1. Short title and commencement - (1) These Rules will be called Information Technology (Certifying Authorities) Rules, 2010.

(2) They shall come into force immediately.

2. Definitions - In these Rules, unless the context otherwise requires,–

(a) "Act" means the Information, Communication and Technology Act, 2006 (Act no. 39 of 2006);

(b) "applicant" means the person who applied for acting as Certifying Authority;

(c)"auditor" means internationally accredited computer security professional or agency appointed by the Certifying Authority and recognized by the Controller for conducting technical audit of operation of Certifying Authority;

(d) "Electronic Signature" means electronic signature as defined in section 2(1) of the Act and for the purpose of these Rules, digital signature will also be considered as electronic signature;

(e)"information asset" means all information resources utilized in the course of any organisation's business and includes all information, application of exhibited or developed or purchased software, and technology (hardware, system software and networks);

(f) "person" means an individual, or a company or association and shall include authorities of the Government of Bangladesh having knowledge of issuance of Electronic Signature Certificates;

(g) "Public key" means a specific value determined by the nominated authority, which is used as "encryption key" combining with "private key" to effectively encrypt information and electronic signature;

(h) "Private key" means secret information or electronic signature giver's known encryption or decryption key, which is used to encrypt information into electronic signature or public key used with private key;

(i) "Schedule" means schedule annexed to these Rules;

(j) "subscriber identity verification method" means the method used to verify and authenticate the identity of a subscriber;

(k) "trusted or dependable person" means any person whose: –

i. principal responsibility is to ensure day-to-day activities, provide security and direct any other activities of a Certifying Authority under the Act and any Rules or Regulations formulated under the Act; or

ii. duty involves verification of identity of a person who requested Electronic Signature Certificate from a Certifying Authority, and also issuance, renewal, cancellation or suspension of that Electronic Signature Certificate, creation of private key or administration of the computing facilities of the Certifying Authority.

3. Method in which information can be authenticated by means of Electronic Signature –

(1) An Electronic Signature shall be created and verified by such cryptography which transform electronic records into seemingly unintelligible form and back;

(2) A method, known as "Public Key Cryptography", shall be used for creating and verifying electronic signature, which employs an algorithm using two different but mathematically related "keys" – one for creating an Electronic Signature or transforming data into a seemingly unintelligible form, and another key for verifying an Electronic Signature or returning the electronic record to original form,

(3) The process termed as hash function shall be used in both creating and verifying a Digital Signature.

4. Creation of Electronic Signature.- To sign an electronic record or any other item of information, the signer shall apply the following method:

(a) use hash function in the signer's own software, for all usage needs, which in the case of electronic record shall compute a hash result of standard length which is unique to the electronic record;

(b) use private key to transform the hash result of the signer's software into an Electronic Signature;

(c) the Electronic Signature created by following the method contained in sub-Rule (a) and (b), shall be unique or uniform to both electronic record and private key used to create it; and

(d) the Electronic Signature shall be attached to the electronic record and appropriately protected and thereafter transmitted with the electronic record.

5. Verification of Electronic Signature- (1) The verification of an Electronic Signature shall be accomplished by the following method:-

(a) by computing a new hash result of the original electronic record by means of the hash function used to create an Electronic Signature and by sing the public key;

(b) the encrypted digital digest shall be decrypted by using public key;

(c) by comparing the new hash result with the decrypted hash;

(2) In instances, when:-

(a) similar private and public key is used to create an Electronic Signature,

(b) newly computed hash result is similar with the original result, and

(c) which transforms into Electronic Signature during the signing process.

the verifier shall verify the Electronic Signature.

(3) The verification software will confirm the Electronic Signature as verified if:-

(a) in order to digitally sign the electronic record, the private key of the signer is used and the public key of the signer is used to verify the signature, in that instance the electronic record shall be considered to have been digitally signed;

(b) an electronic record will be deemed to be unaltered, if the hash result computed by the verifier is identical to the hash result extracted from the Digital Signature during the verification process.

6. Authentication of Public Key – A public key shall be authenticated in the following manner-

(a) if the public key was generated by using secret cryptography; and

(b) the Controller authenticates the said public key.

