i.e. that of penetration service providers, but there is no method of determining the bonafides or other intentions of the buyers.

The final act of the buyer is to use the software to hack into a computer system and steal some confidential information. Even prima facie, such buyer is clearly guilty under Section 66 of the Act (Hacking). But the question arises whether the online retailer would be liable under the rather widely phrased Section 43(g) *("provides any assistance to any person to facilitate access any computer, computer system or computer network by any means").*

If such an action were filed against the online retailer, in the absence of any detailed documentation between the online retailer and such manufacturer, would the online retailer be able to avail of the immunity under Section 79? Would the retail provider be a NSP in the first place i.e. an intermediary? Can it be said to have no knowledge of such contravention? Can it be said to have carried out all due diligence?

This hypothetical situation is not very far removed from reality. Recently, a hugely popular portal "rediff.com" faced criminal charges for abetting pornography, since users visiting rediff.com could use the search engine to locate pornographic sites. Although, the case was brought under the provisions of the Indian Penal Code (Section 292 (distribution of pornographic material) and Section 109 (abetment)), it could well have been brought under Section 67 of the Act (Publishing of information which is obscene in electronic form). In such an event, would it be possible for Rediff to have successfully claimed immunity under Section 79?

The person who has initiated action against Rediff insists that other sites such as 123india.com and Compuserve.com, had successfully filtered all obscene materials from their sites, using technology for filtering the obscene material. If so, then would the standard of "all due diligence" mean adopting such technology? For, it appears difficult for a website to claim no knowledge of the content that it throws up.

This highly ambiguous provision is in contrast to other legislations in the world such as the Digital Millenium Copyright Act, 1998 or the Communications Decency Act 1996 of the USA, which are very detailed legislations on just this one concept. The lack of clarity in the Indian provision may give rise to peculiar situations.

There are at present, no precedents in India to address either the question of lack of knowledge or the standards of "due diligence". There are theoretical possibilities with regard to attribution of knowledge such as "constructive knowledge" which may be applied to an NSP, even when it has no actual knowledge. However, whether such a principle of "constructive knowledge" can be applied to an NSP remains to be seen. Much deeper thought is necessary as regards the definition and role of a NSP to enable fair fixation of liability and immunity.

The immunity is for contravention under this Act and not under any other law. Thus even if Rediff was able to claim immunity under IT Act, it could have been prosecuted under the IPC. Also, liability with respect to copyright violation that is a major issue globally (for which the US has enacted the Digital Millenium Copyright Act, 1998) is not addressed. Such exceptions may render the immunity under this section ineffective.

Chapter 8

Recent Developments

A. LEGISLATION

1. Internet Based Securities Trading and Services

The Internet offers an express and economically feasible mode of conducting trade in securities. In order to efficaciously tap this source, the Securities and Exchange Board of India (**SEBI**) constituted a standing committee on Internet Based Securities Trading and Services (**Committee**). The Committee, under the chairmanship of Mr. O.P. Gahrotra, examined and clarified some of the regulatory and other issues related to Internet based securities trading and services. The Committee took stock of the developments in the use of Internet in securities business at the international level and within the country. The Committee submitted its report to SEBI, which issued a circular on January 31, 2000 introducing the Internet Based Securities Trading and Services Guidelines (**Guidelines**).

As per the Guidelines, Internet based trading can take place through order routing systems, which will route client orders to exchange trading systems for execution of trades on the existing stock exchanges. Brokers registered with the SEBI under the SEBI (Stock Brokers and Sub-brokers) Rules and Regulations, 1992 can introduce the service after obtaining permission from the recognized stock exchanges.

For the purpose of the law, the transactions entered into under these Guidelines would be electronic contracts and hence the provisions of the Information Technology Act would be applicable. The Guidelines supplement this view by stipulating that the participants / traders must use authentication technologies to verify / authenticate the transactions. As of now, the Act recognises only digital signatures based the Public Key Infrastructure system and thus only this technology can be used to verify or authenticate an electronic contract. The Guidelines further state that signatures must only be obtained from Certifying Authorities that are notified by the SEBI. However, till such time that the Controller of Certifying Authorities issues licenses to Certifying Authorities, all electronic trading transactions will have to be backed up by offline contract note. Also the guidelines envisage offline agreement between the subscribers and broker for the purposes of online trading.

Moreover, as per the Act, an electronic record would also be considered to be evidence in a court of law.

2. Internet Banking

On June 14, 2001, the Reserve Bank of India ("**RBI**") announced Internet Banking Guidelines ("**Banking Guidelines**") in India. The Banking Guidelines focus on three areas:

- technology and security issues;
- legal issues; and

- regulatory and supervisory issues.

