The Information Technology Act, 2000
(21 of 2000)

as amended by
The Negotiable Instruments (Amendment and Miscellaneous Provisions) Act, 2002
(55 of 2002)
&
The Information Technology (Removal of Difficulties)
Order, 2002
alongwith
♦ The Information Technology (Certifying Authorities)
Rules, 2000
♦ The Cyber Regulations Appellate Tribunal (Procedure)
Rules, 2000
♦ The Information Technology (Certifying Authority)
Regulations, 2001
♦ The Cyber Regulations Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Presiding Office.) Rules, 2003
♦ The Information Technology (Other Powers of Civil Court Vested in Cyber Appellate Tribunal) Rules, 2003
♦ The Information Technology (Other Standards) Rules, 2003
♦ The Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004
&
♦ The Information Technology (Security Procedure)
Rules, 2004

Edited by
Krishan Arora

PROFESSIONAL BOOK PUBLISHERS
NEW DELHI
THE INFORMATION TECHNOLOGY ACT, 2000

CONTENTS

CHAPTER I
PRELIMINARY
1. Short title, extent, commencement and application
2. Definitions

CHAPTER II
DIGITAL SIGNATURE
3. Authentication of electronic records

CHAPTER III
ELECTRONIC GOVERNANCE
4. Legal recognition of electronic records
5. Legal recognition of digital signatures
6. Use of electronic records and digital signatures in Government and its agencies
7. Retention of electronic records
8. Publication of rules, regulations, etc., in Electronic Gazette
9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form
10. Power to make rules by Central Government in respect of digital signature

CHAPTER IV
ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS
11. Attribution of electronic record
12. Acknowledgement of receipt
13. Time and place of despatch and receipt of electronic records

CHAPTER V
SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES
14. Secure electronic record
15. Secure digital signature
16. Security procedure

CHAPTER VI
REGULATION OF CERTIFYING AUTHORITIES
17. Appointment of Controller and other officers
18. Functions of Controller
19. Recognition of foreign Certifying Authorities
20. Controller to act as repository
21. Licence to issue Digital Signature Certificates
22. Application for licence
23. Renewal of licence
24. Procedure for grant or rejection of licence
25. Suspension of licence
26. Notice of suspension or revocation of licence
27. Power to delegate
28. Power to investigate contraventions
29. Access to computers and data
30. Certifying Authority to follow certain procedures

Page
2
3
5
6
6
6
7
7
8
8
8
9
9
10
11
11
11
11
12
12
12
12
13
13
13
13
13
CONTENTS

1. Certifying Authority to ensure compliance of the Act, etc. .......................... 31
2. Display of licence ......................................................................................... 32
3. Surrender of licence ..................................................................................... 33
4. Disclosure ..................................................................................................... 33

CHAPTER VII

GITAL SIGNATURE CERTIFICATES .................................................................. 35
5. Certifying Authority to issue Digital Signature Certificate .................. 35
6. Representations upon issuance of Digital Signature Certificate ........ 36
7. Suspension of Digital Signature Certificate .............................................. 37
8. Revocation of Digital Signature Certificate ............................................. 38
9. Notice of suspension or revocation ............................................................. 39

CHAPTER VIII

DUTIES OF SUBSCRIBERS .............................................................................. 40
10. Generating key pair ...................................................................................... 40
11. Acceptance of Digital Signature Certificate .......................................... 41
12. Control of private key .................................................................................. 42

CHAPTER IX

PENALTIES AND ADJUDICATION ................................................................ 43
13. Penalty for damage to computer, computer system, etc. .................... 43
14. Penalty for failure to furnish information, return, etc. ......................... 44
15. Residuary penalty ......................................................................................... 45
16. Power to adjudicate ...................................................................................... 46
17. Factors to be taken into account by the adjudicating officer ............. 47

CHAPTER X

THE CYBER REGULATION: APPELLATE TRIBUNAL .................................. 48
18. Establishment of Cyber Appellate Tribunal ............................................ 48
19. Composition of Cyber Appellate Tribunal .............................................. 49
20. Qualification for appointment as Presiding Officer of the Cyber Appellate Tribunal ........................................................................................................... 50
21. Term of office ............................................................................................... 51
22. Salary, allowances and other terms and conditions of service of Presiding Officer ........................................................................................................... 52
23. Filling up of vacancies .................................................................................. 53
24. Resignation and removal ............................................................................. 54
25. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings ........................................................................................................... 55
26. Staff of the Cyber Appellate Tribunal ....................................................... 56
27. Appeal to Cyber Appellate Tribunal .......................................................... 57
28. Procedure and powers of the Cyber Appellate Tribunal .................... 58
29. Right of legal representation ..................................................................... 59
30. Limitation .................................................................................................... 60
31. Civil Court not to have jurisdiction ............................................................ 61
32. Appeal to High Court .................................................................................. 62
33. Compounding of contraventions ................................................................. 63
34. Recovery of penalty ...................................................................................... 64

CHAPTER XI

OFFENCES ........................................................................................................ 65
35. Tampering with computer source documents ....................................... 65
36. Hacking with computer system .................................................................. 66
37. Publishing of information which is obscene in electronic form ........... 67

THE INFORMATION TECHNOLOGY (CERTIFYING AUTHORITIES) RULES, 2000

1. Short title and commencement .................................................................... 37
2. Definitions ..................................................................................................... 37
3. The manner in which information be authenticated by means of Digital Signature ........................................................................................................... 38
4. Creation of Digital Signature ...................................................................... 38
5. Verification of Digital Signature ................................................................. 38
6. Standards ...................................................................................................... 38
7. Digital Signature Certifying Standard ....................................................... 39
8. Licensing of Certificate Authorities ............................................................ 40
Table of Contents

**THE CYBER REGULATIONS APPELLATE TRIBUNAL (PROCEDURE) RULES, 2000**

1. Short title and commencement
2. Definitions
3. Procedure for filing applications
4. Presentation and scrutiny of applications
5. Place of filing application
6. Application fee
7. Contents of application
8. Paper book, etc., to accompany the application
9. Plural remedies
10. Service of notice of application on the respondents
11. Filing of reply and other documents by the respondent
12. Date and place of hearing to be notified
13. Sittings of the Tribunal
14. Decision on applications
15. Action on application for applicant's default
16. Hearing on application ex parte
17. Adjournment of application
18. Order to be signed and dated
19. Publication of orders
20. Communication of orders to parties
21. No fee for inspection of records
22. Orders and directions in certain cases
23. Registration of legal practitioners' clerks
24. Working hours of the Tribunal
25. Sitting hours of the Tribunal
26. Powers and functions of the Registrar
27. Additional powers and duties of Registrar
28. Seal and emblem

**THE INFORMATION TECHNOLOGY (CERTIFYING AUTHORITY) REGULATIONS, 2001**

Section 1
1. Short title and commencement
2. Definitions
3. Terms and conditions of licence to issue Digital Signature Certificate
4. The standards followed by the Certifying Authority for carrying out its functions
5. Every Certifying Authority shall disclose
6. Communication of compromise of Private Key

**THE CYBER REGULATIONS APPELLATE TRIBUNAL (PROCEDURE FOR INVESTIGATION OF MISBEHAVIOUR OR INCAPACITY OF PRESIDING OFFICER) RULES, 2003**

1. Short title and commencement
2. Definitions
3. Committee for investigation of complaints
4. Judge to conduct inquiry
5. Application of the Departmental Inquiries (Enforcement of Witness and Production of Documents) Act, 1972 to inquiries under these rules
6. Powers of Judge
7. Suspension of Presiding Officer
8. Subsistence allowance
9. Inquiry Report

**THE INFORMATION TECHNOLOGY (OTHER POWERS OF CIVIL COURT VESTED IN CYBER APPELLATE TRIBUNAL) RULES, 2003**

1. Short title and commencement
2. Definitions
3. Powers of Cyber Appellate Tribunal
### THE INFORMATION TECHNOLOGY (OTHER STANDARDS) RULES, 2003

<table>
<thead>
<tr>
<th>Rule</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Short title and commencement</td>
<td>......</td>
</tr>
<tr>
<td>2. Definitions</td>
<td>......</td>
</tr>
<tr>
<td>3. Standards to be observed by the Controller</td>
<td>......</td>
</tr>
</tbody>
</table>

### THE INFORMATION TECHNOLOGY (USE OF ELECTRONIC RECORDS AND DIGITAL SIGNATURES) RULES, 2004

<table>
<thead>
<tr>
<th>Rule</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Short title and commencement</td>
<td>......</td>
</tr>
<tr>
<td>2. Definitions</td>
<td>......</td>
</tr>
<tr>
<td>3. Filing of form, application or any other document</td>
<td>......</td>
</tr>
<tr>
<td>4. Issue or grant of any licence, permit, sanction or approval</td>
<td>......</td>
</tr>
<tr>
<td>5. Payment and receipt of fee or charges</td>
<td>......</td>
</tr>
</tbody>
</table>

