Bangladesh National Parliament

Dhaka, 23 Ashwin, 1413/8 October, 2006

The following Act undertaken by the Parliament received approval from the President on 23 Ashwin, 1413 corresponding to 8 October 2006 and thus published for the public: --

Act No. 39 of the year 2006

Act prepared to provide legal recognition and security of Information and Communication Technology and rules of relevant subjects

Since it is plausible and necessary to provide legal recognition and security of Information & Communication Technology and prepare rules of relevant subjects;

Thus hereby the following Act has been created:--

Chapter I
PRELIMINARY

1. Short Title, extent and commencement.--(1) This Act may be called the Information & Communication Technology Act, 2006.

(2) It shall extend to the whole of Bangladesh.

2. Definitions.-- In this Act, unless the context otherwise requires,--

(1) "digital signature" means data in an electronic form, which--

(a) is related with any other electronic data directly or logically; and

(b) is able to satisfy the following conditions for validating the digital signature--

(i) affixing with the signatory uniquely;

(ii) capable to identify the signatory;

(iii) created in safe manner or using a means under the sole control of the signatory; and

(iv) related with the attached data in such a manner that is capable to identify any alteration made in the data thereafter.

(2) "digital signature certificate" means a certificate issued under section 36;

(3) "electronic" means electrical, digital, magnetic, wireless, optical, electromagnetic or any technology having equivalent such capability;

(4) "electronic data interchange" means transferring data from one computer to another computer electronically by following a standard for the purpose of organizing information;

(5) "electronic form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated microfiche or similar device or technology;

(6) "electronic gazette" means the official gazette published in the electronic form in addition to official printed & published gazette;

(7) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche;

(8) "internet" means such an international computer network by which users of computer, cellular phone or any other electronic system around the globe can communicate with

one another and interchange information and can browse the information presented in the websites;

(9) "electronic mail" means information generated electronically and transmitted using internet;

(10) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized 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, punch cards, punched tapes or stored internally in the memory of the computer;

(11) "data message" means electronic, electronic data interchange including optical, electronic mail, telegram, telex, fax, telecopy, short message or created something similar, sent, received or stored information;

(12) "website" means document and information stored in computer and web server which can be browsed or seen by the user through internet;

(13) "computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetical 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;

(14) "computer network" means the interconnection of one or more computers through the use of satellite, microwave, terrestrial line, wireless equipment, wide area network, local area network, infrared, WiFi, bluetooth or other communication media; and terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

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

(16) "chairman" means a chairman appointed under cyber appeal tribunal of section 82 of this Act;

(17) "civil procedure" means Code of Civil Procedure, 1908 (Act V 0f 1908);

(18) "penal code" means Penal Code, 1860 (Act XLV of 1860);

(19) "prescribed" means prescribed by rules;

(20) "secure signature generating machine or technology" means any signature generating machine or technology subject to the conditions illustrated under section 17;

(21) "addressee" with reference to data message means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(22) “verification” means such procedure used to identify signatory or authentication of data message;

(23) "originator" with reference to data message means a person who sends or prepares data message before preservation or causes any date message to be sent, generated, stored or transmitted but does not include an intermediary;

(24) "regulation" means regulation prepared under this Act;

(25) "criminal procedure" means Code of Criminal Procedure, 1898 (Act V of 1898);

(26) “person” relates to unique person having any natural entity, partnership business, union, company, body corporate, cooperatives;

(27) “adjudicating officer” means an adjudicating officer of cyber tribunal constituted under section 68 of this Act;

(28) “rule” means rule prepared under this Act;

(29) "medium" means any person sending, receiving, advancing or saving any data message or any service rendering on this data message on behalf of any other person for a particular data message;

(30) "licence" means a licence granted under section 22 of this Act;

(31) "authentication service provider" means certificate issuing authority or any person rendering service related to digital signature.

(32) "certifying authority" means a person or authority who has been granted a licence under section 18 to be read with section 22 of this Act to issue a Digital Signature Certificate:

(33) "certification practice and description of procedure" means certification practice and description of procedure defined by the regulation where practices and procedures are written for issuing Digital Signature Certificate;

(34) "member" means a member of cyber appeal tribunal constituted under section 82 of this Act;

(35) "signatory" means a person providing signature generated through signature generating machine or procedure;

(36) "signature verification machine" means software or hardware used for verifying signature;

(37) "signature generating machine" means software or hardware used generating data for creating signature;

(38) "cyber tribunal" or "tribunal" means a cyber tribunal constituted under section 82 of this Act;

(39) "cyber appeal tribunal" means a cyber appeal tribunal constituted under section 82 of this Act.