7. Standards – The Information Technology architecture followed by Certifying Authorities shall be of appropriate and acceptable standards and the activities of such authority shall be in accordance with the standards as set out in Schedule-2 or as prescribed by the Controller from time to time.

8. Standard of issuance of Electronic Signature Certificate- All Electronic Signature Certificates issued by the Certifying Authorities shall conform to ITU X.509 version 3 (or above) standard or similar standards and shall contain the following data, namely:-

(a) Unique Serial Number, which is assigned by Certifying Authority in the Electronic Signature Certificate in order to distinguish it from other certificate;

(b) Information for authentication of the algorithm process used to compute signature, which is used by the Certifying Authority for authentication of the process of computing signature for signing an Electronic Signature Certificate;

(c) Name of the issuer, which shall include the name of the Certifying Authority;

(d) Validity period of the Electronic Signature Certificate;

(e) Name of the subscriber, which can authenticate the public key in the Certificate; and

(f) Public Key information of the subscriber.

9. Licensing of Certifying Authorities.- (1) Any person interested to obtain licence to issue Electronic Signature Certificate shall apply to the Controller at such time and manner as determined by the Controller, and shall, along with the application, furnish such information and pay such security and fees as may be prescribed time to time.

(2) A licence may be issued in favour of a citizen, association, company, partnership firm or any other entity, if -

(a) in the case of association or company, at least sixty percent of the shares of the association or company is owned or controlled by Bangladeshi citizens; and

(b) in the case of partnership firm or any other entity, the capital or proprietary right of the firm or the entity, is owned or controlled by Bangladeshi citizens.

10. Bank Guarantee – (1) In order to obtain licence under rule 9, applicant has to as security for the licence furnish a bank guarantee from a scheduled bank in favour of the Controller in such form and manner as may be approved by the Controller.

(2) The amount of security in the form of bank guarantee shall be determined by the Controller from time to time.

(3) The Bank Guarantee shall be valid for a period of 5 (five) years from the date of issuance of the licence as per Rule 16

(4) The Controller may order encashment of the bank guarantee for the following reasons–

(a) when the Controller has cancelled or suspended the licence under sub-section (2) of section 26 of the Act; or

(b) for payment of compensation imposed by the Controller; or

(c) for payment of liabilities and rectification costs attributed to the negligence of the Certifying Authority, its officers or employees; or

(d) for payment of the costs incurred in the discontinuation or transfer of operations of the licensed Certifying Authority, if the Certifying Authority's licence or operations is discontinued; and

(e) for failure of the default made by the Certifying Authority in complying with the provisions of the Act or rules made there under.

11. Location of the Facilities - The infrastructure associated with all functions of generation, issue and management of Electronic Signature Certificate under these Rules as well as maintenance of Directories containing information about the status, and validity of Electronic Signature Certificate shall be installed at any location in Bangladesh.

12. Submission of Application- (1) Every application for a licensed Certifying Authority shall submit to the Controller in the form prescribed by the Controller/given at Schedule-I; and

(2) the application shall be supported by the following documents-

(a) a Certification Practice Statement (CPS);

(b) a description including the procedures to determine the identification of the applicant;

(c) a description to have an idea of the technology used for providing Electronic Signature, management or operations which are outsourced;

(d) attested copies of certificate of incorporation or trade licence of Certifying Authority who applied for licence;

(e) past and current information from financial institution, that proves the ability of the applicant to act as a Certifying Authority;

(f) an undertaking by the applicant that to its best knowledge and belief it will comply with the Certification Practice standard while issuing certificates;

(g) an undertaking that the Certifying Authority shall not not commence its operation until its operation and facilities associated with the functions of generation, issuance and management of Electronic Signature Certificate are audited by the auditors and approved by the Controller;

(h) an undertaking to furnish bank guarantee as per Rule 10 within one month of receipt of direction relating approval from the Controller to operate as a Certifying Authority;

(i) any other information required by the Controller.

13. Fees- Fees, as prescribed by the Controller, from time to time shall be deposited by way of non-refundable bank draft, pay order or electronically, along with the application for licence or renewal of licence.