### THE INFORMATION TECHNOLOGY (SECURITY PROCEDURE) RULES, 2004

<table>
<thead>
<tr>
<th>Rule</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Short title and commencement</td>
<td>......</td>
</tr>
<tr>
<td>2. Definitions</td>
<td>......</td>
</tr>
<tr>
<td>3. Secure electronic record</td>
<td>......</td>
</tr>
<tr>
<td>4. Secure digital signature</td>
<td>......</td>
</tr>
</tbody>
</table>

---

**THE INFORMATION TECHNOLOGY ACT, 2000**

(21 OF 2000)

[9th June, 2000]

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce" which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto;


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

And Whereas it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records;

Be it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:

**Statement of Objects and Reasons.—** New communication systems and digital technology have made dramatic changes in the way we live. A revolution is occurring in the way people transact business. Businesses and consumers are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in electronic form has many advantages. It is cheaper, easier to store, retrieve and speedier to communicate. Although people are aware of these advantages, they are reluctant to conduct business or conclude any transaction in the electronic form due to lack of appropriate legal framework. The two principal hurdles which stand in the way of facilitating electronic commerce and electronic governance are the requirements as to writing and signature for legal recognition. At present many legal provisions assume the existence of paper-based records and documents and records which should bear signatures. The Law of Evidence is traditionally based upon paper based records and oral testimony. Since electronic commerce eliminates the need for paper based transactions, hence to facilitate e-commerce, the need for legal changes have become an urgent necessity. International trade through the medium of e-commerce is growing rapidly in the past few years and many countries have switched over from traditional paper based commerce to e-commerce.

The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in 1996. The General Assembly of United Nations by its Resolution No. 51/162, dated 30th January, 1997, recommended that all States should give favourable considerations to the said Model Law when they enact or revise their laws. The Model Law provides for equal legal treatment of users of electronic communication and paper based communication. Pursuant to a recent declaration by member countries, the World Trade Organisation is likely to form a work programme to handle its work in this area including the possible creation of multilateral trade deals through the medium of electronic commerce.
3. There is a need for bringing in suitable amendments in the existing laws in our country to facilitate e-commerce. It is, therefore, proposed to provide for legal recognition of electronic records and digital signatures. This will enable the conclusion of contracts and the creation of rights and obligations through the electronic medium. It is also proposed to provide for a regulatory regime to supervise the Certifying Authorities issuing Digital Signature Certificates. To prevent the possible misuse arising out of transactions and other dealings concluded over the electronic medium, it is also proposed to create civil and criminal liabilities for contravention of the provisions of the proposed legislation.

4. With a view to facilitate Electronic Governance, it is proposed to provide for the use and acceptance of electronic records and digital signatures in the Government offices and its agencies. This will make the citizens interaction with the Governmental offices hassle free.

5. It is also proposed to make consequential amendments in the Indian Penal Code and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions. It is also proposed to amend the Reserve Bank of India Act, 1934 to facilitate electronic fund transfers between the financial institutions and banks and the Banks’ Books Evidence Act, 1891 to give legal sanctity for books of account maintained in the electronic form by the banks.

6. The proposal was also circulated to the State Governments. They have supported the proposed legislation and have also expressed urgency for such legislation.

7. The Bill seeks to achieve the above objectives.

CHAPTER I
PRELIMINARY

1. Short title, extent, commencement and application.—(1) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, apply also to any offence or contravention thereunder committed outside India by any person.

(3) It shall come into force on such date as the Central Government may, by notification appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

(4) Nothing in this Act shall apply to—

(a) a negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881 (26 of 1881);

(b) a power of attorney as defined in section 1-A of the Powers-of-Attorney Act, 1882 (7 of 1882);

(c) a trust as defined in section 3 of the Indian Trusts Act, 1882 (2 of 1882);

(d) a Will as defined in clause (h) of section (2) of the Indian Succession Act, 1925 (39 of 1925), including any other testamentary disposition by whatever name called;

(e) any contract for the sale or conveyance of immovable property or any interest in such property;

(f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

2. Definitions.—(1) In this Act, unless the context otherwise requires—

(a) “access”, with its grammatical variations and cognate expressions, means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;

(b) “addressee” means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) “adjudicating officer” means an adjudicating officer appointed under sub-section (1) of section 46;

(d) “affixing digital signature”, with its grammatical variations and cognate expressions, means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

(e) “appropriate Government” means as respects any matter,—

(i) enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution,

the State Government and in any other case, the Central Government;

(f) “asymmetric crypto system” means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) “Certifying Authority” means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;

(h) “certification practice statement” means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

(i) “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;

(j) “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;

(k) “computer resource” means computer, computer system, computer network, data, computer database or software;

(l) “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 programs, electronic instructions, input data


2. Substituted by the Negotiable Instruments (Amendment and Miscellaneous Provisions) Act, 2002 (55 of 2002), Sec. 12, for Cl. (a) (w.e.f. 6-2-2003). Prior to its substitution, Cl. (a) read as under—“(a) a negotiable instrument as defined in section 1 of the Negotiable Instruments Act, 1881 (26 of 1881).”
and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 17;

(n) "Cyber Appellate Tribunal" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

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

(q) "Digital Signature Certificate" means a Digital Signature Certificate issued under sub-section (4) of section 35;

(r) "electronic form", with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) "Electronic Gazette" means the Official Gazette published in the electronic form;

(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(u) "function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(v) "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;

(w) "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;

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

(y) "law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be, Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made thereunder;

(z) "licence" means a licence granted to a Certifying Authority under section 24;

(zA) "originator" means a person who sends, generates, stores or transmits any electronic message, or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb) "prescribed" means prescribed by rules made under this Act;

(zc) "private key" means the key of a key pair used to create a digital signature;

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

(ze) "secure system" means computer hardware, software, and procedure that—

(a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

(zf) "security procedure" means the security procedure prescribed under section 16 by the Central Government;

(zg) "subscriber" means a person in whose name the Digital Signature Certificate is issued;

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

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

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

(2) Any reference in this Act to any enactment or any provision thereof shall, in relation to an area in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER II

DIGITAL SIGNATURE

3. Authentication of electronic records.—(1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

'2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation.—For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

CHAPTER III
ELECTRONIC GOVERNANCE

4. Legal recognition of electronic records.—Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

5. Legal recognition of digital signatures.—Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

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

6. Use of electronic records and digital signatures in Government and its agencies.—(1) Where any law provides for—

(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner,

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe—

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fees or charges for filing, creation or issue of any electronic record under clause (a).

7. Retention of electronic records.—(1) Where any law provides that documents, records or information shall be retained for any specific period,

then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if—

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

8. Publication of rule, regulation, etc., in Electronic Gazette.—Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

Provided that where any rule, regulation, order, by-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form.—Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

10. Power to make rules by Central Government in respect of digital signature.—The Central Government may, for the purposes of this Act, by rules, prescribe—

(a) the type of digital signature;

(b) the manner and format in which the digital signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the digital signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to digital signatures.
CHAPTER IV
ATRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

11. Attribution of electronic records.—An electronic record shall be attributed to the originator—

(a) if it was sent by the originator himself;
(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.

12. Acknowledgment of receipt.—(1) Where the originator has not agreed with the addressee that the acknowledgement of receipt of electronic record be given in a particular form or by a particular method, an acknowledgement may be given by—

(a) any communication by the addressee, automated or otherwise; or
(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) 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.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then, the originator may give notice to the addressee stating that no acknowledgement has been received by him specifying a reasonable time by which the acknowledgement must be received by him and if no acknowledgement is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and place of despatch and receipt of electronic record.—(1) Save as otherwise agreed between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the exclusive control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, for the time of receipt of an electronic record shall be determined as follows, namely:

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records,—

(i) receipt occurs at the time when the electronic record enters the designated computer resource; or
(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(c) any conduct of the originator to act in a manner which was not reasonable in the circumstances prevailing at the time when the procedure was used, including—

(i) the nature of the transaction;
(ii) the level of sophistication of the parties with reference to their technological capacity;
(iii) the volume of similar transactions engaged in by other parties;
(iv) the cost of alternative procedures; and
(v) the procedures in general use for similar types of transactions or communications.
CHAPTER VI
REGULATION OF CERTIFYING AUTHORITIES

17. Appointment of Controller and other officers.—(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification, appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

18. Functions of Controller.—The Controller may perform all or any of the following functions, namely:

(a) exercising supervision over the activities of the Certifying Authorities;
(b) certifying public keys of the Certifying Authorities;
(c) laying down the standards to be maintained by the Certifying Authorities;
(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;
(g) specifying the form and content of a Digital Signature Certificate and the key;
(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
(l) resolving any conflict of interests between the Certifying Authorities and the subscribers:
(m) laying down the duties of the Certifying Authorities;
(n) maintaining a database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

19. Recognition of foreign Certifying Authorities.—(1) Subject to such conditions and restrictions as may be specified, by regulations, the Controller may, with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

20. Controller to act as repository.—(1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall—

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;
(b) observe such other standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.