3. Domination of the Act.-- Where any law provides whatever anything it contained, the rules of this Act shall be in force;

4. Inter-state application of the Act.--(1) If any person commits offence or contravention under this Act outside of Bangladesh which is punishable under this Act if he commits it in Bangladesh, then this Act shall apply as such he commits offence or contravention in Bangladesh;

(2) If any person commits offence or contravention in Bangladesh under this Act from outside Bangladesh using a computer, computer system or computer network located in Bangladesh, then this Act shall apply as such the entire process of the offence or contravention took place in Bangladesh;

(3) If any person from within Bangladesh commits offence or contravention outside of Bangladesh under this Act, then this Act shall apply against him as such the entire process of the offence or contravention took place in Bangladesh;

Chapter II
DIGITAL SIGNATURE & ELECTRONIC RECORDS

5. Authentication of electronic records by digital signature.--(1) Subject to the provision of sub-section (2) of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of electronic record shall be effected by the use of technology neutral system or standard authentic signature generating machine or strategy.

6. 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 information or matter is rendered or made available in an electronic form:

Provided that such information or matter is accessible so as to be usable for a subsequent reference.

7. Legal recognition of digital signatures.--Where any law provides that--

(a) any information or any other matter shall be authenticated by affixing the signature; or

(b) any document shall be authenticated by signature or bear the signature of any person;

then, notwithstanding anything contained in such law, such information or matter is authenticated by means of digital signature affixed in defined manner or so is the case of any document.

8. Use of electronic records and electronic 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, approval or order by whatever name called in a particular manner;

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

then, notwithstanding anything contained in such law, filing, issue, grant of the document and receipt and payment of money, as the case may be, is effected by means of prescribed electronic form.

(2) The manner and format in which such electronic records shall be filed, created or issued and the manner or methods of payment of any fee or charges for creation and filing shall be fixed by the rules for fulfilling the purposes of this section.

9. Retention of electronic records.--(1) Where any law provides that any document, record or information shall be retained for any specific period, then such requirement shall be deemed to have been satisfied if such documents, records or information, as the case may be, are retained in the electronic form if the following conditions are satisfied--

(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) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained:

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

(2) A person may satisfy the requirements referred to in sub-section (1) of this section by using the services of any other person, if the conditions in clauses (a) to (c) of that sub-section are complied with.

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

10. Electronic gazette.-- Where any law requires that any law, 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 law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:

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

11. No liability on Government to accept documents in electronic form.--Nothing contained in this Act shall by itself compel any Ministry or Department of the Government or any authority or body established by or under any law or controlled or funded by the Government to accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

12. Power of Government to make rules in respect of digital signatures.--The Government may, by notification in the Official Gazette and in additionally optionally in the Electronic Gazette, make the following rules (all or any of them) to prescribe for the purposes of this Act--

(a) the type of digital signature;

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

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

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

(e) any other matter which is necessary to give legal effect to digital signatures.

Chapter III
ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS

13. Attribution. -- (1) An electronic record shall be that of the originator it was sent by the originator himself.

(2) As between the originator and the addressee, an electronic record shall be 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 electronic record; 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 shall be entitled to regard an electronic record as being that of the originator and to act on that assumption if--

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

(b) the information 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 the electronic records as its own.

(4) Sub-section (3) of this section shall not apply--

(a) from the time when the addressee has received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly;

(b) in such case as in clause (b) of section (3) of this section, at any time when the addressee knew or ought to have known, after using reasonable care or using agreed procedure, that the electronic record was not that of the originator;

(c) if, in all circumstances of the case, it is unconscionable for the addressee to regard the electronic record as being that of the originator or to act on that assumption.

(5) Where an electronic record 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 shall be entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption.

(6) Whatever is there in sub-section (5) of this section, the addressee shall not be so entitled when the addressee knew or should have known, after exercising reasonable care or using any agreed procedure, that the transmission resulted in any error in the electronic record as received.

(7) The addressee shall be entitled to regard each electronic record received as separate electronic record and to act on that assumption; however, it shall not be applicable for the following electronic records--

(a) duplicates of other electronic records created by the addressee; and

(b) the addressee knew or should have known, after exercising reasonable care or using any agreed procedure, that the electronic record was a duplicate.

14. Acknowledgement of receipt.-- (1) Sub-sections (2), (3) & (4) of this section shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or has agreed with the addressee that receipt of the electronic record 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 electronic record has been received.

(3) Where the originator has stipulated that the electronic record shall be conditional on receipt of the acknowledgement, then, until the acknowledgement has been received, the electronic record shall be deemed to have been never sent by the originator.

(4) Where the originator has not stipulated that the electronic record shall be 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 no acknowledgement is received within the time specified in clause (a) of this sub-section, may, after giving notice to the addressee, treat the electronic record as though it has never been sent.

(5) Where the originator receives the addressee's acknowledgement of receipt, it shall be presumed that the related electronic record was received by the addressee, but that presumption shall not imply that the content of the electronic record corresponds to the content of the record received.

(6) Where the received acknowledgement states that the related electronic record met technical requirements, either agreed upon or set forth in applicable standards, it shall be presumed that those requirements have been met.

15. Time and place of dispatch and receipt of electronic record. -- (1) Save as otherwise agreed to between the originator and the addressee,--

(a) the time of dispatch of an electronic record shall be determined when it enters a computer or electronic machine or resource out side the control of the originator;

(b) the time of receipt of an electronic record shall be determined as follows, namely:--

(i) if the addressee has designated an electronic device or resource for the purpose of receiving electronic records, receipt occurs,--

(a) at the time when the electronic record enters the designated electronic device or resource;

(b) if the electronic record is sent to an electronic device or resource of the addressee that is not designated electronic device or resource, at the time when the electronic record is retrieved by addressee;

(ii) if the addressee has not designated an electronic device or resource along with the specified timings, if any, receipt occurs when the electronic record enters the electronic device or resource.

