The Information Technology (Certifying Authorities) Rules, 2000

Notification, New Delhi, the 17th October, 2000, G.S.R 789(E).—In exercise of the powers conferred by Section 87 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules regulating the application and other guidelines for Certifying Authorities, namely:—

1. Short title and commencement.—(1) These Rules may be called Information Technology (Certifying Authorities) Rules, 2000.

(2) They shall come into force on the date of their publication in the Official Gazette.

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

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "applicant" means Certifying Authority applicant;

(c) "auditor" means any 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) "Controller" means Controller of Certifying Authorities appointed under sub-section (1) of Section 17 of the Act;

(e) "Digital Signature Certificate" means Digital Signature Certificate issued under sub-section (4) of Section 35 of the Act;

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

(g) "licence" means a licence granted to Certifying Authorities for the issue of Digital Signature Certificates under these rules;

(h) "licensed Certifying Authority" means Certifying Authority who has been granted a licence to issue Digital Signature Certificates;

(i) "person" shall include an individual; or a company or association or body of individuals; whether incorporated or not; or Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments;

(j) "Schedule" means a schedule annexed to these rules;

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

(l) "trusted person" means any person who has:—

  (i) direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or these Rules in respect of a Certifying Authority; or

  (ii) duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys or administration of a Certifying Authority's computing facilities.

(m) words and expressions used herein and not defined but defined in Schedule-IV shall have the meaning respectively assigned to them in that schedule.

3. The manner in which information be authenticated by means of Digital Signature.—A Digital Signature shall.—(a) be created and verified by cryptography that concerns itself with transforming electronic record into seemingly unintelligible forms and back again;

(b) use what is known as "Public Key Cryptography", which employs an algorithm using two different but mathematical related "keys" – one for creating a Digital Signature or transforming data into a seemingly unintelligible form, and another key for verifying a Digital Signature or returning the electronic record to original form, the process termed as hash function shall be used in both creating and verifying a Digital Signature.

Explanation: Computer equipment and software utilizing two such keys are often termed as "asymmetric cryptography".

4. Creation of Digital Signature.—To sign an electronic record or any other item of information, the signer shall first apply the hash function in the signer's software; the hash function shall compute a hash result of standard length which is unique (for all practical purposes) to the electronic record; the signer's software transforming the hash result into a Digital Signature using signer's private key; the resulting Digital Signature shall be unique to both electronic record and private key used to create it; [1][the Digital Signature and the digital signature Certificate attached to its electronic record shall be stored or transmitted along with its electronic record].

5. Verification of Digital Signature.—The verification of a Digital Signature shall be accomplished by computing a new hash result of the original electronic record by means of the hash function used to create a Digital Signature and by using the public key and the new hash result, the verifier shall check—

(i) if the Digital Signature was created using the corresponding private key; and

(ii) if the newly computed hash result matches the original result which was transformed into Digital Signature during the signing process. The verification software will confirm the Digital Signature as verified if:—

(a) the signer's private key was used to digitally sign the electronic record, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a Digital Signature created with the signer's private key; and

(b) the electronic record was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the Digital Signature during the verification process.

[2]**[5A. Verification of Digital Signature Certificate.—**(a) The self signed certificate generated by the controller, which begins the trust chain for the public key infrastructure, shall be used to verify the authority of the public key certificate of the licensed Certifying Authorities;

(b) the public key certificate of the licensed Certifying Authorities shall be used to verify the authenticity of the digital signature certificate issued to the subscribers;

(c) the certificate revocation list maintained by the licensed Certifying Authorities shall be checked to confirm whether the certificate is valid or whether it has been revoked under Section 38 of the Act;

(d) while verifying the validity of a digital signature the corresponding digital signature certificates should chain up through the public key certificate of the issuing Certifying Authority to the self signed certificate of the Controller and if any of the certificates in the trust chain is not trusted the signature will not be verified.]