14. Cross Certification- (1) Certificate issued by Certifying Authority which can be cross certified with other licenced Certifying Authority situated in Bangladesh, must have such arrangement, which has to be submitted to the Controller prior to commencement of operation under Rule 21:

Provided that any dispute arising as a result of any such arrangement between the Certifying Authorities or between the Certifying Authority and the subscriber, shall be referred to the Controller for arbitration or resolution.

(2) If cross certification is required between Certifying Authority and foreign Certifying Authority, upon request from the local Certifying Authority the Controller shall complete such certification as per prescribed forms and process determined by regulation.

(3) Without the written approval of the Controller, licensed Certifying Authority shall not conduct any cross certification operations.

15. Validity of licence.- Every licence shall be valid for a period of 5 (five) years from the date of its issue or for such a period as determined by the Controller and such license is not transferable.

16. Issuance of Licence- (1) The Controller may, within six weeks from the date of receipt of the application, after considering the documents accompanying the application and such other factors, as may deem fit, grant the licence or reject the application:

Provided that in exceptional circumstances and for reasons to be recorded in writing, the Controller may extend the time period in such manner so that in no way it exceeds 8 (eight) weeks.

(2) If the application for licensed Certifying Authority is approved, the applicant shall -

(a) furnish bank guarantee within 1 (one) month from the date of such approval to the Controller in accordance with Rule 10; and

(b) submit and undertaking to the Controller binding himself to comply with the terms and conditions of the licence and the provisions of the Act and the Rules made there under.

17. Renewal of Licence- (1) In case of renewal of of a licence issued under this Rules, the provisions of Rules 9, 10, 12, 13 and 14 shall be applicable in the same manner as it apply to new application.

(2) Application for renewal of licence has to be made not less than sixty (60) days before the date of expiry of the licence.

18.Refusal of Licence- The Controller may refuse to grant or renew a licence in the following circumstances:-

(a) if the applicant does not provided the Controller with such information relating to its business as mentioned in Rule 12, and if it seems to the Controller that such information may affect the business of the applicant;

(b) if the applicant is in the course of being wound up;

(c) if any Court appoint a receiver and manager with respect to the applicant;

(d) if the applicant, whether in or out of Bangladesh, is convicted of an offence of dishonesty or fraud or any other offence under the existing laws;

(e) if the applicant fails to furnish bank guarantee as per direction of the Controller for the reasons stated in Rule 10(1);

(f) if a Certifying Authority breaches or fails to take steps as per the Certification Practice Statement;

(g) if a Certifying Authority does not or fails to submit audit report as per Rule 32;

(h) if it can be seen from the audit report that the Certifying Authority is unable to continue operation as a Certifying Authority;

(i) if a Certifying Authority fails to comply with the directions of the Controller.

19. Suspension or Cancellation of License - (1) The Controller may by order revoke or suspend the licence in accordance with the provisions contained in section 26 of the Act.

(2) The licence granted to the persons referred to in rule 9 shall stand suspended if upon being called upon to submit the performance bond, or banker's guarantee as required under Rule 10, he fails to submit the same.

(3) A license could also be suspended or cancelled for the following reasons: namely

(a) if the Certifying Authority fails to comply the with the security guidelines, Or

(b) If any Certifying Authority became bankrupted or loan defaulter or any administrator or receiver has been appointed, or

(c) if the Certifying Authority fails to comply with the requirement of audit as mentioned in Rule 32.

20. **Security Guidelines for Certifying Authorities**- (1) The Certifying Authorities shall have the responsibility of integrity, confidentiality and protection of information and information assets employed in its operation, considering classification, declassification, labeling, storage, access and destruction of information assets according to their value, sensitivity and importance of operation.

(2) The controller shall issue the Information Technology Security Guidelines and Security Guidelines for Certifying Authorities aimed at protecting the integrity, confidentiality and availability of service of the Certifying Authority.

(3) The Certifying Authority shall formulate its Information Technology and Security Policy within 60 (sixty) days after issuance of the licence for operation complying with these guidelines and submit the same to the Controller before commencement of operation:

Provided that the controller may make any change(s) in the Information Technology and Security Policy formulated by the Certifying Authority if the Controller thinks fit and the

Controller shall inform such amendment to the Certifying Authority within 14(fourteen) days from the date of its submission to the Controller.