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

21. Licence to issue Digital Signature Certificates.—(1) Subject to the provisions of sub-section (2), any person may make an application to the Controller for a licence to issue Digital Signature Certificates.

(2) No licence shall be issued under sub-section (1), unless the applicant fulfils such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government.

(3) A licence granted under this section shall—

(a) be valid for such period as may be prescribed by the Central Government;
(b) not be transferable or heritable;
(c) be subject to such terms and conditions as may be specified by the regulations.

22. Application for licence.—(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by—

(a) a certification practice statement;
3. Substituted by the Information Technology (Removal of Difficulties) Order, 2002, or Cl. (c) (w.e.f. 19-9-2002). Prior to its substitution, Cl. (c) read as under—‘‘(c) failed to maintain the standards specified under clause (b) of sub-section (2) of section 20.”

Provided that the database containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock:

Provided further that the Controller may, if he considers necessary, publicise the contents of database in such electronic or other media, as he may consider appropriate.

27. Power to delegate.—The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

28. Power to investigate contraventions.—(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 (43 of 1961), and shall exercise such powers, subject to such limitations laid down under that Act.

29. Access to computers and data.—(1) Without prejudice to the provisions of sub-section (1) of section 68, the Controller or any person authorised by him shall, if he has reasonable cause to believe that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purposes of sub-section (1), the Controller or any person authorised by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

30. Certifying Authority to follow certain procedures.—Every Certifying Authority shall—

(a) make use of hardware, software, and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) observe such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc.—Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations or orders made thereunder.

32. Display of licence.—Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

33. Surrender of licence.—(1) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.
(2) Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

34. Disclosure.—(1) Every Certifying Authority shall disclose in the manner specified by regulations—
(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;
(b) any certification practice statement relevant thereto;
(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and
(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority’s ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall—
(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or
(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

CHAPTER VII
DIGITAL SIGNATURE CERTIFICATES

35. Certifying authority to issue Digital Signature Certificate.—(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application:

Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that—
(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;
(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant;

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

36. Representations upon issuance of Digital Signature Certificate.—A Certifying Authority while issuing a Digital Signature Certificate shall certify that—
(a) it has complied with the provisions of this Act and the rules and regulations made thereunder;
(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;
(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;
(d) the subscriber’s public key and private key constitute a functioning key pair;
(e) the information contained in the Digital Signature Certificate is accurate; and
(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

37. Suspension of Digital Signature Certificate.—(1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,

(a) on receipt of a request—
(i) from the subscriber listed in the Digital Signature Certificate; or
(ii) any person duly authorised to act on behalf of that subscriber;

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.

(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

38. Revocation of Digital Signature Certificate.—(1) A Certifying Authority may revoke a Digital Signature Certificate issued by it—
(a) where the subscriber or any other person authorised by him makes a request to that effect;
(b) upon the death of the subscriber; or
(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital
Signature Certificate which has been issued by it at any time, if it is of opinion that—

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;
(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;
(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;
(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Notice of suspension or revocation.—(1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

CHAPTER VIII
DUTIES OF SUBSCRIBERS

40. Generating key pair.—Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, [1*], the subscriber shall generate [that key] pair by applying the security procedure.

41. Acceptance of Digital Signature Certificate.—(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate—

(a) to one or more persons;
(b) in a repository; or
otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

4. The word “then” omitted by the Information Technology (Removal of Difficulties) Order, 2002 (w.e.f. 19-9-2002).

5. Substituted by the Information Technology (Removal of Difficulties) Order, 2002, for “the key” (w.e.f. 19-9-2002).

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

42. Control of private key.—(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure [* * *].

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation.—For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

CHAPTER IX
PENALTIES AND ADJUDICATION

43. Penalty for damage to computer, computer system, etc.—If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network—

(a) accesses or secures access to such computer, computer system or computer network;
(b) downloads, copies or extracts any data, computer database —

information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(d) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programs residing in such computer, computer system or computer network;
(e) disrupts or causes disruption of any computer, computer system or computer network;
(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
(h) charges the services availed by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation.—For the purposes of this section,—

(i) “computer contaminant” means any set of computer instructions that are designed—

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

6. The words “to a person not authorised to affix the digital signature of the subscriber” omitted by the Information Technology (Removal of Difficulties) Order, 2002 (w.e.f. 19-9-2002).
(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(ii) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

44. Penalty for failure to furnish information, return, etc.—If any person who is required under this Act or any rules or regulations made thereunder—

(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(c) maintain a book of account or record fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. Residuary penalty.—Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

46. Power to adjudicate.—(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder, the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a Civil Court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and—

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code (45 of 1860);

(b) shall be deemed to be a Civil Court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974).

47. Factors to be taken into account by the adjudicating officer.—While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely—

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default.

CHAPTER X

THE CYBER REGULATIONS APPELLATE TRIBUNAL

48. Establishment of Cyber Appellate Tribunal.—(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

49. Composition of Cyber Appellate Tribunal.—A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Presiding Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government.

50. Qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal.—A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he—

(a) is, or has been, or is qualified to be, a Judge of a High Court, or—

(b) is, or has been, a member of the Indian Legal Service and is holding a post in Grade I of that Service for at least three years.

51. Term of office.—The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.

52. Salary, allowances and other terms and conditions of service of Presiding Officer.—The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Presiding Officers shall be varied to his disadvantage after appointment.
53. Filling up of vacancies.—If, for reason other than temporary absence, any vacancy occurs in the office of the Presiding Officer of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

54. Resignation and removal.—(1) The Presiding Officer of a Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

Provided that the said Presiding Officer shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Presiding Officer concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehaviour or incapacity of the aforesaid Presiding Officer.

55. Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings.—No order of the Central Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

56. Staff of the Cyber Appellate Tribunal.—(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as that Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries, allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

57. Appeal to Cyber Appellate Tribunal.—(1) Save as provided in sub-section (2), any person aggrieved by an order made by Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter.

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

Provided that the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

58. Procedure and powers of the Cyber Appellate Tribunal.—(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a Civil Court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:

(a) summoning and enforcing the attendance of any person and examining him on oath;
(b) requiring the discovery and production of documents or other electronic records;
(c) receiving evidence on affidavits;
(d) issuing commissions for the examination of witnesses or documents;
(e) reviewing its decisions;
(f) dismissing an application for default or deciding it ex parte;
(g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code (45 of 1860) and for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

59. Right to legal representation.—The appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

60. Limitation.—The provisions of the Limitation Act, 1963 (36 of 1963), shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.
61. Civil Court not to have jurisdiction.—No Court shall have jurisdiction to entertain any suit or proceeding in respect of any matter in which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any Court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

62. Appeal to High Court.—Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

63. Compounding of contraventions.—(1) Any contravention under this Act may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorised by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

Provided that such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation.—For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

64. Recovery of penalty.—A penalty imposed under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the licence or the Digital Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

CHAPTER XI
OFFENCES

65. Tampering with computer source documents.—Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.


70. Protected system.—(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

Explanation.—For the purposes of this section, “computer source code” means the listing of programs, computer commands, design and layout and programme analysis of computer resource in any form.

66. Hacking with computer system.—(1) Whenever with the intent to cause or to know that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

67. Publishing of information which is obscene in electronic form.—Whoever publishes or transmits or causes to be published in the electronic form any material which is lascivious or appeals to the prurient interest or its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

68. Power of Controller to give directions.—(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or regulations made thereunder.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to fine not exceeding two lakh rupees or both.

69. Directions of Controller to a subscriber to extend facilities to decrypt information.—(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to five years.
(2) The appropriate Government may, by order in writing, authorise the person who are authorised to access protected systems notified under subsection (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

71. Penalty for misrepresentation.—Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72. Penalty for breach of confidentiality and privacy.—Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

73. Penalty for publishing Digital Signature Certificate false in certain particulars.—(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—
   (a) the Certifying Authority listed in the certificate has not issued it; or
   (b) the subscriber listed in the certificate has not accepted it; or
   (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

74. Publication for fraudulent purpose.—Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

75. Act to apply for offence or contravention committed outside India.—(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

76. Confiscation.—Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation.

Provided that where it is established to the satisfaction of the Court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the Court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

77. Penalties or confiscation not to interfere with other punishments.—No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

78. Power to investigate offences.—Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

CHAPTER XII

NETWORK SERVICE PROVIDERS NOT TO BE LIABLE IN CERTAIN CASES

79. Network service providers not to be liable in certain cases.—For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.—For the purposes of this section—
(a) “network service provider” means an intermediary;
(b) “third party information” means any information dealt with by a network service provider in his capacity as an intermediary.