(c) An electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(2) The provision of sub-section (1) (b) of this section shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (1) (c) of this section.

(3) For the purposes of this section,--

(a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

Explanation.-- "principal place of business" or "usual place of residence" in relation to a body corporate or body incorporated means the place where it is registered.

Chapter IV
SECURE ELECTRONIC RECORDS & DIGITAL SIGNATURES

16. Secure electronic record.-- Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to a secure electronic record from such point of time to the time of verification.

17. Secure digital signature.-- (1) If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was--

(a) unique to the person affixing it;

(b) capable of identifying the person affixing it; and

(c) created in manner or using a means under the sole control of the person affixing;

then such digital signature shall be deemed to be a secure digital signature as per sub-section (2).

(2) Despite the fact of sub-section (1), the digital signature would be invalidated if the electronic record was altered relating to this very digital signature.

Chapter V
CONTROLLER & CERTIFYING AUTHORITIES

18. Certifying Authorities Controller and other officers.-- (1) For the purpose of this Act, the Government may, by notification in the Official Gazette and additionally optionally in Electronic Gazette, appoint a Controller and such number of Deputy Controller(s) and Assistant Controller(s) as it deems fit within 90 days of the enactment of this law.

(2) The Controller shall discharge such functions as are vested in him under this Act under the general superintendence and control of the Government.

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

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

(5) The Head Office of the Controller shall be located at Dhaka and as the Government may think fit may establish Branch Offices at such places for fixed time duration or permanently.

(6) There shall be a seal of the office of the controller, which will be used in places approved by the Government and other defined areas.

(7) For the purpose of preserving all electronic records under this Act there shall be a room in the Office of Controller which will be named as "electronic records repository room."

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

(a) exercising supervision over the activities of the Certifying Authorities;

(b) laying down the standards to be maintained by the Certifying Authorities;

(c) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(d) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(e) specifying the contents of written, printed or visual materials and advertisements that may be used in respect of a Digital Signature Certifying;

(f) specifying the form and content of a Digital Signature Certificate;

(g) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(h) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them for auditing the Certifying Authorities;

(i) facilitatining the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(j) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(k) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(l) laying down the duties and responsibilities of the Certifying Authorities;

(m) maintaining computer based databases, which--

(i) contain the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations; and

(ii) shall be accessible to the member of the public;

(n) perform any other function under this Act or Codes prepared under this Act.

20. 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 Government, and by notification in the Official Gazette and additionally optionally in Electronic Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognized under sub-section (1) of this section, 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) of this section, for reasons to be recorded in writing, by notification in the Official Gazette and additionally optionally in Electronic Gazette, revoke such recognition.

21. 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 ensure that the secrecy and security of the digital signature are assured and in order to do so shall make use of hardware, software and procedures that are secure from intrusion and misuse and follow such standards as may be prescribed.

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

(2) No licences shall be issued under sub-section (1) of this section unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities which are necessary to issue Digital Signature Certificates.

(3) A licence granted under sub-section (1) of this section—

(a) shall be valid for certain period;

(b) shall be delivered subject to fulfilling defined terms and conditions; and

(c) shall not be transferable or heritable.

23. Application for licence.-- (1) Every application for issue of a licence shall be submitted in a prescribed form.

(2) Every application of sub-section (1) of this section shall be accompanied by—

(a) a certification practice statement;

(b) necessary documents with respect to identification of the applicant;

(c) evidence of payment of defined fees;

(d) such other documents as may be prescribed.

24. Renewal of licence.—Licence issued under this Act shall be renewed automatically for a certain period subject to paying fees in a prescribed procedure.

25. Procedure for grant or rejection of licence.—The Controller may, on receipt an application under sub-section (1) of section 22 of this Act, after considering the documents accompanying the application and such other factors as he deems fit, grant the licence or reject the application:

Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

26. Revocation and suspension of licence.—(1) The Controller may suspend or revoke any licence under this Act, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has—

(a) made statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

(c) failed to main the standards specified under section 21(2) of this Act;

(d) contravened any provisions of this Act, rules, regulations or orders made thereunder.

(2) No licence shall be revoked unless the Certifying Authority has been given reasonable opportunity of showing cause against the proposed revocation under sub-section (1) of this section.

(3) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1) of this section, by or, suspend such licence temporarily pending the completion of any enquiry ordered by him.

(4) No licence shall be suspended for a period exceeding 14 (fourteen) days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the propose suspension under sub-section (3) of this section;

(5) A Certifying Authority whose licence has been suspended temporarily shall not issue any Digital Signature Certificate during the period of such suspension.

27. Notice of revocation or suspension of licence.—(1) Where the licence of a Certifying Authority is revoked or suspended temporarily, the Controller shall publish notice of such revocation or suspension, as the case may be, in the database maintained by him.