The Banking Guidelines state that though the PKI system of technology is favourable for securing Internet banking services, while the PKI is being developed certain alternative technologies can be used. (However, it is uncertain whether these alternative technologies will be acceptable as per the Information Technology Act.) The Banking Guidelines themselves recognise this factor as a legal risk with respect to Internet Banking services.

3. Communications Convergence Bill

Pursuant to a landmark judgment in *Union of India v Cricket Association of Bengal*, the Supreme Court of India pointed out that the existing legislation for broadcasting media was inadequate. It was therefore imperative for Parliament to make a law in respect of broadcasting media as a whole. Pursuant to this, the Communications Convergence Bill (**Bill**) was drafted and is still pending its introduction in the Parliament. Once the Bill is passed by both houses of Parliament, receives Presidential assent and is duly notified,it will become law.

The Bill addresses the carriage issues as well as the content issues. The carriage issue deals with telecom infrastructure and network service provider, while the content issue deals with application service provider like broadcasting services and e-commerce services. The Bill provides essentially for a single super-regulator i.e the Communications Commission of India (**CCI**) to govern the information, communication and entertainment sectors. The CCI will handle all regulatory and licensing functions in the areas of telecommunications, broadcasting and Internet.

The current draft of the Bill includes a clause to form two separate bureaus to regulate 'content' and 'carriage' under the CCI. The content bureau under the CCI is expected to regulate and monitor contents in the electronic media. It is likely that the bureau for content regulation under CCI would comprise of people concerned with art, literature, education, and consumers, while carriage would be overseen by technical experts.

Payment Systems Regulations Act

The Information Technology Act paved the way for digital signatures and digital contracts in India. As a logical follow up, the Reserve Bank of India (**RBI**), in consultation with the National Payment Council is in the process of giving final touches to the draft of the Payment Systems Regulations Act. This proposed legislation will bring in all electronic fund transfers in the country, such as money orders, settlements at payment gateways, stock and commodity exchanges and clearing houses under the jurisdiction of the RBI.

B. PUBLIC INTEREST LITIGATION (PIL)

1. PIL filed in Delhi High Court to prevent cyberporn.[4950]

[49] http://groups.yahoo.com/group/cyberlaw-india/message/289

The case of the Delhi schoolboy who was arrested for creating a pornographic website has provided more ammunition to India's moral busybodies who want to restrict access to the Internet by adolescents.

In March, public interest litigation was filed in Delhi High Court by the New Delhi-based advocate, Mr. Pradeep Kumar, against the Cabinet Secretary, the police commissioner of Delhi, the Delhi government, and the union ministries of Communications, Science and Technology, Home Affairs, Information and Broadcasting, Human Resources Development, and Social Welfare, Justice and Empowerment.

The petitioners wanted the government to formulate procedures to prevent Indians, especially minors, from accessing pornographic websites as well as those advocating drugs, alcohol, and tobacco. They wanted the government to direct all Indian Internet service providers (ISPs) to install filtering software at their gateways to prevent access to such websites. They also wanted all cyber cafes and educational institutions to compulsorily installfiltering software on their computers to "prevent exposure to inappropriate material that is sexual, hateful, or violent in nature, or encourages activities that are dangerous or illegal". They sought compulsory licensing of cyber cafes by the government, and demanded: "At cyber cafes, children below 18 years of age should be allowed to surf the internet only when they produce a permission letter from their parents, attested by a gazetted officer". The petitioners also wanted all cybercafés to maintain complete records of all the websites, chat rooms and bulletin boards visited by each one of their customers.
Admitting the PIL, a division bench consisting of Chief Justice Arijit Passayat and Justice D. K. Jain directed the cabinet secretary to "hold a meeting of various ministries and file an affidavit indicating the definite stand taken by the government."

The Delhi petitioners' demand that all cyber cafes and educational institutions should maintain complete records of all the websites, chat rooms and bulletin boards visited by each one of their customers was rejected by both the Lok Sabha and Rajya Sabha in May 2000 while passing the Information Technology Act, 1999. It would not be correct for Indian courts to permit such a measure when Parliament has already rejected clause 73 of the IT Act.

The Delhi petitioners' demand that all Indian ISPs should install filtering software at their servers is neither technologically feasible nor legally tenable. Surfers can easily bypass filtering programs installed at their ISP's gateway, such as Cyber Cop, Cyber Patrol, etc. Joe McNamee, head of the European Internet Service Providers Association in Brussels, admitted: "It is nearly impossible for any ISP to prevent its subscribers from accessing any particular website. The easiest way of bypassing ISP-level filters is to use one of the many Anonymizer services that are available for free."