---

1. Substituted by G.S.R. 782(E), dated 25-10-2011 (w.e.f. 25-10-2011).

2. Inserted by G.S.R. 782(E), dated 25-10-2011 (w.e.f. 25-10-2011).

6. Standards.—The Information Technology (IT) architecture for Certifying Authorities may support open standards and accepted de facto standards; the most important standards that may be considered for different activities associated with the Certifying Authority's functions are as under:

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	[3][SHA-2]
RSA Public Key Technology	PKCS#1 RSA Encryption Standards [4][(2048, 4096 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

[5][*Explanation*:—The Digital Signature certificate granted before the commencement of the Information Technology (Certifying Authorities Amendment) Rules, 2011 using SHA-1, digital hash function standard shall continue to be valid till the date of expiry of such certificate.]

7. Digital Signature Certificate Standard.—All Digital Signature Certificates issued by the Certifying Authorities shall conform to ITU X.509 version 3 standard as per rule 6 and shall inter alia contain the following data, namely:—

(a) Serial Number (assigning of serial number to the Digital Signature Certificate by Certifying Authority to distinguish it from other certificate);

(b) Signature Algorithm Identifier (which identifies the algorithm used by Certifying Authority to sign the Digital Signature Certificate);

(c) Issuer Name (name of the Certifying Authority who issued the Digital Signature Certificate);

---

3. Substituted by G.S.R. 783(E), dated 25-10-2011 (w.e.f. 25-10-2011).
4. Substituted by G.S.R. 783(E), dated 25-10-2011 (w.e.f. 25-10-2011).
5. Inserted by G.S.R. 783(E), dated 25-10-2011 (w.e.f. 25-10-2011).

(d) Validity period of the Digital Signature Certificate;

(e) Name of the subscriber (whose public key the Certificate identifies); and

(f) Public Key information of the subscriber.

8. Licensing of Certifying Authorities.—(1) The following persons may apply for grant of a licence to issue Digital Signature Certificates, namely:—

(a) an individual, being a citizen of India and having a capital of five crores of rupees or more in his business or profession;

(b) a company having–

(i) paid up capital of not less than five crores of rupees; and

(ii) net worth of not less than fifty crores of rupees:

Provided that no company in which the equity share capital held in aggregate by the Non-resident Indians, Foreign Institutional Investors, or foreign companies, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence:

Provided further that in a case where the company has been registered under the Companies Act, 1956 (1 of 1956) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of its majority shareholders holding at least 51 per cent of paid equity capital, being the Hindu Undivided Family, firm or company:

Provided also that the majority shareholders referred to in the second proviso shall not include Non-resident Indian, foreign national, Foreign Institutional Investor and foreign company:

Provided also that the majority shareholders of a company referred to in the second proviso whose net worth has been determined on the basis of such majority shareholders, shall not sell or transfer its equity shares held in such company—

(i) unless such a company acquires or has its own net worth of not less than fifty crores of rupees;

(ii) without prior approval of the Controller;

(c) a firm having —

(i) capital subscribed by all partners of not less than five crores of rupees; and

(ii) net worth of not less than fifty crores of rupees:

Provided that no firm, in which the capital held in aggregate by any Non-resident Indian, and foreign national, exceeds forty-nine per cent of its capital, shall be eligible for grant of licence:

Provided further that in a case where the firm has been registered under the Indian Partnership Act, 1932 (9 of 1932) during the preceding financial year or in the financial year during which it applies for grant of licence under the Act and whose main object is to act as Certifying Authority, the net worth referred to in sub-clause (ii) of this clause shall be the aggregate net worth of all of its partners:

Provided also that the partners referred to in the second proviso shall not include Non-resident Indian and foreign national:

Provided also that the partners of a firm referred to in the second proviso whose net worth has been determined on the basis of such partners, shall not sell or transfer its capital held in such firm—

(i) unless such firm has acquired or has its own net worth of not less than fifty crores of rupees;

(ii) without prior approval of the Controller;

(d) Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments.