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

Provided that the database containing the temporarily notice of such revocation or suspension, as the case may be, shall be made available electronically including website or any other medium which shall be accessible round the clock.

28. Power to delegate.—The Controller may, in writing, authorize the Deputy Controller, Assistant Controller or any other officer to exercise any of the power of the Controller under this Act.

29. Power to investigate contraventions.—(1) The Controller or any officer authorized 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 authorized by him in this behalf shall, for the purposes of sub-section (1) of this section, have the same power as are vested in a Civil Court under the Code of Civil Procedure, when trying a suit in respect of the following matters, namely:--

(a) discovery and inspection;

(b) enforcing the attendance of any person and examining him on oath or affirmation;

(c) compelling the production of any document; and

(d) issuing commissions for the examination of witness.

30. Access to computers and data.—(1) Without prejudice to the provisions of section 45 of this Act the Controller or any officer authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act or rules and regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any 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 purpose of sub-section (1) of this section the Controller or any officer authorized 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.

(3) If authorization has been given to a person, the authorized person shall oblige to assist as instructed under sub-section (1) of this section.

31. 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 reasonable suited to the performance of intended function under this Act;

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

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

32. Certifying Authority to ensure compliance of the Act, rules, regulations, 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.

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

34. Surrender of licence.—Every Certifying Authority whose licence is revoked or suspended, as the case may be, shall immediately after such revocation or suspension, as the case may be, surrender the licence to the Controller.

35. Disclosures.—(1) Every Certifying Authority shall disclose in the manner specified by regulations—

(a) Digital Signature Certificate used by the 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 the materially and adversely affects either the reliability of a Digital Signature Certificate, which the Certifying Authority has issued, or the Certifying Authority's ability to perform its service.

(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 use reasonable efforts to notify any person who is likely to affected by the occurrence, or act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

36. Issue of certificate.—The Certifying Authority may issue a certificate to a prospective subscriber only after the Certifying Authority—

(a) has received an application in the prescribed form requesting for issuance of a certificate from the prospective subscriber;

(b) if it has a certification practice statement, complied with all of the practices and procedures set forth in such certification practice

(c) if the prospective subscriber is the person to be listed in the certificate to be issued;

(d) if all information in the certificate to be issued is correct; and

(e) whether the prospective subscriber paid such fees as may be prescribed for issuance of certificate.

37. Representations upon issuance of certificate.—(1) By issuing a certificate, the Certifying Authority represents to any person who reasonably relies on the certificate or digital signature described in the certificate that the Certifying Authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice.

(2) In the absence of such certification practice statement mentioned in sub-section (1) of this section, the Certifying Authority represents that it has confirmed that—

(a) the Certifying Authority has complied with all applicable requirements of this Act and the rule and regulations made thereunder in issuing the certificate, and if the Certifying Authority has published the certificate or otherwise made it available to such relying person, that the subscriber listed in the certificate has accepted it;

(b) all information in the certificate is accurate, unless the Certifying Authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed;

(c) the Certifying Authority has no knowledge of any material fact which if it had been included in the certificate would adversely effect the reliability of the representations in clauses (a) and (b) of this sub-section.

(3) Where there is an applicable certification practice statement which has been incorporated by reference in the certificate, or of which the relying person has notice, sub-section (2) of this section shall apply to the extent that the representations are not inconsistent with the certification practice statement.

38. Revocation of Digital Signature Certificate.—A Certifying Authority shall revoke a Digital Signature Certificate issued by it—

(a) where the subscriber or any person authorized by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) where the subscriber is a firm or a company, if it has been dissolved or wound up or has otherwise ceased to exist.

(2) Subject to the provisions of sub-section (3) of this section and without prejudice to the provisions of sub-section (1) of this section, 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 identification/security system was compromised in a manner materially or as a whole affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent by a competent court or authority.

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

(a) on receipt of a request to that effect from the subscriber listed in the Digital Signature certificate or any person duly authorized to act on behalf of that subscriber;

(b) if it is 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 30 (thirty) days without giving the subscriber a notice under sub-section 1 (b) of this section.

(3) Certifying Authority can suspend the Digital Signature Certificate, if the Authority is satisfied on the ground that the explanation given by the subscriber in response to the notice of sub-section (2) of this section is not acceptable.

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

40. Notice of revocation or suspension.—(1) Where a Digital Signature Certificate is revoked under section 38 of this Act or suspended under section 39 of this Act, the Certifying Authority shall publish a notice of such revocation or suspension, 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 revocation or suspension, as the case may be, in all such repositories.

Chapter VI
DUTIES OF SUBSCRIBERS

41. Application of security procedure.--The subscriber shall apply required security procedure to ensure the purity of Digital Signature Certificate issued by a Certifying Authority.

42. Acceptance of Digital Signature Certificate.--(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate to one or more persons or in a repository.

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

(a) all representations made by the subscriber to the Certifying Authority and all materials relevant to the information contained in the Digital Certificate are true; and

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

43. Presumption of represented information of obtaining Digital Signature Certificate.-- All material representations made by the subscriber to a Certifying Authority for purposes of obtaining a certificate, including all information known to the subscriber and represented in the Digital Signature Certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the Certifying Authority.