In response to this PIL, the Ministry of Information Technology (**MIT**) has just kicked off a fight against the menace of cyber-porn and its entry into Indian homes. In collaboration with National Informatics Centre (**NCI**), the MIT has put up a Web site which hosts comprehensive information on the impact the harmful content on the internet might have on children and the ways to tackle it. [51] A working group headed by the Secretary,

[50] http://www.hindustantimes.com/nonfram/010501/bigidea.asp

Information Technology, and the Home Secretary, Human Resource Development, among others, is simultaneously working out an action plan to tackle the issue before it acquired alarming proportions.

The recommendations of the working group will be submitted to the Cabinet, which will take it up for discussion before chalking out a comprehensive action plan.

However MIT's action plan will be largely dependent on how much response they get from the public. While it is largely the responsibility of parents to monitor Internet usage, MIT has put up a guide on their Web site for them to follow. Any other strategy that MIT might chalk out will necessarily depend on the extent of concern among the public about this issue. The Government site lists out the e-mail addresses of various State police headquarters, including Delhi, Haryana, Chandigarh and Madhya Pradesh, which can be contacted by anybody coming across instances of online exploitation of children.

2. Petition in the Mumbai High Court seeks ban on cyberporn [52]

A writ petition, was admitted *suo moto* by Justice Ranjan Kochar of the Mumbai High Court as a PIL on June 25, 2001 to curb cyberporn over the Internet. Justice Kochar described the issue of pornography on Internet as ``cultural pollution".

Jayesh Thakkar, a law student at K C College, and his classmate Sunil Thacker, had written a letter to the chief justice of the city high court, drawing his attention to one website in particular which contained details like whereabouts of sex workers, agents, massage parlours and pick-up joints in Maharashtra and other states in the country. They requested him to ban such sites and initiate legal action that prevents or controls access to cyberporn.

This, however, is easier said than done. Officers at the cyber crime cell of the Mumbai police say that provisions of the Information Technology Act or the Indian Penal Code fall short of coping with this menace. Moreover, servers abroad usually host such sites and it involves a complex procedure and a bit of luck to get the Internet Service Provider to cooperate and black out the site. However, even that can be bypassed by floating mirror sites.

While the Indian legal fraternity is slowly waking up to the cyberporn issue, a PIL, like the one filed in Mumbai, is pending with the Delhi High Court.

C. DOMAIN NAME DISPUTES

Indian Courts have been instrumental in protecting popular in the offline world (such as TATA, Tanishq) and the online world (such as Yahoo, Rediff) against cybersquatting.

In the cases of *Yahoo, Inc. v. Akash Arora* (Delhi) and *Rediff Communications Ltd. v Cyberbooth* (Bombay), the Indian Courts held that using a domain name similar to that of another person's trademark constitutes violation of trademark rights and such actions

[51] http://www.indiasoftware.com/news/n1707.html

[52] http://www.indiatimes.com/news/130701toi/13indi14.htm

were treated as passing off. In the *Yahoo* case, the Court further held that due to the nature of Internet use, the defendant's appropriation of the plaintiff's mark as a domain name and home page address couldn't adequately be remedied by a disclaimer.

Hence, it appears that the Indian judiciary is also keen to develop an effective and balanced jurisprudence, which is not unfair to anyone.

D. RECENT NEWS ITEMS

ED raids Skybiz offices[53]

During May 2001, the Enforcement Directorate raided several offices of Skybiz 2000, an internet company, in Mumbai, Pune, Chennai and Bangalore for gross violations of the Foreign Exchange Maintenance Act, 1999 running into Rs. 100 crore. Siphoning off money through Internet schemes amounted to hawala transactions. Besides the RBI regulations, the company violated the provisions of the Prize Chits and Money Circulation Schemes (Banning) Act and the Information Technology Act. The Company since its inception in 1999, cultivated subscribers who had to shell out US $ 125 in the beginning followed by US $ 100 every year. The subscriber in turn, would get 70% of the money for every new subscriber he arranged for the company.

Skybiz has over 4 lakh subscribers from India and 8 websites through which people can line up as subscribers. The demand draft for Rs. 6,500 (US $ 125) favouring Skybiz India Pvt. Ltd. Mumbai has to be sent to Oklahoma office. As the entire business is conducted through the net, the RBI would have no details of the exchange transactions taking place. The ED raids followed the recent decision of the Delhi High Court to admit a PIL filed against Skybiz in this regard.

[53] http://cbi.nic.in/fmay01.htm