21. **Commencement of Operation by Licensed Certifying Authorities**- The licensed Certifying Authority shall commence its operation and issue of Digital Signature only after the following activities completed; namely -

(a) it has confirmed to the Controller the adoption of Certification Practice Statement;

(b) it has generated its key pair, namely, private and corresponding public key, and submitted the public key to the Controller;

(c) the installed facilities and infrastructure associated with all functions of generation, issue and management of Electronic Signature Certificate have been audited by the accredited auditor in accordance with the provisions of rule 32; and

(d) it has submitted the arrangement for cross certification with other licensed Certifying Authorities to the Controller.

22. **Requirements Prior to Cessation as Certifying Authority.-** (1) Before ceasing to act as a Certifying Authority, a Certifying Authority shall, give notice to the Controller of its intention to cease acting as a Certifying Authority:

Provided that the notice shall be given ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of licence;

(2) shall advertise sixty days before the expiry of licence or ceasing to act as Certifying Authority, as the case may be by publishing notice of the intention in such daily newspaper or electronic media and website and in such manner as the Controller may determine;

(3) notify its intention to cease acting as a Certifying Authority to the subscribers and Cross Certifying Authority of each unrevoked or unexpired Electronic Signature Certificate issued by it :

Provided that the notice shall be given 60 (sixty) days before ceasing to act as a Certifying Authority or 60(sixty) days before the date of expiry of Electronic Signature Certificate, as the case may be;

(4) the notice shall be sent to the Controller, affected subscribers and Cross Certifying Authorities by electronically signed e-mail and registered post;

(5) revoke all Electronic Signature Certificates that remain unrevoked or unexpired, whether or not the subscribers have requested revocation;

(6) take appropriate steps to ensure that discontinuing its certification services does not prejudice its subscribers and to persons duly in need to verify Electronic Signatures by reference to the public keys contained in outstanding Electronic Signature Certificates;

(7) make reasonable arrangements for preserving the records for a period of ten years;

(8) pay appropriate compensation (not exceeding the cost involved in obtaining the new Electronic Signature Certificate) to subscribers for revoking the Electronic Signature Certificates before the date of expiry;

(9) after the date of expiry as mentioned in the licence, the Certifying Authority shall destroy the certificate–signing private key and inform the date and time of destruction of the private key to the Controller.

23. Database of Certifying Authorities- The Controller shall maintain a database of the disclosed record of every Certifying Authority, Cross Certifying Authority and Foreign Certifying Authority, containing the following details:

(a) the name of the person/names of the Directors, nature of business, Taxpayers Identification Number (TIN), website address, office and residential address, facilities associated with functions of Electronic Signature Certificate, telephone and fax numbers, e-mail address(es), administrative contacts and addresses of authorized representatives;

(b) the public key(s) used by the Certifying Authority and recognized foreign Certifying Authority to sign Elecronic Signature Certificate;

(c) current and past versions of Certification Practice Statement of Certifying Authority;

(d) following information indicating the date and time of -

(i) grant of licence;

(ii) confirmation of adoption of Certification Practice Statement and its past versions by Certifying Authority;

(iii) commencement of operations of generation and issuance of Electronic Signature Certificate by the Certifying Authority;

(iv) revocation or suspension of licence of Certifying Authority;

(v) commencement of operation of Cross Certifying Authority;

(vi) recognition of foreign Certifying Authority;

(vii) revocation or suspension of recognition of foreign Certifying Authority.

24. Electronic Signature Certificate.- (1) The Certifying Authority shall, for issuing the Electronic Signature Certificates, while complying with the provisions of section 36 of the Act, shall also comply with the following, namely:-

(a) the Electronic Signature Certificate shall be issued only after a Electronic Signature Certificate application in the form provided by the Certifying Authority has been submitted by the subscriber to the Certifying Authority and the same has been approved by it:

(b) no interim Electronic Signature Certificate shall be issued;

(c) the Electronic Signature Certificate shall be issues by the Certifying Authority upon receipt of an authorized and validated request for new Electronic Signature Certificate or for renewal of an and Electronic Signature Certificates;