44. Control of safety measure of subscriber.--(1) Every subscriber shall exercise reasonable care to retain control of using of Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber.

(2) If the security of Digital Signature Certificate has been compromised by disobeying the rules in sub-section (1) of this section, the subscriber shall communicate the same without any delay to the Certifying Authority who has issued the Digital Signature Certificate in an agreed manner.

Chapter VII
BREACHING RULES, PREVENTION, PENALTIES ETC.

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

46. Power of Controller to give directions in emergency.—If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty, integrity, or security of Bangladesh, friendly relations of Bangladesh with other States, public order or for preventing incitement to commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information to be transmitted through any computer resource.

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

47. Power to announce protected systems.—(1) The Controller may, by notification in the Official Gazette or in Electronic Gazette, declare any computer, computer system or computer network to be a protected system.

(2) The Controller, by order in writing, authorize the persons who are authorized to secure access to protected systems notified under sub-section (1) of this section.

48. Penalty for failure to furnish document, return and report.—If any person fails to submit given document, return and report under the provisions of this Act, or rules and regulations made thereunder to the Controller or Certifying Authority, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person which may extend to Taka ten thousands mentioning reasons in written by administrative order.

49. Penalty for failure to file return, information, book etc.—If any person fails to deliver any information, books or any other documents under the provisions of this Act, or rules and regulations made thereunder within stipulated time, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person which may extend to Taka ten thousand mentioning reasons in written by administrative order.

50. Penalty for failure to maintain books of accounts or record.—If any person fails to maintain books of accounts or records which is supposed to be preserved under the provisions of this Act, or rules and regulations made thereunder, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person which may extend to Taka two lakhs mentioning reasons in written by administrative order.

51. Residuary penalty.—If any person contravenes any rules of this Act for which the provision of penalties has not been fixed separately under the provisions of this Act, or rules and regulations made thereunder, the Controller or any officer of the Government authorized by the Government by special order, as the case may be, can fine the person for breaching the very rule which may extend to Taka twenty five thousands mentioning reasons in written by administrative order.

52. Power of Controller to issue prohibition of possible breaching of rules.—(1) If the Controller is in the opinion that, any person has attempted or is attempting to do such activities which is breaching or may breach the provisions of this Act, rules, regulations made thereunder, or conditions or any order of the Controller then the Controller shall issue a notice within the stipulated time limit ordering the person to present his statement in written why he should not refrain himself from doing such activity and if such statement is presented then the Controller shall issue an order to refrain him from doing such activity or any other instruction about the activity sthat deems fit to him.

(2) If the Controller is satisfied that, the nature of breaching or possible breaching under sub-section (1) of this section is such that to prevent the person from that activity immediately, then the Controller shall issue an interim order which deems fit to him during the time of issuing a notice under that sub-section.

(3) If any instruction under sub-sections (1) and (2) of this section is given to anyone, he shall be bound to obey it.

(4) If any person breaches the given instructions of this section, the Controller can fine the person which may extend to Taka ten thousand.

53. Penalties.—(1) The Controller can impose penalties for breaching other rules under this Act defined by the rules as an addition to imposable penalties under this Act.

(2) No penalty shall be imposed under this Act for breaching this Act or any rules of this Act without giving reasonable opportunity to the offender on hearing.

(3) The accused person can lodge an application to the Controller for auditing the decision of imposing penalties by the Controller within seven days from the date the decision is made and if any such application is lodged, the Controller shall give opportunity to the Applicant for hearing and dissolve it within fifteen days.

(4) Unless the penalties are paid under this Act which is due, is collectable as a Government demand under the Public Demands Recovery Act, 1913 (Ben. Act III of 1913).

Chapter VIII
OFFENCES, INVESTIGATION, ADJUDICATION, PENALTIES ETC.

Part-1
Offences & Penalties

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

(a) accesses or secure access to such computer, computer system or computer networks for the purpose of destroying information or retrieving or collecting information or assists other to do so;

(b) downloads, copies or extracts any data, computer database or 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 willingly in any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies of causes the denial of access to any person authorized 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) for the purpose of advertisement of goods and services, generates or causes generation of spams or sends unwanted electronic mails without any permission of the originator or subscriber;

(i) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network;

then the above said activities shall be treated as offences of the said person.

(2) If any person commits offence under sub-section (1) of this section, he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to Taka ten lakhs, or with both.

Explanation.--For the purpose of this section--

(i) "computer contaminant" means any set of computer instructions that are designed--

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

(b) by any means to usurp the normal operation of the computer, computer system or computer network;

(ii) "computer database" means a representation information, knowledge, facts, concepts or instructions in the form of text, image, audio or video that--

(a) are being prepared or have been prepared in a formalized manner by a computer, computer system or computer network; and

(b) are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means such computer instruction, information, data or program, that--

(a) destroys, damages, degrades or adversely affects the performance of a computer resource; or

(b) attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer;

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

55. Punishment for tampering with computer source code.--(1) Whoever intentionally or knowingly conceals, destroys or alters or intentionally or knowingly causes other person to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by any law for time being in force, then this activity of his will be regarded as offence.