Explanation.—For the purpose of this rule,—

(i) "company" shall have the meaning assigned to it in clause 17 of Section 2 of the Income-tax Act,1961 (43 of 1961);

(ii) "firm", "partner" and "partnership" shall have the meanings respectively assigned to them in the Indian Partnership Act, 1932 (9 of 1932); but the expression "partner" shall also include any person who, being a minor has been admitted to the benefits of partnership;

(iii) "foreign company" shall have the meaning assigned to it in clause (23A) of Section 2 of the Income-tax Act,1961 (43 of 1961);

(iv) "net worth" shall have the meaning assigned to it in clause (ga) of sub-section (1) of Section 3 of the Sick Industrial Companies (Special Provisions) Act, 1985 (1 of 1986);

(v) "Non-resident" shall have the meaning assigned to it as in clause 26 of Section 2 of the Income-tax Act,1961 (43 of 1961).

(2) The applicant being an individual, or a company, or a firm under sub-rule (1), shall [6][furnish a performance bond in the form of a banker's guarantee] from a scheduled bank in favour of the Controller in such form and in such manner as may be approved by the Controller for an amount of not less than [7][fifty lakhs] of rupees and the [8][performance bond in the form of banker's guarantee] shall remain valid for a period of six years from the date of its submission:

Provided that the company and firm referred to in the second proviso to clause (b) and the second proviso to clause (c) of sub-rule (1) shall [9][furnish a performance bond in the form of a banker's guarantee] for [10][one crore] of rupees:

Provided further that nothing in the first proviso shall apply to the company or firm after it has acquired or has its net worth of fifty crores of rupees.

(3) Without prejudice to any penalty which may be imposed or prosecution may be initiated for any offence under the Act or any other law for the time being in force, the performance bond or banker's guarantee may be invoked—

(a) when the Controller has suspended the licence under sub-section (2) of Section 25 of the Act; or

(b) for payment of an offer of compensation made 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

---

6. Substituted by G.S.R. 902(E), dated 21-11-2003, for the words "submit a performance bond or furnish a banker's guarantee" (w.e.f. 27-11-2003).

7. Substituted by G.S.R. 902(E), dated 21-11-2003, for "five crores" (w.e.f. 27-11-2003).

8. Substituted by G.S.R. 902(E), dated 21-11-2003, for the words "performance bond or banker's guarantee" (w.e.f. 27-11-2003).

9. Substituted by G.S.R. 902(E), dated 22-11-2003, for the words "submit a performance bond or furnish a banker's guarantee" (w.e.f. 27-11-2003).

10. Substituted by G.S.R. 902(E), dated 21-11-2003, for "ten crores" (w.e.f. 27-11-2003).

(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; or

(e) any other default made by the Certifying Authority in complying with the provisions of the Act or rules made thereunder.

Explanation.—"transfer of operation" shall have the meaning assigned to it in clause (47) of Section 2 of the Income-tax Act, 1961 (43 of 1961).

9. Location of the Facilities.—The infrastructure associated with all functions of generation, issue and management of Digital Signature Certificate as well as maintenance of Directories containing information about the status, and validity of Digital Signature Certificate shall be installed at any location in India.

10. Submission of Application.—Every application for a licensed Certifying Authority shall be made to the Controller,—

(i) in the form given at Schedule-I; and

(ii) in such manner as the Controller may, from time to time, determine, supported by such documents and information as the Controller may require and it shall inter alia include—

(a) a Certification Practice Statement (CPS);

(b) a statement including the procedures with respect to identification of the applicant;

(c) a statement for the purpose and scope of anticipated Digital Signature Certificate technology, management, or operations to be outsourced;

(d) certified copies of the business registration documents of Certifying Authority that intends to be licensed;

(e) a description of any event, particularly current or past insolvency, that could materially affect the applicant's ability to act as a Certifying Authority;

(f) an undertaking by the applicant that to its best knowledge and belief it can and will comply with the requirements of its Certification Practice Statement;

(g) an undertaking that the Certifying Authority's operation would not commence until its operation and facilities associated with the functions of generation, issue and management of Digital Signature Certificate are audited by the auditors and approved by the Controller in accordance with rule 20;

(h) an undertaking to submit a performance bond or banker's guarantee in accordance with sub-rule (2) of rule 8 within one month of Controller indicating his approval for the grant of licence to operate as a Certifying Authority;

(i) any other information required by the Controller.