(d) the Electronic Signature Certificate must contain or incorporate, such information, as is sufficient to locate or identify one or more repositories and such information must be listed in the list of revocation or suspension of the Electronic Signature Certificate in the event the Electronic Signature Certificate is suspended or revoked;

(e) the subscriber identity verification method employed for issuance of Electronic Signature Certificate shall be in accordance with the method specified in the Certification Practice Statement and shall be subject to the approval of the Controller during the application for a licence;

(f) where the Electronic Signature Certificate is issued to a person which is considered as a New Electronic Signature Certificate, on the basis of another valid Electronic Signature Certificate held by the said person which is considered as an Originating Electronic Signature Certificate, and subsequently the originating Electronic Signature Certificate has been suspended or revoked, the Certifying Authority that issued the new Electronic Signature Certificate shall conduct investigations to determine

whether it is necessary to suspend or revoke the new Electronic Signature Certificate;

(g) the Certifying Authority shall provide a reasonable opportunity for the subscriber to verify the contents of the Electronic Signature Certificate before it is accepted;

(h) in the event the subscriber accepts the Electronic Signature Certificate, the Certifying Authority shall publish a signed copy of the Electronic Signature Certificate;

(i) where the Electronic Signature Certificate has been issued by the licensed Certifying Authority and has been accepted by the subscriber, and the Certifying Authority later comes to know of any fact, that affects the validity or reliability of such Electronic Signature Certificate, it shall notify the same to the subscriber immediately;

(j) all Electronic Signature Certificates shall be issued with a designated expiry date.

25. Generation and usages of Electronic Signature Certificate - The usages and transmission of the Electronic Signature Certificate shall involve the following, namely :-

(a) receipt of an approved and verified Electronic Signature Certificate request;

(b) creation of a new Electronic Signature Certificate;

(c) binding the key pair associated with the Electronic Signature Certificate to a Electronic Signature Certificate owner;

(d) a distinguished name associated with the Electronic Signature Certificate owner;

(e) a recognized and relevant name as defined in Certification Practice Statement.

26. **Issuance of Electronic Signature Certificate** - Before the issue of the Electronic Signature Certificate, the Certifying Authority shall confirm the followings, namely:-

(a) the user's name does not appear in its list of compromised users;

(b) comply with the procedure as defined in its Certification Practice Statement including verification of identification and employment;

(c) comply with all privacy requirements; and

(d) obtain a consent of the person requesting the Electronic Signature Certificate, that the details of such Electronic Signature Certificate can be published on a directory service.

27. <u>The Lifetime policy of Certificate</u> - (1) the Electronic Signature Certificate,-

(a) shall be issued with a designated expiry date;

(b) which is suspended shall return to the operational use, if the suspension is withdrawn in accordance with the provisions of section 39 of the Act;

(c) shall be extinguished automatically upon reaching the designated expiry date by which time the Electronic Signature Certificate shall be archived;

(d) on expiry, shall not be re-used.

(2) The period for which an Electronic Signature Certificate has been issued shall not be extended, but a new Electronic Signature Certificate may be issued after the expiry of such period.

28. Archival of Electronic Signature Certificate - A Certifying Authority shall keep in archive the following documents at least for 7(Seven) years or for such period as may be required by any other legal proceedings, namely -

(a) application of the applicant for issue of Electronic Signature Certificates;

(b) registration and verification documents of Electronic Signature Certificates;

(c) Electronic Signature Certificates;

(d) notices of temporary suspension;

(e) information relating to temporary suspended Electronic Signature Certificates;

(f) information relating to withdrawal of suspension orders; and

(g) information relating to expiration of Electronic Signature Certificates,

29. Compromise of Electronic Signature Certificate – (1) Electronic Signature Certificates in operational use that become compromised shall be revoked in

accordance with the procedure defined in the Certification Practice Statement of Certifying Authority.

Explanation : For the purpose of this rules, Electronic Signature Certificates shall,-

(a) be deemed to be compromised where the integrity if:-

(i) doubt arises in relation to the private key associated with the Electronic Signature Certificate; or

(ii)doubt arises as to the use, or attempted use of the key pairs by the Electronic Certificate owner or if he uses or attempts to use the keys for malicious or unlawful purposes;

The certificate described under sub-rule (1) shall remain in the compromised state for only such time as it takes to arrange for necessary actions.