(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to three years, or with fine which may extend to Taka three lakhs, or with both.

Explanation.--For the purpose of this section, "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resources in any form.

56. Punishment for hacking with computer system.--(1) If any person--

(a) with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(b) damage through illegal access to any such computer, computer network or any other electronic system which do not belong to him;

then such activity shall be treated as hacking offence.

(2) Whoever commits hacking offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to Taka one crore, or with both.

57. Punishment for publishing fake, obscene or defaming information in electronic form.--(1) If any person deliberately publishes or transmits or causes to be published or transmitted in the website or in electronic form any material which is fake and obscene 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, or causes to deteriorate or creates possibility to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity of his will be regarded as an offence.

(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to ten years and with fine which may extend to Taka one crore.

58. Punishment for failure to surrender licence.--(1) Where any Certifying Authority fails to surrender a licence under section 34 of this Act, the person in whose favour the licence is issued, the failure of the person shall be an offence.

(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to six months, or with fine which may extend to Taka ten thousands, or with both.

59. Punishment for failure to comply with order.--(1) Any person who fails to comply with any order made under section 45 of this Act, then this activity of his will be regarded as an offence.

(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to one year, or with fine which may extend to Taka one lakh, or with both.

60. Punishment for failure to comply with order made by the Controller in emergency --(1) Any person who fails to comply with any order made under section 46 of this Act, then this activity of his will be regarded as an offence.

(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to five years, or with fine which may extend to Taka five lakhs, or with both.

61. Punishment for unauthorized access to protected systems.--(1) Any person who secures access or attempts to secure access to protected system in contraventions of section 47 of this Act, then this activity of his will be regarded as an offence.

(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to ten years, or with fine which may extend to Taka ten lakhs, or with both.

62. Punishment for misrepresentation and obscuring information.--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 shall be regarded as an offence.

(2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.

63. Punishment for disclosure of confidentiality and privacy.--Save as otherwise provided by this Act or any other law for the time being in force, no person who, in pursuance of any of the powers conferred under this Act, or rules and regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record, book, register, correspondence, information, document or other material to any other person shall be regarded as an offence.

(2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.

64. Punishment for publishing false Digital Signature Certificate.--No person shall publish a Digital Signature Certificate or otherwise make it available to any other person knowing 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 and by breaching the rules such Digital Signature Certificate is published or otherwise make it available to others shall be regarded as an offence.

(2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakhs, or with both.

65. Punishment for publishing Digital Signature Certificate for fraudulent purpose etc.-- Whosoever knowingly creates and publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be regarded as an offence.

(2) Whoever commits any offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Taka two lakh, or with both.

66. Punishment for using computer for committing an offence.--(1) Whosoever knowingly assists committing crimes under this Act, using any computer, e-mail or computer network, resource or system shall be regarded as an offence.

(2) Whoever aids committing any offence under sub-section (1) of this section he shall be punishable with the punishment provided for the core offence.

67. Offences committed by companies etc.--If any offence is committed by a company under this Act, then each director, manager, secretary, partner, officer and staff of the company who has directly involvement in committing the said offence shall be guilty of the offence or the contraventions, as the case may be, unless he proves that the offence or contravention was committed without his knowledge or that he exercised sue diligence in order to prevent commission of such offence or contravention.

Explanation.—For the purposes of this section.—

(a) "company" means any body corporate and includes commercial firm, partnership business, cooperatives, association, organization or other association of individuals; and

(b) "director" in relation to a commercial firm includes a partner or member of Board of Directors.

Part-2
Establishment of Cyber Tribunal, Investigation of Offences, Adjudication, Appeal Etc.

68. Establishment of Cyber Tribunal.—(1) The Government shall, by notification in the Official Gazette, establish one or more Cyber Tribunals to be known as Tribunal at times for the purposes of speedy and effective trials of offences committed under this Act.

(2) Cyber Tribunal established under sub-section (1) of this section in consultation with the Supreme Court shall be constituted by a Session Judge or an Additional Session Judge appointed by the Government; and similarly appointed a Judge to be known as "Judge, Cyber Tribunal."

(3) Local jurisdiction of entire Bangladesh or jurisdiction of one or more Session Divisions can be given to the Cyber Tribunal established under this Act; and the Tribunal only prosecutes the offences committed under this Act.

(4) The on-going prosecution of any case of any Session Court shall not be suspended or transferred automatically to the Tribunal of local jurisdiction concerned due to tendering of local jurisdiction of entire Bangladesh or parts of jurisdiction constituted by one or more Session Divisions to the Tribunal established by the Government later on, however, the Government by notification in the Official Gazette, transfer the case to the Tribunal having special local jurisdiction.

(5) Any Tribunal, taken decision otherwise, shall not be bound to retaking statement of witness who has already given statement, or taking rehearing or begin again any other activities already undertaken under sub-section (1) of this section, however, the Tribunal shall continue the prosecution from where it stood on the basis of already taken or presented statement from the witness.