CHAPTER XIII

MISCELLANEOUS

80. Power of police officer and other officers to enter, search, etc.—(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of being about to commit any offence under this Act.

Explanation.—For the purposes of this sub-section, the expression “public place” includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.
(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974), shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

81. Act to have overriding effect.—The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

[81-A. Application of the Act to electronic cheque and truncated cheque.—(1) The provisions of this Act, for the time being in force, shall apply to, or in relation to, electronic cheques and the truncated cheques subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.

(2) Every notification made by the Central Government under sub-section (1) shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or both Houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or innullment shall be without prejudice to the validity of anything previously done under that notification.

Explanation.—For the purposes of this section, the expressions “electronic cheque” and “truncated cheque” shall have the same meaning as assigned to them in section 2 of the Negotiable Instruments Act, 1881 (26 of 1881).

82. Controller, Deputy Controller and Assistant Controllers to be public servants.—The President may constitute and other officers and employees of a Cyber Appellate Tribunal, the Controller, the Deputy Controller and the Assistant Controllers shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code (45 of 1860).

83. Power to give directions.—The Central Government may give directions to any State Government as to the carrying into execution in the State of any of the provisions of this Act or of any rule, regulation or order made thereunder.

84. Protection of action taken in good faith.—No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Presiding Officer, adjudicating officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or of any rule, regulation or order made thereunder.

85. Offences by companies.—(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.—For the purposes of this section,—

(i) “company” means any body corporate and includes a firm or other association of individuals; and

(ii) “director”, in relation to a firm, means a partner in the firm.

86. Removal of difficulties.—(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

Provided that no order shall be made under this section after the expiry of a period of two years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.


(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:

(a) the manner in which any information or matter may be authenticated by means of digital signature under section 5;

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 6;

(c) the manner and format in which electronic records shall be filed, or issued and the method of payment under sub-section (2) of section 6;

(d) the matters relating to the type of digital signature, manner and format in which it may be affixed under section 10;
(e) the security procedure for the purpose of creating secure electronic record and secure digital signature under section 16;
(f) the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers under section 17;
(g) other standards to be observed by the Controller under clause (h) of sub-section (2) of section 20;
(h) the requirements which an applicant must fulfill under sub-section (2) of section 21;
(i) the period of validity of licence granted under clause (a) of sub-section (1) of section 22;
(j) the form in which an application for licence may be made under sub-section (1) of section 22;
(k) the amount of fees payable under clause (c) of sub-section (2) of section 22;
(l) such other documents which shall accompany an application for licence under clause (d) of sub-section (2) of section 22;
(m) the form and the fee for renewal of a licence and the fee payable thereof under section 23;
(n) the form in which application for issue of a Digital Signature Certificate may be made under sub-section (1) of section 35;
(o) the fee to be paid to the Certifying Authority for issue of a Digital Signature Certificate under sub-section (2) of section 35;
(p) the manner in which the adjudicating officer shall hold inquiry under sub-section (1) of section 46;
(q) the qualifications and experience which the adjudicating officer shall possess under sub-section (3) of section 46;
(r) the salary, allowances and the other terms and conditions of service of the Presiding Officer under section 52;
(s) the procedure for investigation of misbehaviour or incapacity of the Presiding Officer under sub-section (3) of section 54;
(t) the salary and allowances and other conditions of service of other officers and employees under sub-section (3) of section 56;
(u) the form in which appeal may be filed and the fee thereof under sub-section (3) of section 57;
(v) any other power of a civil Court required to be prescribed under clause (g) of sub-section (2) of section 58; and
(w) any other matter which is required to be, or may be, prescribed.

(3) Every notification made by the Central Government under clause (f) of sub-section (4) of section 1 and every rule made by it shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session or the immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the notification or the rule or both Houses agree that the notification or the rule should not be made, the notification or the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that notification or rule.

88. Constitution of Advisory Committee.—(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests principally affected or having special knowledge of the subject matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise—

(a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;

(b) the Controller in framing the regulations under this Act.

(4) There shall be paid to the non-official members of such Committee such travelling and other allowances as the Central Government may fix.

89. Power of Controller to make regulations.—(1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:

(a) the particulars relating to maintenance of database containing the disclosure record of every Certifying Authority under clause (n) of section 18;

(b) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (1) of section 18;

(c) the terms and conditions subject to which a licence may be granted under clause (c) of sub-section (3) of section 21;

(d) other standards to be observed by a Certifying Authority under clause (d) of section 30;

(e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;

(f) the particulars of statement which shall accompany an application under sub-section (3) of section 35;

(g) the manner in which the subscriber shall communicate the compromise of private key to the Certifying Authority under sub-section (2) of section 35;

(h) any other matter which is required to be, or may be, prescribed.

3) Every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session or the immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect only
in such modified form or be of no effect, as the case may be; so, however, any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

90. Power of State Government to make rules.—(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:

(a) the electronic form in which filing issue, grant, receipt or payment shall be effected under sub-section (1) of section 6;

(b) for matters specified in sub-section (2) of section 6;

(c) any other matter which is required to be provided by rules by the State Government.

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

91. Amendment of Act 45 of 1860.—The Indian Penal Code shall be amended in the manner specified in the First Schedule to this Act.

92. Amendment of Act 1 of 1872.—The Indian Evidence Act, 1872 shall be amended in the manner specified in the Second Schedule to this Act.

93. Amendment of Act 18 of 1891.—The Bankers' Books Evidence Act, 1891 shall be amended in the manner specified in the Third Schedule to this Act.

94. Amendment of Act 2 of 1934.—The Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule to this Act.

THE FIRST SCHEDULE

(See section 91)

AMENDMENTS TO THE INDIAN PENAL CODE

1. After section 29, the following section shall be inserted, namely—

29-A. Electronic record.—The words "electronic record" shall have the meaning assigned to them in clause (i) of sub-section (1) of section 2 of the Information Technology Act, 2000.

2. In section 167, for the words "such public servant, charged with the preparation of translation of any document, frames or translates that document", the words "such public servant, charged with the preparation or translation of any document or electronic record, frames or translates that document or electronic record" shall be substituted.

3. In section 172, for the words "produce a document in a Court of Justice", the words "produce a document or an electronic record in a Court of Justice" shall be substituted.

4. In section 173, for the words "to produce a document in a Court of Justice", the words "to produce a document or an electronic record in a Court of Justice" shall be substituted.

5. In section 175, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

6. In section 192, for the words "makes any false entry in any book or record, or makes any document containing a false statement", the words "makes any false entry in any book, or record, or electronic record or makes any document or electronic record containing a false statement" shall be substituted.

In section 204, for the word "document" at both the places where it occurs, the words "document or electronic record" shall be substituted.

In section 463, for the words "whoever makes any false documents or part of a document with intent to cause damage or injury", the words "whoever makes any false documents or electronic record or part of a document or electronic record, with intent to cause damage or injury" shall be substituted.

9. In section 466,—

(a) for the portion beginning with the words "A person is said to make a false document" and ending with the words "by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration", the following shall be substituted, namely:

"A person is said to make a false document or false electronic record—"

First.—Who dishonestly or fraudulently—

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any digital signature on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the digital signature,

with the intention of causing it to be believed that such document or part of document, or electronic record or digital signature was made, signed, sealed, executed, transmitted or altered by or by the authority of a person whom or by whose authority he knows that it was not made, signed, sealed, executed or altered; or

Secondly,—Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration;

Thirdly,—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration;

(b) after Explanation 2, the following Explanation shall be inserted at the end, namely:

"Explanation 3.—For the purposes of this section, the expression 'affixing digital signature' shall have the meaning assigned to it in clause (d) of sub-section (1) of section 2 of the Information Technology Act, 2000'.

10. In section 466,—

(a) for the words "Whoever forges a document or an electronic record", the words "Whoever forges a document or electronic record" shall be substituted;

(b) the following Explanation shall be inserted at the end, namely:

"Explanation,—For the purposes of this section, 'register' includes any at, data or record or any entries maintained in the electronic forms, defined in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000'.

1. In section 468, for the words "document forged", the words "document or electronic record forged" shall be substituted.

12. In section 469, for the words "intending that the document forged", the words "intending that the document or electronic record forged" shall be substituted.

13. In section 470, for the word "document" in both the places where it occurs, the words "document or electronic record" shall be substituted.
14. In section 471, for the word "document" wherever it occurs, the words "document or electronic record" shall be substituted.

15. In section 474, for the portion beginning with the words "Whoever has in his possession any document" and ending with the words "if the document is one of the description mentioned in section 466 of this Code", the following shall be substituted, namely:

"Whoever has in his possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as a genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code."

16. In section 476, for the words "any document", the words "any document or electronic record" shall be substituted.

17. In section 477-A, for the words "book, paper, writing" at both the places where they occur, the words "book, electronic record, paper, writing" shall be substituted.