11. Fee.—(1) The application for the grant of a licence shall be accompanied by a non-refundable fee of twenty-five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(2) The application submitted to the Controller for renewal of Certifying Authority's licence shall be accompanied by a non-refundable fee of five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.

(3) Fee or any part thereof shall not be refunded if the licence is suspended or revoked during its validity period.

12. Cross Certification.—(1) The licensed Certifying Authority shall have arrangement for cross certification with other licensed Certifying Authorities within India which shall be submitted to the Controller before the commencement of their operations as per rule 20:

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

(2) The arrangement for Cross Certification by the licensed Certifying Authority with a Foreign Certifying Authority along with the application, shall be submitted to the Controller in such form and in such manner as may be provided in the regulations made by the Controller; and the licensed Certifying Authority shall not commence cross certification operations unless it has obtained the written or digital signature approval from the Controller.

13. Validity of licence.—(1) A licence shall be valid for a period of five years from the date of its issue.

(2) The licence shall not be transferable.

14. Suspension of Licence.—(1) The Controller may by order suspend the licence in accordance with the provisions contained in sub-section (2) of Section 25 of the Act.

(2) The licence granted to the persons referred to in clauses (a) to (c) of sub-rule (1) of rule 8 shall stand suspended when the [11][performance bond in the form of banker's guarantee furnished] by such persons is invoked under sub-rule (2) of that rule.

15. Renewal of licence.—(1) The provisions of rule 8 to rule 13, shall apply in the case of an application for renewal of a licence as it applies to a fresh application for licensed Certifying Authority.

(2) A Certifying Authority shall submit an application for the renewal of its licence not less than forty-five days before the date of expiry of the period of validity of licence.

(3) The application for renewal of licence may be submitted in the form of electronic record subject to such requirements as the Controller may deem fit.

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

Provided that in exceptional circumstances and for reasons to be recorded in writing, the period of four weeks may be extended to such period, not exceeding eight weeks in all as the Controller may deem fit.

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

(a) [12][furnish a performance bond in the form of a banker's guarantee] within one month from the date of such approval to the Controller in accordance with sub-rule (2) of rule 8; and

(b) [13][give an 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 thereunder.

17. Refusal of Licence.—The Controller may refuse to grant or renew a licence if—

(i) the applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require; or

(ii) the applicant is in the course of being wound up or liquidated; or

---

11. Substituted by G.S.R. 902(E), dated 22-11-2003, for the words "performance bond submitted or the banker's guarantee furnished" (w.e.f. 27-11-2003).

12. Substituted by G.S.R. 902(E), dated 22-11-2003, for the words "submit a performance bond or furnish a banker's guarantee" (w.e.f. 27-11-2003).

13. Substituted by G.S.R. 536(E), dated 20-8-2004, for the words "execute an agreement with the Controller".

(iii) a receiver has, or a receiver and manager have, been appointed by the court in respect of the applicant; or

(iv) the applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these rules; or

(v) the Controller has invoked performance bond or banker's guarantee; or

(vi) a Certifying Authority commits breach of, or fails to observe and comply with, the procedures and practices as per the Certification Practice Statement; or

(vii) a Certifying Authority fails to conduct, or does not submit, the returns of the audit in accordance with rule 31; or

(viii) the audit report recommends that the Certifying Authority is not worthy of continuing Certifying Authority's operation; or

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

18. Governing Laws.—The Certification Practice Statement of the Certifying Authority shall comply with, and be governed by, the laws of the country.

19. Security Guidelines for Certifying Authorities.—(1) The Certifying Authorities shall have the sole 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) Information Technology Security Guidelines and Security Guidelines for Certifying Authorities aimed at protecting the integrity, confidentiality and availability of service of Certifying Authority are given in Schedule-II and Schedule-III respectively.

(3) The Certifying Authority shall formulate its Information Technology and Security Policy for operation complying with these guidelines and submit it to the Controller before commencement of operation:

Provided that any change made by the Certifying Authority in the Information Technology and Security Policy shall be submitted by it within two weeks to the Controller.