(6) The Government, by order, shall define the place and time; accordingly the special Tribunal shall conduct its activities from that place and time.

69. Trial procedure of Cyber Tribunal.--(1) Without written report of a police officer not below the rank of Sub-Inspector or the prior approval of the Controller or any other officer authorized by the Controller the special Tribunal shall not accept any offence trial.

(2) The Tribunal shall follow the rules mentioned in the Chapter 23 of the Code of Criminal Procedure, if they are not inconsistent with the rules of this Act, which is used in Session Court.

(3) Any Tribunal shall not suspend any prosecution without having written reasons and unless it is required for the sake of just adjudication.

(4) If the Tribunal is in the opinion that the accused person has been absconded and for that it is not possible to arrest him and produce him before the Tribunal and there is no possibility to arrest him immediately, in that case the Tribunal can order the accused person to appear before the Tribunal by publishing such order in two mass circulated national Bengali dailies and if the accused person fails to do so, the prosecution shall take place in his absence.

(5) The rules mentioned in sub-section (4) of this section shall not be applicable if the accused person fails to appear before the Tribunal or absconded after getting bail.

(6) The Tribunal can order any police officer, or the Controller, or any officer authorized by the Controller, as the case may be, to reinvestigate the case and submit the report within the stipulated time of its own initiative or any application lodged to the Tribunal,

70. Application of code of criminal procedure in the activities of Tribunal.—(1) Rules of Code of Criminal Procedure, as far as, are not inconsistent with the rules of this Act shall be applicable in the activities of this Tribunal and it will have all the power as exercised by the Session Court.

(2) The person prosecuting the case on behalf of the Government in this tribunal to be known as public prosecutor.

71. Rules relating to bail.—The Judge of Cyber Tribunal shall not bail any person accused in committing crime under this Act, which is punishable, unless--

(a) Hearing opportunity is given to the Government side on similar bail orders;

(b) The Judge is satisfied that,--

(i) There is reasonable cause to believe that the accused person may not be proved guilty in the trial;

(ii) The offence is not severe in relative term and the punishment shall not be tough enough even the guilt is proved.

(c) He writes down the reasons of similar satisfactions.

72. Time limit to deliver verdict.--(1) The Judge of Cyber Tribunal shall give the verdict within ten days from the date of completing of taking evidence or debate, what happened later, unless he extends the time limit no more than ten days with having written reasons.

(2) If the verdict is given by the Cyber Tribunal under sub-section (1) of this section or any appeal is lodged against the verdict to the Cyber Appellate Tribunal then Cyber Tribunal or Cyber Appellate Tribunal concerned shall forward the copy of the verdict of the appeal to the Controller for preserving it in the electronic records repository room established under section 18 (7) of this Act.

73. Prescribed timeframe for dissolving cases by Cyber Tribunal.—(1) The Judge of Cyber Tribunal shall complete the prosecution within six months since the date of filing the charge sheet.

(2) If the Judge of Cyber Tribunal fails to complete the prosecution within the time limit fixed under sub-section (1) of this section can extend the time limit another three months having written the reasons.

(3) If the Judge of Cyber Tribunal fails to complete the prosecution within the timeframe fixed under sub-section (2) of this section can continue the prosecution process having written the reasons and submitted it as a report to the High Court and the Controller.

74. Prosecution of offence by Session Court.—Whatever is contained in the Code of Criminal Procedure, until the special tribunal has not been established, the Session Court shall prosecute any offence committed under this Act.

75. Prosecution procedure followed by the Session Court.—(1) To prosecute any offence committed under this Act which is trialed in Session Court, Session Court shall follow the rules mentioned in section 23 of the Code of Criminal Procedure which is applicable in Session Court trial.

(2) Any Session Court shall not accept any prosecution/trial of any offence committed under this Act without any written report from the police officer not below the rank of Sub-Inspector of the Police and prior approval of the Controller or any officer authorized by the Controller, whatever is contained in the Code of Criminal Procedure.

76. Investigation of crime, etc.—(1) Whatever is contained in the Code of Criminal Procedure, the Controller or any officer authorized by the Controller, or any police officer not below the rank of Sub-Inspector of the Police shall investigate any offence committed under this Act.

(2) Offence committed under this Act shall be non-cognizable offence.

77. Confiscation.—(1) Any computer, computer system, floppies, compact disks (CDs), 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, or in respect of which any offence has been committed, shall be liable to confiscation by an order of the court trying an offence or contravention.

(2) If the court is satisfied, that the computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories belonging to a person or under control of him related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has not been responsible to contravene, or committing an offence, then the computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories shall not be confiscated.

(3) If any legal computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories is found with the computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories which is confiscated under sub-section (1) of this section shall also be confiscated.

(4) Any computer or other relevant accessories belonging to the Government or Body Government Authority is used to commit an offence under sub-section (1) of this section, whatever contained in this section, shall not be confiscated.

78. Penalties or confiscation no bar against 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 may be liable under any other law for the time being in force.

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, or rules and 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 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.