THE SECOND SCHEDULE

(See section 92)

AMENDMENTS TO THE INDIAN EVIDENCE ACT, 1872

(1 OF 1872)

1. In section 3,-

(a) in the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the words "all documents including electronic records produced for the inspection of the Court" shall be substituted;

(b) after the definition of "India", the following shall be inserted, namely:

"the expressions "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" shall have the meanings respectively assigned to them in the Information Technology Act, 2000."

2. In section 17, for the words "oral or documentary", the words "oral or documentary or contained in electronic form" shall be substituted.

3. After section 22, the following section shall be inserted, namely:

"22-A. When oral admission as to contents of electronic records are relevant.—Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question."

4. In section 34, for the words "Entries in the books of account", the words "Entries in the books of account, including those maintained in an electronic form" shall be substituted.

5. In section 35, for the word "record", in both the places where it occurs, the words "record or an electronic record" shall be substituted.

6. For section 39, the following section shall be substituted, namely:

"39. What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.—When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made.

7. After section 47, the following section shall be inserted, namely:

"47-A. Opinion as to digital signature when relevant.—When the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact."

8. In section 59, for the words "contents of documents", the words "contents of documents or electronic records" shall be substituted.

9. After section 65, the following sections shall be inserted, namely—

"65-A. Special provisions as to evidence relating to electronic record.—The contents of electronic records may be proved in accordance with the provisions of section 65-B.

65-B. Admissibility of electronic records.—(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or is out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or derived from such information fed into the computer in the ordinary course of the said activities.

(3) 'Wherever over any period, the function of storing or processing information for the purposes or any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say—

(e) identifying the electronic record containing the statement and describing the manner in which it was produced;

(f) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(g) dealing with any of the matters to which the conditions mentioned in subsection (2) relate.

and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities.
(whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section—

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived thereto by calculation, comparison or any other process.

10. After section 7, the following section shall be inserted, namely:

"76-A. Proof as to digital signature.—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 the fact that such digital signature is the digital signature of the subscriber must be proved."

11. After section 73, the following section shall be inserted, namely:

"73-A. Proof as to verification of digital signature.—In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct—

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) in any other case to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

Explanation.—For the purposes of this section, "Controller" means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000."

12. After section 81, the following section shall be inserted, namely:

"81-A. Presumption as to Gazettes in electronic form.—The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.

Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived thereto by calculation, comparison or any other process.

13. After section 85, the following section shall be inserted, namely:

"85-A. Presumption as to electronic agreements.—The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signatures of the parties.

85-B. Presumption as to electronic records and digital signatures.—(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved that—

(a) the secure electronic record is signed by or on behalf of the subscriber with the intention of authenticating the electronic record;

(b) the secure electronic record is not altered after the point of time as to which the secure status relates.

(2) In any proceedings involving secure digital signature, the Court shall presume unless the contrary is proved that—

(a) the secure digital signature is affixed by or on behalf of the subscriber with the intention of authenticating the electronic record;

(b) the secure digital signature is not altered after the point of time as to which the secure status relates.

14. After section 88, the following section shall be inserted, namely:

"88-A. Presumption as to electronic messages.—The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as sent into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation.—For the purposes of this section, the expressions "addressee" and "originator" shall have the same meanings respectively assigned to them in clauses (b) and (ca) of sub-section (1) of section 2 of the Information Technology Act, 2000."

15. After section 90, the following section shall be inserted, namely:

"90-A. Presumption as to electronic records five years old.—Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explanation.—Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.

This Explanation applies also to section 81-A."

16. For section 131, the following section shall be substituted, namely:

"131. Production of documents or electronic records which another person, having possession, could refuse to produce.—No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production.

THE THIRD SCHEDULE

(See section 93)

AMENDMENTS TO THE BANKERS' BOOKS EVIDENCE ACT, 1891

(18 OF 1891)

1. In section 2,—

(b) except in the case of a secure electronic record, a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

85-C. Presumption as to Digital Signature Certificates.—The Court shall presume, unless the contrary is proved, that the information listed in a Digital Signature Certificate is correct except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

12. After section 81, the following section shall be inserted, namely:

"81-A. Presumption as to Gazettes in electronic form.—The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody.

Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived thereto by calculation, comparison or any other process.

13. After section 85, the following section shall be inserted, namely:

"85-A. Presumption as to electronic agreements.—The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signatures of the parties.

85-B. Presumption as to electronic records and digital signatures.—(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved that—

(a) the secure electronic record is signed by or on behalf of the subscriber with the intention of authenticating the electronic record;

(b) the secure electronic record is not altered after the point of time as to which the secure status relates.

(2) In any proceedings involving secure digital signature, the Court shall presume unless the contrary is proved that—

(a) the secure digital signature is affixed by or on behalf of the subscriber with the intention of authenticating the electronic record;

(b) the secure digital signature is not altered after the point of time as to which the secure status relates.
the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and

(b) consist of printouts a data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2-A.

2. After section 2, the following section shall be inserted, namely:

"2-A. Conditions in the printout.—A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely:

(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and

(b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of—

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

(B) the safeguards adopted to prevent and detect unauthorised change of data;

(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;

(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;

(F) the mode of identification of such data storage devices;

(G) the arrangements for the storage and custody of such storage devices;

(H) the safeguards to prevent and detect any tampering with the system; and

(I) any other factor which will vouch for the integrity and accuracy of the system.

(c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data."

THE FOURTH SCHEDULE

(See section 94)

AMENDMENT TO THE RESERVE BANK OF INDIA ACT, 1934

(2 OF 1934)

In the Reserve Bank of India Act, 1934, in section 58, in sub-section (2), after clause (p), the following clause shall be inserted, namely:

"(p) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (c) of section 45-1, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers;"
The Internet Governance Project (IGP) is an interdisciplinary consortium of academics with scholarly and practical expertise in international governance, Internet policy, and information and communication technology. The Project is conducting research on and publishing analysis of Internet governance. Some of the work is intended to contribute to the World Summit on the Information Society (WSIS), and the United Nations Working Group on Internet Governance as well as related debates at the international, regional and national levels.

IGP Partners: Statement Opposing Political Intervention in the Internet's Core Technical Administrative Functions. (August 29, 2005)


Mathiason and Mueller: Internet Governance Quo Vadis? A Response to the WGIG Report (July 2005)


IGP Issues Statement Opposing Political Intervention in the Internet's Core Technical Functions

August 25, 2005. Concerned about the long-term implications of the Commerce Department's intervention in ICANN's policy making process, which was prompted by censorship advocates targeting the .xxx domain, the Internet Governance Project has issued a statement and a call for public support of its position. The statement, which was covered in the Washington Internet Daily, charges that the NTIA intervention "undermines assurances from the U.S. and from ICANN that it would never be used to shape policy but was only a means of protecting the stability of the organization and its processes." The statement notes that the concern is particularly strong in this case because "because of the open acknowledgement in the NTIA's letter of the influence of an organized campaign by domestic religious groups devoted to content regulation of the Internet." View and Sign on to the Statement here

US Government Vetoes ICANN Decision

August 15, 2005. The US Commerce Department, responding to censorship calls by domestic political groups, intervened unilaterally in ICANN's top level domain process to delay delegation of the .xxx domain. A letter from Commerce Department's Michael Gallagher, Assistant Secretary for Communications and Information, told ICANN to Commerce Department's Michael Gallagher, Assistant Secretary for Communications and Information, told ICANN to...
Introduction

Origin of the Working Group on Internet Governance

The first phase of World Summit on the Information Society (WSIS) agreed to pursue the dialogue on Internet Governance in the Declaration of Principles and Action Plan adopted on 12 December 2003, with a view to preparing the ground for a decision at the second phase of the WSIS in Tunis in November 2005. In this regard, the first phase of the Summit requested the United Nations Secretary-General to establish a Working Group on Internet Governance (WGIG). The WGIG has been asked to present the result of its work in a report "for consideration and appropriate action for the second phase of the WSIS in Tunis 2005." More information on the mandate of the WGIG.

Funding

The Secretariat’s activities are funded through extra-budgetary contributions paid into a Trust Fund.

The WGIG Report

The WGIG Report is available in all UN languages:

<table>
<thead>
<tr>
<th>WGIG Final Report*</th>
<th>[Arabic] [Chinese] [English] [French] [Russian] [Spanish]</th>
</tr>
</thead>
</table>

* The Arabic and Spanish versions are revised versions made on 21 July 2005 and 4 August 2005, respectively. Please also note that documents in non-ASCII characters take a while to download.

[New!] Click here to view a compilation of the comments received on the WGIG Report.