20. Commencement of Operation by Licensed Certifying Authorities.—The licensed Certifying Authority shall commence its commercial operation of generation and issue of Digital Signature only after—

(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 Digital Signature Certificate have been audited by the accredited auditor in accordance with the provisions of rule 31; and

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

21. Requirements Prior to Cessation as Certifying Authority.—Before ceasing to act as a Certifying Authority, a Certifying Authority shall.—

(a) give notice to the Controller of its intention to cease acting as a Certifying Authority:

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

(b) advertise sixty days before the expiry of licence or ceasing to act as Certifying Authority, as the case may be, the intention in such daily newspaper or newspapers and in such manner as the Controller may determine;

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

Provided that the notice shall be given sixty days before ceasing to act as a Certifying Authority or sixty days before the date of expiry of unrevoked or unexpired Digital Signature Certificate, as the case may be;

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

(e) revoke all Digital Signature Certificates that remain unrevoked or unexpired at the end of the ninety days notice period, whether or not the subscribers have requested revocation;

(f) make a reasonable effort to ensure that discontinuing its certification services causes minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding Digital Signature Certificates;

(g) make reasonable arrangements for preserving the records for a period of seven years;

(h) pay reasonable restitution (not exceeding the cost involved in obtaining the new Digital Signature Certificate) to subscribers for revoking the Digital Signature Certificates before the date of expiry;

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

22. Database of Certifying Authorities.—The Controller shall maintain a database of the disclosure record of every Certifying Authority, Cross Certifying Authority and Foreign Certifying Authority, containing *inter alia* the following details:

(a) the name of the person/names of the Directors, nature of business, Income-tax Permanent Account Number, web address, if any, office and residential address, location of facilities associated with functions of generation of Digital Signature Certificate, voice and facsimile telephone numbers, electronic mail address(es), administrative contacts and authorized representatives;

(b) the public key(s), corresponding to the private key(s) used by the Certifying Authority and recognized foreign Certifying Authority to digitally sign Digital Signature Certificate;

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

(d) time stamps indicating the date and time of—

  (i) grant of licence;

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

  (iii) commencement of commercial operations of generation and issue of Digital Signature Certificate by the Certifying Authority;

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

  (v) commencement of operation of Cross Certifying Authority;

  (vi) issue of recognition of foreign Certifying Authority;

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

23. Digital Signature Certificate.—The Certifying Authority shall, for issuing the Digital Signature Certificates, while complying with the provisions of Section 35 of the Act, also comply with the following, namely:—

(a) the Digital Signature Certificate shall be issued only after a Digital 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:

Provided that the application Form contains, *inter alia*, the particulars given in the modal Form given in Schedule-IV;

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

(c) the Digital Signature Certificate shall be generated by the Certifying Authority upon receipt of an authorised and validated request for:—

(i) new Digital Signature Certificates;

(ii) Digital Signature Certificates renewal;

(d) the Digital Signature Certificate must contain or incorporate, by reference such information, as is sufficient to locate or identify one or more repositories in which revocation or suspension of the Digital Signature Certificate will be listed, if the Digital Signature Certificate is suspended or revoked;

(e) the subscriber identity verification method employed for issuance of Digital Signature Certificate shall be 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 Digital Signature Certificate is issued to a person (referred to in this clause as a New Digital Signature Certificate) on the basis of another valid Digital Signature Certificate held by the said person (referred in this clause as an Originating Digital Signature Certificate) and subsequently the originating Digital Signature Certificate has been suspended or revoked, the Certifying Authority that issued the new Digital Signature Certificate shall conduct investigations to determine whether it is necessary to suspend or revoke the new Digital Signature Certificate;

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

(h) if the subscriber accepts the issued Digital Signature Certificate, the Certifying Authority shall publish a signed copy of the Digital Signature Certificate in a repository;

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

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

24. Generation of Digital Signature Certificate.—The generation of the Digital Signature Certificate shall involve:

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

(b) creating a new Digital Signature Certificate;

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

(d) issuing the Digital Signature Certificate and the associated public key for operational use;

(e) a distinguished name associated with the Digital Signature Certificate owner; and

(f) a recognized and relevant policy as defined in Certification Practice Statement.