80. Power of seize or arrest in public place, etc.—Any investigation taken under this Act, the Controller, or any officer of Government authorized by the Government or any police officer not below the rank of a Sub-Inspector of Police are in opinion that an offence has been committed or being committed or offence which is punishable under this Act has been committed, then having written the reasons, may enter the public place and search and seize the germane materials and arrest the concerned person or the offender.

81. Procedure of search, etc.—The provisions of the Code of Criminal Procedure shall, subject to the provisions of this Act, apply, so far as may be, in relation to all investigations, entry, search and arrest made under this Act.

Part-3
Establishment of Cyber Appellate Tribunal, Etc.

82. Establishment of Cyber Appellate Tribunal.—(1) The Government shall, by notification in the Official Gazette, establish one or more Cyber Appellate Tribunals to be known as Appellate Tribunal.

(2) Cyber tribunal established under sub-section (1) of this section shall consist of one Chairman and two members to be appointed by the Government.

(3) A person shall not be qualified as the Chairman of a Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of the Supreme Court and one of the members shall be serving in judicial department or retired District Judge and the other member shall be a person having adequate knowledge and experience in information and communication technology.

(4) Chairman and members shall be retained in the positions since the date of joining between no less than three years and no more than five years and their terms of reference shall be determined by the Government.

83. Procedure and powers of Cyber Appellate Tribunal.--(1) Cyber Appellate Tribunal shall have the power to hear appeal and dissolving the verdict and order given by Cyber Tribunal and Session Court, as the case may be.

(2) In case of hearing and dissolving the appeal, Cyber Appellate Tribunal shall follow the procedure defined by rules and if the rules do not exist in that case Appellate Tribunal shall maintain the procedure in relation to hearing and dissolving of criminal appeal followed by the High Court Division of the Supreme Court.

(3) Cyber Appellate Tribunal shall have the power to retain, revoke, alter, or rectify the verdict or order made by the Cyber Tribunal.

(4) The decision made by the Appellate Tribunal shall be final.

84. Appeal procedure in case of not establishing Cyber Appellate Tribunal.--If the Cyber Appellate Tribunal has not been established, whatever contained in the Code of Criminal Procedure,

appeal shall be lodged in the High Court Division of Supreme Court against the verdict and order given by the Session Court or Cyber Tribunal, as the case may be.

Chapter IX
MISCELLANEOUS

85. Public servants.--The Controller, the Deputy Controller, the Assistant Controller or any person empowered under this Act to exercise his power and carrying out the tasks shall be deemed to be public servants within the meaning of section 21 of Penal Code.

86. Protection of action in good faith.--No suit, prosecution or other legal proceedings shall lie against the Government, the Controller, the Deputy Controller, the Assistant Controller or any person acting on his behalf, for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation, order or direction made thereunder.

87. Augmented use of few definitions used in few acts.--For the purpose of this Act,--

(a) The definition of "document" in section 29 of Penal Code, 1860 (Act XLV of 1860) also includes the document generated or prepared by electronic machine or technology;

(b) The definition of "document" in section 3 of Evidence Act, 1872 (Act I of 1872) also includes the document generated or prepared by electronic machine or technology;

(c) The definition of "bankers books" in section 2, Clause (3) of Banker's Books Evidence Act, 1891 (Act XVIII of 1891) also includes the books viz. ledgers, day-books, cash-books, account-books and all other books generated or prepared by electronic machine or technology;

88. Power of Government to make rules.--The Government may, by notification in the Official Gazette and in the Electronic Gazette, make for all or any of the following rules for carrying out of this Act:

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

(b) the electronic form in which filing, issue, grant or payment;

(c) the manner and format in which electronic records shall be filed, or issued and the method of payment;

(d) the matters relating to the type of digital signature, manner and format in which it may be affixed;

(e) the qualifications, experience and terms and conditions of service of the Controller, Deputy Controllers and Assistant Controllers;

(f) other standards to be observed by the Controller;

(g) the requirements which an applicant must fulfill;

(h) the period of validity of licence;

(i) the format in which an application may be made;

(j) the amount of fees payable with application for licence;

(k) such other document which shall accompany an application for licence;

(l) the form of application for renewal of a licence and the fee payable;

(m) the form in which application for issue of a Digital Signature Certificate and the amount of fees payable;

(n) the qualifications and experience of Chairman and members of Cyber Appeal Tribunal;

(o) the form in which appeal may be filed;

(p) the procedure of investigation;

(q) other such necessary matters.

89. Power of Controller to make regulations.--The Controller with prior approval of the Government, by notification in the Official Gazette and in the Electronic Gazette, make for all or any of the following regulations:--

(a) the particulars relating to maintenance of database containing the disclosure record of every Certify Authority;

(b) the conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority;

(c) the terms and conditions subject to which a licence may be granted;

(d) other standards to be observed by a Certifying Authority;

(e) the manner in which the Certifying Authority shall disclose the particular matters;

(f) the particulars of statement which shall accompany an application.

90. Original script & English script.--The original script shall be in Bengali and there shall be a dependable English transcription of it.

Provided that any conflict arises between Bengali & English scripts the Bengali script shall get domination.