Further comments have reached the WGIG Secretariat:

- WSIS Civil Society Privacy and Security Working Group
- UNESCO Information For All Programme National Committee of Russia
- The Internet Mark 2 Project (click here to view a letter addressed by Mr Ian Peter, Project Manager, to WGIG Executive Coordinator)
- Letter from Mr Alexander Dix, Chairman of the International Working Group on Data Protection in Telecoms to WGIG Chairman
- Letter from Mr James Wimberley to the Executive Coordinator of WGIG

You may view an open format version of the Report (OpenOffice version 1.9 or higher is needed to view
1. Internet Society (ISOC) is an international organization for global cooperation and coordination for the Internet and its networking technologies and applications. Category: Internet Organizations > Internet Society

2. Internet Society (ISOC) includes a directory of pages offering Internet history. Category: Internet History > Web Directories

3. Internet Society (ISOC) All About The Internet: History of the Internet

A Brief History of the Internet. Introduction. The Internet has revolutionized the computer and communications world like nothing before. ... This document <http://www.isoc.org/internet/history/brief.shtml ... All Rights Reserved. Webmaster@ISOC.ORG. Privacy Statement ...

4. All About The Internet: Standards

... This document <http://www.isoc.org/internet/standards/papers/amr-on-standards.shtml ... All Rights Reserved. Webmaster@ISOC.ORG. Privacy Statement ...

5. The Internet Report is a catalogue of Internet Engineering Task Force (IETF) documents, including RFCs and Internet Drafts, that document the technology, protocols and operating procedures that form the Internet. ietfreport.isoc.org - 17k - Cached - More from this site - Save - Block

6. Internet Society (ISOC) All About The Internet; Legal Guide

The Internet Society's Online Guide to Internet Law is a comprehensive and up-to-date reference source which includes sections on legal research, legal news, litigation, legislation, treaties, international trade and investment, glossaries, ...

7. Internet Society (ISOC) All About ISOC: Jon Postel

... isoc.org/postel/index.shtml> was last updated Monday, 18-Oct-2004 13:25:20 EDT. Copyright © 2005 Internet Society. All Rights Reserved. Webmaster@ISOC.ORG ...

8. All About ISOC: Conferences - INET2000

INTERNATIONAL SUMMIT. Global Distributed Intelligence for Everyone. The 10th Annual Internet Society Conference. 18-21 July 2000

9. INET focusing on the Internet economy, new technical developments, social impact, educational environments, and more. Category: Internet Organizations > Internet Society


Project India Cracked Statistics

About || The News || The List || The Links || Mailing Lists || Interviews || Statistics || Media Coverage || FAQ/FGA || Older News || Disclaimer

Overall stats

- Total number of defacements recorded - 780
- Earliest Mirror - 2000-02-05 (yyyy/mm/dd)
- Latest Mirror - 2002-12-07 (yyyy/mm/dd)
- No. of distinct defacers - 150

Breakdown in terms of domain

- co.in - 115 defacements - 14.74%
- gov.in - 29 defacements - 3.72%
- net.in - 23 defacements - 2.95%
- org.in - 15 defacements - 1.92%
- nic.in - 45 defacements - 5.77%
- ac.in - 33 defacements - 4.23%
-ernet.in - 56 defacements - 7.18%
- res.in - 20 defacements - 2.56%
- .com - 398 defacements - 51.03%
- .net - 18 defacements - 2.31%
- .org - 25 defacements - 3.21%
- .edu - 2 defacements - 0.26%

Top 5 attackers:

- AIC - 166 defacements - 21.28%
- GForce Pakistan - 116 defacements - 14.87%
- Silver Lords - 101 defacements - 12.95%
- WFD - 59 defacements - 7.56%
- ISOTK - 17 defacements - 2.18%

Graphical statistics of defacements are as shown below.

Year 2002 - Last update 3 Mar 2003 10:22 GMT

http://www.srijith.net/indiacracked/stats/index.shtml
In keeping with the demands of the times, the Cyber Crime Investigation Cell (CCIC) of the CBI, notified in September 1999, started functioning w.e.f. 3.3.2000. The Cell is headed by a Superintendent of Police. The jurisdiction of this Cell is all India, and besides the offences punishable under Chapter XI, IT Act, 2000, it also has power to look into other high-tech crimes.

cyber crime police departments

<table>
<thead>
<tr>
<th>Location</th>
<th>Officer In Charge</th>
<th>Address</th>
<th>Telephone No</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chennai</td>
<td>Sri S. Balu</td>
<td>Assistant Commissioner of Police Cyber Crime Cell Commissioner office Campus Egmore, Chennai 600008</td>
<td>55498211 Mobile: 98410-13541 Res: 25500503</td>
<td><a href="mailto:cyberac@rediffmail.com">cyberac@rediffmail.com</a> <a href="mailto:baluac@vsnl.net">baluac@vsnl.net</a></td>
</tr>
<tr>
<td>Chennai</td>
<td>Cyber Crime Cell</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Contact Person</td>
<td>Phone Numbers</td>
<td>Email Address</td>
<td>Website</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------</td>
<td>----------------------------------------</td>
<td>--------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>for Rest of Tamil Nadu</td>
<td>Smt Venmati</td>
<td>CB, CID Chennai 98414-22844</td>
<td><a href="mailto:venmathi_vip@yahoo.co.in">venmathi_vip@yahoo.co.in</a></td>
<td></td>
</tr>
<tr>
<td>Bangalore for the Whole of Karnataka</td>
<td>Cyber Crime, Police Station C.O.D Headquarters, Carlton House, # 1, Palace Road, Bangalore - 560 001</td>
<td>22201026 22943050 238&quot; 11 (FAX)</td>
<td><a href="mailto:ccps@kar.nic.in">ccps@kar.nic.in</a></td>
<td><a href="http://www.cyberpolicebangalore.nic.in">http://www.cyberpolicebangalore.nic.in</a></td>
</tr>
<tr>
<td>Hyderabad</td>
<td>Crime Investigation Department D.G.P. Office, Lakdikapool, 11, Hyderabad-500004</td>
<td>22240663 27852274 23297474 (Fax)</td>
<td><a href="mailto:cidap@cidap.gov.in">cidap@cidap.gov.in</a></td>
<td><a href="mailto:info@cidap.gov.in">info@cidap.gov.in</a></td>
</tr>
</tbody>
</table>

http://www.indianchild.com/cybercrimeinindia.htm
Address of CBI Cyber Crime Cell

Supdt. of Police, Cyber Crime Investigation Cell Central Bureau of Investigation, 5th Floor, Block No.3, CGO Complex, Lodhi Road, New Delhi -3, Phone: 4362203, 4392424 : EMail: cbiccc@bol.net.in : Web: http://cbi.nic.in/

Contact Address of Yahoo Mail and Hotmail Representative offices in India having responsibility as service providers for any Cyber Crime committed in India under ITA-2000 or other Laws.

Address of Yahoo India office:

Yahoo Web Services India Private Limited, 386 Veer Savarkar Marg, Opposite Siddhivinayak temple, Mumbai 400 025, 22 56622222, 22 56622244.e-mail: ad-sales-india@yahoo-inc.com

Address of MSN India Office:

MSN India, Prestige Takt, 23 Kasturba Gandhi Cross, Bangalore - 560 001, eMail: msnadind@microsoft.com, Tel: 91-80-2121-12

http://www.indianchild.com/cybercrime.in/india.htm

Recommended useful sites:

http://www.cybercellmumbai.com/ - This is the official website of the cyber crime cell of Mumbai police, India. Useful net safety tips, latest cyber crime news and how to lodge complain. Must visit site.

http://www.naavi.org - A very useful & informative site on cyber crime India information. Another Must visit site!
QUESTIONNAIRE
ON
OFFENCES IN CYBER-SPACE

TO WHOM IT MAY CONCERN

AN APPEAL

This is an appeal to all persons concerned with the subject to provide some material information, suggestion, and opinion as to the cyber-offences in India for the purposes of purely academic research work.

India, in this 21st century, is rapidly entering the cyber-age involving electronic computer and the Internet.

The social activities in various sectors such as commerce, banking, administration, research, education,
industry, transport, power supply, Communication, resource management, information management, scientific projects, national security and defense etc. are increasingly taking the help of electronic Computers, computer systems and computer networks and the Internet.

And along with this, the problem of safety and security in Cyber-space activities is also increasing and this has already become a serious concern of the society.

The Information Technology Act-2000 attempts to control the cyber crimes i.e. Tampering with computer source documents (s/65) Hacking with Computer system,(s/66), publishing obscene materials in electronic form (s/67) and also some other offences (u/s.43) such as unauthorised access, downloading data without permission, introducing virus and worms in to any computer, computer-system or computer networks, causing any damage or disruption to any computer system or networks, blocking access to authorised persons, assisting illegal access, diverting service charge to innocent user by tampering with or manipulating Computer system & network.