25. Issue of Digital Signature Certificate.—Before the issue of the Digital Signature Certificate, the Certifying Authority shall:—

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

(ii) comply with the procedure as defined in his Certification Practice Statement including verification of identification and/or employment;

(iii) comply with all privacy requirements;

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

26. Certificate Lifetime.—(1) A Digital 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 37 of the Act;

(c) shall expire automatically upon reaching the designated expiry date at which time the Digital Signature Certificate shall be archived;

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

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

27. Archival of Digital Signature Certificate.—A Certifying Authority shall archive—

(a) applications for issue of Digital Signature Certificates;

(b) registration and verification documents of generated Digital Signature Certificates;

(c) Digital Signature Certificates;

(d) notices of suspension;

(e) information of suspended Digital Signature Certificates;

(f) information of revoked Digital Signature Certificates;

(g) expired Digital Signature Certificates;

for a minimum period of seven years or for a period in accordance with legal requirement.

28. Compromise of Digital Signature Certificate.—Digital 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 : Digital Signature Certificates shall,—

(a) be deemed to be compromised where the integrity of:—

(i) the private key associated with the Digital Signature Certificate is in doubt;

(ii) the Digital Signature Certificate owner is in doubt, as to the use, or attempted use of his key pairs, or otherwise, for malicious or unlawful purposes;

(b) remain in the compromised state for only such time as it takes to arrange for revocation.

29. Revocation of Digital Signature Certificate.—(1) Digital Signature Certificate shall be revoked and become invalid for any trusted use, where—

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

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

(c) there is a misrepresentation or errors in the Digital Signature Certificate;

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

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

30. Fees for issue of Digital Signature Certificate.—(1) The Certifying Authority shall charge such fee for the issue of Digital Signature Certificate as may be prescribed by the Central Government under sub-section (2) of Section 35 of the Act.

(2) Fee may be payable in respect of access to Certifying Authority's X.500 directory for certificate downloading. Where fees are payable, Certifying Authority shall provide an up-to-date fee schedule to all its subscribers and users, this may be done by publishing fee schedule on a nominated website.

(3) Fees may be payable in respect of access to Certifying Authority's X.500 directory service for certificate revocation or status information. Where fees are payable, Certifying Authority shall provide an up-to-date fee schedule to all its subscribers and users, this may be done by publishing the fee schedule on a nominated website.

(4) No fee is to be levied for access to Certification Practice Statement *via* Internet. A fee may be charged by the Certifying Authority for providing printed copies of its Certification Practice Statement.

31. Audit.—(1) The Certifying Authority shall get its operations audited annually by an auditor and such audit shall include *inter alia*,—

(i) security policy and planning;

(ii) physical security;

(iii) technology evaluation;

(iv) Certifying Authority's services administration;

(v) relevant Certification Practice Statement;

(vi) compliance to relevant Certification Practice Statement;

(vii) contracts/agreements;

(viii) regulations prescribed by the Controller;

(ix) policy requirements of Certifying Authorities Rules, 2000.

[14][(2) The Certifying Authority shall conduct half yearly internal audit of the security policy, physical security, planning of its operations and the repository]

(3) The Certifying Authority shall submit copy of each audit report to the Controller within four weeks of the completion of such audit and where irregularities are found, the Certifying Authority shall take immediate appropriate action to remove such irregularities.

32. 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 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.

33. Confidential Information.—The following information shall be confidential namely:—

(a) Digital Signature Certificate application, whether approved or rejected;

(b) Digital Signature Certificate information collected from the subscriber or elsewhere as part of the registration and verification record but not included in the Digital Signature Certificate information;

(c) subscriber agreement.

---

14. Substituted by G.S.R. 32(E), dated 18-1-2006 (w.e.f. 18-1-2006).

34. 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 33 shall be kept in secure and locked container or filing system, separately from all other records.

(3) The confidential information shall not be taken out of the country except in a case where a properly constitutional warrant or other legally enforceable document is produced to the Controller and he permits to do so.