30. Revocation of Electronic Signature Certificate- (1) Electronic Signature Certificate may be revoked for the following reasons and the same will become unusable, namely -

(a) there is a compromise of the Electronic Signature Certificate owner's private key; or

(b) there is a misuse of the Electronic Signature Certificate; or

(c) false or wrong information have been presented in the Electronic Signature Certificate; or

(d) the Electronic Signature Certificate is no longer required.

(2) The revoked Electronic Signature Certificate shall be added to the Certificate Revocation List (CRL).

31. Fees for issue of Electronic Signature Certificate.- (1)The Certifying Authority may issue Electronic Signature Certificate upon charging such fee as may be approved by the Controller.

(2) Fee may be paid by downloading and accessing to the Certifying Authority's X.500 directory . Certifying Authority shall provide an up-to-date fee schedule to all its subscribers and users.

(3) The schedule of fees may published in the specified website or in other media.

(4) Fees could be collected via Internet.

32. Audit - (1) The Certifying Authority shall get its operations audited annually by an auditor and such audit shall include the following information, namely,-

(a) security policy and planning;

(b) practical security;

(c) technology evaluation;

(d) Certifying Authority's services administration;

(e) Certification Practice Statement and its compliance;

(f) Any executed contracts/agreements;

(g) regulations prescribed by the Controller; and

(h) policy in according to the requirement of Certifying Authorities.

(2) The Certifying Authority shall conduct,-

(a) half yearly audit of the Security Policy, physical security and planning of its operation;

(b) a quarterly audit of its repository.

(3) The Certifying Authority shall submit copy of each compliance report to the Controller within four weeks of the completion of such audit and where irregularities are detected in such audit or submitted report, the Certifying Authority shall take immediate appropriate steps.

33. Auditor's relationship with Certifying Authority.- (1) The auditor shall be independent of the Certifying Authority being audited and shall not be a software or hardware vendor which is, or has been providing services or supplying equipment to the said Certifying Authority.

(2) the auditor for the purpose of Rule shall be enlisted to the Controller being satisfied that that the auditor has sufficiently equipped, technically skilled, expertise, manpower and technology for auditing Certifying Authority ;

(3) The auditor and the Certifying Authority shall not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

34. Confidential Information.- The certifying authority should keep the following information confidential, namely:--

(a) Application for Electronic Signature Certificate, whether approved or rejected;

(b) Information relating to Electronic Signature Certificate collected from the subscriber or elsewhere as part of the registration and verification record but this will not include information contained in the Digital Signature Certificate information;

(c) Executed subscriber agreement.

35. Access to Confidential Information- (1) Access to confidential information by Certifying Authority's operational staff shall be on a "need-to-know" and "need-to-use" basis.

(2) Paper based records, documentation and backup data containing all confidential information as prescribed in rule 34 shall be kept in secure and locked container or filing system, separately from all other records.

(3) No confidential information shall be allowed to be taken outside the country, however, the controller may grant permission for taking confidential information outside the country if the same is required for performing constitutional obligation or any document is produced before him which legally obliges him to grant such permission.

(3) SCHEDULE-I

[*See* rule 10]

Form for Application for grant of Licence to be a Certifying Authority

SCHEDULE-II

[*See* rule 7]

The product	The standard
Public Key Infrastructure	PKIX
Digital Signature Certificates and Digital Signature revocation list	X.509. version 3 certificates as specified in ITU RFC 1422
Directory (DAP and LDAP)	X500 for publication of certificates and Certification Revocation Lists (CRLs)
Database Management Operations	Use of generic SQL
Public Key algorithm	DSA and RSA
Digital Hash Function	MD5 and SHA-1
RSA Public Key Technology	PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit) PKCS#5 Password Based Encryption Standard PKCS#7 Cryptographic Message Syntax standard PKCS#8 Private Key Information Syntax standard PKCS#9 Selected Attribute Types PKCS#10 RSA Certification Request PKCS#12 Portable format for storing/transporting a user's private keys and certificates
Distinguished name	X.520
Digital Encryption and Digital Signature	PKCS#7
Digital Signature Request Format	PKCS#10