Contd..P/3.
In addition to new crimes like hacking, tampering, virus attack, Denial of Service, spamming etc., some traditional crimes like extortion, theft, gambling, fraud, pornography, pirated software etc., are also committed involving cyber space i.e., Internet. So the present police system and court procedures are very much helpful to deal with cyber offences as a whole.
QUERIES

1. Please give names & Types of Cy-crimes—
   a) known to you —
   b) Actually committed in India
   c) Personal knowledge/experience if any

2. Any Preventive Measure — (Technical)
   a) Known to you —
   b) Usually taken —
   c) Actually taken —

3. Any Other Security Measure — (Physical Control —
   appointment of super-user/system-administrator —network
   administrator
   a) Known to you —
   b) Usually taken
   c) Actually taken —

4. Police (Legal) assistance — (after detection)
   a) Expected and reasonable help
   b) Personal knowledge —
   c) Comment —
5. Cyber-Prosecution - if any (India)
   a) Known to you -
   b) Personal Knowledge -
   c) Comment.

6. Any other cyber crime (other than IT Act)
   (Carding-Piracy-IP Crime-gambling -Extertion-Theft fraud)
   a) Known to you
   b) Personal knowledge
   c) Comment

7. Problems on Investigation & Prosecution
   a) Detection
   b) Identification
   c) Search & Seizure
   d) Evidence Collection
      Preservation & production.

8. Security incident reporting-
   a) Any system of reporting (existing) - Known -
   b) Known incident reporting & response -
   c) Suggestion -
9. Emergency response -
   a) Any system available
   b) Known incident and response -
   c) Suggestion -

10. ISP - Liability at present
   a) in commission of offense
   b) to assist the investigation
   c) Any suggestion as to control ISP-involvement -

Name - __________________________________________

Designation - ______________________________________

Address - _______________________________________

Contact No. - ____________________________________

Date - ______________
UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT, 1996 WITH ADDITIONAL ARTICLE 5 BIS AS ADOPTED IN 1998

UNITED NATIONS

CONTENTS

GENERAL ASSEMBLY RESOLUTION 51/162 OF 16 DECEMBER 1996

UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE

Part one. Electronic commerce in general

Chapter I. General provisions

Article 1. Sphere of application
Article 2. Definitions

15. In November 1997, the OECD and the Government of Finland in cooperation with the European Commission, the Government of Japan and the Business and Industry Advisory Committee to the OECD organised a conference Dismantling the Barriers to Global Electronic Commerce in Turku, Finland. This brought together representatives of government and business to identify major policy problems, to take stock of the initiatives currently underway and to develop a consensus between business and government as to some of the guiding principles that will constitute a framework for electronic commerce policies.

Article 3. Interpretation
Article 4. Variation by agreement

Chapter II. Application of legal requirements to data messages

Article 5. Legal recognition of data messages
Article 5 bis. Incorporation by reference
Article 6. Writing
Article 7. Signature
Article 8. Original
Article 9. Admissibility and evidential weight of data messages
Article 10. Retention of data messages

Chapter III. Communication of data messages

Article 11. Formation and validity of contracts
Article 12. Recognition by parties of data messages
Article 13. Attribution of data messages
Article 14. Acknowledgement of receipt
Article 15. Time and place of dispatch and receipt of data messages

Part two. Electronic commerce in specific areas

Chapter I. Carriage of goods

Article 16. Actions related to contracts of carriage of goods
Article 17. Transport documents

Paragraphs

GUIDE TO ENACTMENT OF THE UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE

Purpose of this Guide

Introduction to the Model Law
A. Objectives
B. Scope
C. Structure
D. A "framework" law to be supplemented by technical regulations
E. The "functional-equivalent" approach
F. Default rules and mandatory law
G. Assistance from UNCITRAL secretariat

II. Article-by-article remarks

Part one. Electronic commerce in general

Chapter I. General provisions

Article 1. Sphere of application
Article 2. Definitions
Article 3. Interpretation
Article 4. Variation by agreement

Chapter II. Application of legal requirements to data messages

Article 5. Legal recognition of data messages

Article 5 bis. Incorporation by reference

Article 6. Writing

Article 7. Signature

Article 8. Original

Article 9. Admissibility and evidential weight of data messages

Article 10. Retention of data messages

Chapter III. Communication of data messages

Article 11. Formation and validity of contracts

Article 12. Recognition by parties of data messages

Article 13. Attribution of data messages

Article 14. Acknowledgement of receipt

Article 15. Time and place of dispatch and receipt of data messages

Part two. Electronic commerce in specific areas

Chapter I. Carriage of goods

Article 16. Actions related to contracts of carriage of goods

Article 17. Transport documents

III. History and background of the Model Law

RESOLUTION ADOPTED BY THE GENERAL ASSEMBLY

[on the report of the Sixth Committee (A/51/628)]


The General Assembly,

Recalling its resolution 2205 (XXI) of 17 December 1966, by which it created the United Nations Commission on International Trade Law, with a mandate to further the progressive harmonization and unification of the law of international trade and in that respect to bear in mind the interests of all peoples, in particular those of developing countries, in the extensive development of international trade,

Noting that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information,

Recalling the recommendation on the legal value of computer records adopted by the Commission at its eighteenth session, in 1983, paragraph 5(a) of General Assembly resolution 40/71 of 11 December 1983, in which the Assembly called upon Governments and international organizations to take action, where appropriate, in conformity with the recommendation of the Commission (1), so as to ensure legal

UNCITRAL Model Law on Electronic Commerce

security in the context of the widest possible use of automated data processing in international trade,

Convinced that the establishment of a model law facilitating the use of electronic commerce that is acceptable to States with different legal, social and economic systems, could contribute significantly to the development of harmonious international economic relations,

Noting that the Model Law on Electronic Commerce was adopted by the Commission at its twenty-ninth session after consideration of the observations of Governments and interested organizations,

Believing that the adoption of the Model Law on Electronic Commerce by the Commission will assist all States significantly in enhancing their legislation governing the use of alternatives to paper-based methods of communication and storage of information and in formulating such legislation where none currently exists,

1. Expresses its appreciation to the United Nations Commission on International Trade Law for completing and adopting the Model Law on Electronic Commerce contained in the annex to the present resolution and for preparing the Guide to Enactment of the Model Law;

2. Recommends that all States give favourable consideration to the Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

3. Recommends also that all efforts be made to ensure that the Model Law, together with the Guide, become generally known and available.

85th plenary meeting 16 December 1996

UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE

[Original: Arabic, Chinese, English, French, Russian, Spanish]

Part one. Electronic commerce in general

CHAPTER I. GENERAL PROVISIONS

Article 1. Sphere of application

This Law applies to any kind of information in the form of a data message used in the context*** of commercial**** activities.

* The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages:

** This Law applies to any kind of information in the form of a data message where the data message relates to international commerce.

*** This Law does not override any rule of law intended for the protection of consumers.

**** The Commission suggests the following text for States that might wish to extend the applicability of this Law: “This Law applies to any kind of information in the form of a data message, except in the following situations: [...].”

***** The term “commercial” should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurances; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.
Article 2. Definitions

For the purposes of this Law:

(a) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telexcopy;
(b) "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information;
(c) "Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;
(d) "Addressee" of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;
(e) "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;
(f) "Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

Article 3. Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 4. Variation by agreement

(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of this Law may be varied by agreement.

(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in Chapter II.

CHAPTER II. APPLICATION OF LEGAL REQUIREMENTS TO DATA MESSAGES

Article 5. Legal recognition of data messages

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Article 5 bis. Incorporation by reference

(as adopted by the Commission at its thirty-first session, in June 1998)

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

Application of Legal Requirements, etc.

Article 6. Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) The provisions of this article do not apply to the following: [....]

Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following: [....]

Article 8. Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph (a) of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(4) The provisions of this article do not apply to the following: [.....]

Article 9. Admissibility and evidential weight of data messages

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,
(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Evidence in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

**Article 10. Relation of data messages**

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b) and (c) of paragraph (1) are met.

**CHAPTER III. COMMUNICATION OF DATA MESSAGES**

**Article 11. Formation and validity of contracts**

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages.

Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provisions of this article do not apply to the following: [...].

**Article 12. Recognition by parties of data messages**

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

(2) The provisions of this article do not apply to the following: [...].

**Article 13. Attestation of data messages**

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

**Article 14. Acknowledgement of receipt**

(1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by
the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements were met.

(7) Except as far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

Article 15. Time and place of dispatch and receipt of data messages

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time the data message enters the designated information system; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time the data message is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

(5) The provisions of this article do not apply to the following: [...]
GUIDE TO ENACTMENT OF THE UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE (1996)

Purpose of this guide

1. In preparing and adopting the UNCITRAL Model Law on Electronic Commerce (hereinafter referred to as "the Model Law"); the United Nations Commission on International Trade Law (UNCITRAL) was mindful that the Model Law would be a more effective tool for States modernizing their legislation if background and explanatory information would be provided to executive branches of Governments and legislators to assist them in using the Model Law. The Commission was also aware that the likelihood that the Model Law would be used in a number of States with limited familiarity with the type of communication techniques considered in the Model Law. This Guide, much of which is drawn from the travaux préparatoires of the model law, is also intended to be helpful to users of electronic means of communication as well as to scholars in that in the preparation of the Model Law, it was assumed that the draft Model Law would be accompanied by such a guide. For example, it was decided in respect of a number of issues not to set them in the draft Model Law but to address them in the Guide so as to provide guidance to States enacting the draft Model Law. The information presented in this Guide is intended to explain why the provisions in the Model Law have been included as essential basic natures of a statutory device designed to achieve the objectives of the Model Law. Such information might assist States also in considering which, if any, of the provisions of the Model Law might have to be varied to take into account particular national circumstances.

I. INTRODUCTION TO THE MODEL LAW

Objectives

2. The use of modern means of communication such as electronic mail and electronic data interchange (EDI) for the conduct of international trade transactions has been increasing rapidly and is expected to develop further as technical supports such information highways and the INTERNET become more widely accessible. However, the communication of legally significant information in the form of paperless messages may be hindered by legal obstacles to the use of such messages, or by uncertainty as to their legal effect or validity. The purpose of the Model Law is to offer international solutions to the set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created for what has become known as "electronic commerce." The principles expressed in the Model Law are also intended to be of use to individual users of electronic commerce in the drafting of some of the contractual solutions that might be needed to overcome the legal obstacles to the increased use of electronic commerce.

3. The decision by UNCITRAL to formulate model legislation on electronic commerce was taken in response to the fact that in a number of countries the existing legislation governing communication and storage of information is inadequate or outdated because it does not contemplate the use of electronic commerce. In certain cases, existing legislation imposes or implies restrictions on the use of modern means of communication, for example by prescribing the use of "written," "signed" or "original" documents. While a few countries have adopted specific provisions to deal with certain aspects of electronic commerce, there exists a lack of legislation dealing with electronic commerce as a whole. This may result in uncertainty as to the legal nature and validity of information presented in a form other than a traditional paper document. Moreover, while sound laws and practices are necessary in all countries where the use of EDI and electronic mail is becoming widespread, this need is also felt in many countries with respect to such communication techniques as telecopy and telex.

4. The Model Law may also help to remedy disadvantages that stem from the fact that inadequate legislation at the national level creates obstacles to international trade, a significant amount of which is linked to the use of modern communication techniques. Disparities among, and uncertainty about, national legal regimes governing the use of such communication techniques may contribute to limiting the extent to which businesses may access international markets.

5. Furthermore, at an international level, the Model Law may be useful in certain cases as a tool for interpreting existing international conventions and other international instruments that create legal obstacles to the use of electronic commerce, for example by prescribing that certain documents or contractual clauses be made in written form. As between those States parties to such international-instruments, the adoption of the Model Law as a rule of interpretation might provide the means to recognize the use of electronic commerce and obviate the need to negotiate a protocol to the international instrument involved.

6. The objectives of the Model Law, which include enabling or facilitating the use of electronic commerce and providing equal treatment to users of paper-based documentation and to users of computer-based information, are essential for fostering economy and efficiency in international trade. By incorporating the procedures prescribed by the Model Law into its national legislation for those situations where parties opt to use electronic means of communication, an enacting State would create a medi-neutral environment.

B. Scope

7. The title of the Model Law refers to "electronic commerce." While a definition of "electronic data interchange (EDI)" is provided in article 2, the Model Law does not specify the meaning of "electronic commerce." In preparing the Model Law, the Commission decided that, in addressing the subject matter before it, it would have in mind a broad notion of EDI, covering a variety of telematics uses of EDI that might be referred to broadly under the rubric of "electronic commerce" (see A/CN.9/360, paras. 28-29), although other descriptive terms could also be used. Among the means of communication encompassed in the notion of "electronic commerce" are the following modes of transmission based on the use of electronic techniques: communication by means of EDI defined narrowly as the computer-to-computer transmission of data in a standardized format; transmission of electronic messages involving the use of either publicly available standards or proprietary standards; transmission of free-formatted text by electronic means, for example through the INTERNET. It was also noted that, in certain circumstances, the notion of "electronic commerce" might cover the use of techniques such as telecopy.
the principles on which the Model Law is based, as well as its provisions, are intended to apply also in the context of less advanced communication techniques, such as telecopy. There may exist situations where digitalized information initially dispatched in the form of a standardized EDI message might, at some point in the communication chain between the sender and the recipient, be forwarded in the form of a computer-generated telex or in the form of a telecopy of a computer print-out. A data message may be initiated as an oral communication and end up in the form of a telecopy, or it may start as a telecopy and end up as an EDI message. A characteristic of electronic commerce is that it covers programmable messages, the computer programming of which is the essential difference between such messages and traditional paper-based documents. Such situations are intended to be covered by the Model Law, based on a combination of the users' need for a consistent set of rules to govern a variety of communication techniques that might be used interchangeably. More generally, it may be noted, as a matter of principle, no communication technique is excluded from the scope of the Model Law since future technical developments need to be accommodated.

9. The objectives of the Model Law are best served by the widest possible application of the Model Law. Thus, although there is provision made in the Model Law for exclusion of certain situations from the scope of articles 6, 7, 8, 11, 12, 15 and 17, an enacting State may well decide not to enact in its legislation substantial restrictions on the scope of application of the Model Law.

10. The Model Law should be regarded as a balanced and discrete set of rules, which are recommended to be enacted as a single statute. Depending on the situation in each enacting State, however, the Model Law could be implemented in various ways, either as a single statute or in several pieces of legislation (see below, para. 143).

C. Structure

11. The Model Law is divided into two parts, one dealing with electronic commerce in general and the other one dealing with electronic commerce in specific areas. It should be noted that part two of the Model Law, which deals with electronic commerce in specific areas, is composed of a chapter I only, dealing with electronic commerce as it applies to the carriage of goods. Other aspects of electronic commerce might need to be dealt with in the future, and the Model Law can be regarded as an open-ended instrument, to be complemented by future work.

12. UNCITRAL intends to continue monitoring the technical, legal and commercial developments that underlie the Model Law. It might, should it regard it advisable, decide to add new model provisions to the Model Law or modify the existing ones.

D. A "framework" law to be supplemented by technical regulations

13. The Model Law is intended to provide essential procedures and principles for facilitating the use of modern techniques for recording and communicating information in various types of circumstances. However, it is a "framework" law that does not itself set forth all the rules and regulations that may be necessary to implement those techniques in an enacting State. Moreover, the Model Law is not intended to cover every aspect of the use of electronic commerce. Accordingly, an enacting State may wish to issue regulations to fill in the procedural details form principles authorized by the Model Law and to take account of the specific, possibly changing, circumstances at play in the enacting State, without compromising the objectives of the Model Law. It is recommended that, should it decide to issue such regulation, an enacting State should give particular attention to the need to maintain the beneficial flexibility of the provisions in the Model Law.

14. It should be noted that the techniques for recording and communicating information considered in the Model Law, beyond raising matters of procedure that may need to be addressed in the implementing technical regulations, may raise certain legal questions the answers to which will not necessarily be found in the Model Law, but rather in other bodies of law. Such other bodies of law may include, for example, the applicable administrative, contract, criminal and judicial-procedure law, which the Model Law is not intended to deal with.

... The "functional-equivalent" approach

15. The Model Law is based on the recognition that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication. In the preparation of the Model Law, consideration was given to the possibility of dealing with impediments to the use of electronic commerce posed by such requirements in national laws by way of an extension of the scope of such notions as "writing," "signature" and "original," with a view to encompassing computer-based techniques. Such an approach is used in a number of existing legal instruments, e.g., article 7 of the UNIFORM Model Law on International Commercial Arbitration and article 13 of the United Nations Convention on Contracts for the International Sale of Goods. It was observed that the Model Law should permit States to adapt their domestic legislation to developments in communications technology applicable to trade law without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements. At the same time, it was said that the electronic fulfillment of writing requirements might in some cases necessitate the development of new rules. This was due to one of many distinctions between EDI messages and paper-based documents, namely the latter were read-only by the human eye, while the former were not so readable unless reduced to paper or displayed on a screen.

16. The Model Law thus relies on a new approach: sometimes referred to as the "functional equivalent approach," which is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic commerce techniques. For example, among the functions served by a paper document are the following: to provide that a document would be legible for all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of a document by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts. It should be noted that in respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met. However, the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment.

17. A data message, in and of itself, cannot be regarded as an equivalent of a paper document in that it is of a different nature and does not necessarily perform all conceivable functions of a paper document. That is why the Model Law adopted a flexible standard, taking into account the various layers of existing requirements in a pa