SCHEDULE-I

[*See* rule 10]

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

For Individual

1. Full Name *
   Last Name/Surname_____
   First Name _____
   Middle Name _____
2. Have you ever been known by any other name? If Yes,
   Last Name/Surname _____
   First Name _____
   Middle Name _____
3. Address
   A. Residential Address *
   Flat/Door/Block No. _____
   Name of Premises/Building/Village _____
   Road/Street/Lane/Post Office _____
   Area/Locality/Taluka/Sub-Division _____
   Town/City/District _____
   State/Union Territory _____ Pin : _____ Telephone No. _____
   Fax _____
   Mobile Phone No. _____
   B. Office Address *
   Name of Office _____
   Flat/Door/Block No. _____
   Name of Premises/Building/Village _____
   Road/Street/Lane/Post Office _____
   Area/Locality/Taluka/Sub-Division _____
   Town/City/District _____
   State/Union Territory _____ Pin : _____
   Telephone No. _____
   Fax _____
4. Address for Communication * Tick Ö as applicable A or B
5. Father's Name *

Last Name/Surname _____

First Name _____

Middle Name _____

6. Sex * (For Individual Applicant only) Tick Ö as applicable : Male / Female
7. Date of Birth (dd/mm/yyyy) * --/--/----
8. Nationality * _____
9. Credit Card Details

   Credit Card Type _____

   Credit Card No. _____

   Issued By _____
10. E-mail Address _____
11. Web URL address _____
12. Passport Details #

    Passport No. _____

    Passport issuing authority _____

    Passport expiry date (dd/mm/yyyy) --/--/----
13. Voter's Identity Card No. # _____
14. Income Tax PAN no. # _____
15. ISP Details

    ISP Name * _____

    ISP's Website Address, if any _____

    Your User Name at ISP, if any _____
16. Personal Web page URL address, if any _____
17. Capital in the business or profession * Rs. _____

    (Attach documentary proof)

    For Company /Firm/Body of Individuals/Association of Persons/ Local Authority
18. Registration Number * _____
19. Date of Incorporation/Agreement/Partnership * --/--/----
20. Particulars of Business, if any: *

    Head Office _____

    Name of Office _____

    Flat/Door/Block No. _____

    Name of Premises/Building/Village _____

    Road/Street/Lane/Post Office _____

    Area/Locality/Taluka/Sub-Division _____

    Town/City/District _____ Pin _____

    State/Union Territory _____

    Telephone No. _____

    Fax _____

    Web page URL address, if any _____

    No. of Branches _____

Nature of Business _____

_____

21. Income Tax PAN No.* _____
22. Turnover in the last financial year Rs. _____
23. Net worth * Rs. _____
    (Attach documentary proof)
24. Paid up Capital * Rs. _____
    (Attach documentary proof)
25. Insurance Details
    Insurance Policy No.* _____
    Insurer Company * _____
26. Names, Addresses *etc.* of Partners/Members/Directors (For Information about more persons, please add separate sheet(s) in the format given in the next page)*
    No. of Partners/Members/Directors _____
    Details of Partners/Members/Directors
    A. Full Name
    Last Name/Surname _____
    First Name _____
    Middle Name _____
    B. Address
    Flat/Door/Block No. _____
    Name of Premises/Building/Village _____
    Road/Street/Lane/Post Office _____
    Area/Locality/Taluka/Sub-Division _____
    Town/City/District _____
    State/Union Territory Pin _____
    Telephone No. _____
    Fax No. _____
    Mobile Phone No. _____
    C. Nationality _____
    In case of foreign national, Visa details_____
    D. Passport Details #
    Passport No. _____
    Passport issuing authority _____
    Passport expiry date _____
    E. Voter's Identity Card No. # _____
    F. Income Tax PAN no. # _____
    G. E-mail Address _____
    H. Personal Web page URL, if any _____
27. Authorised Representative *
    Name _____

Flat/Door/Block No. _____

Name of Premises/Building/Village _____

Road/Street/Lane/Post Office _____

Area/Locality/Taluka/Sub-Division _____

Town/City/District _____ Pin _____

State/Union Territory _____

Telephone No. _____

Fax _____

Nature of Business _____

For Government Ministry/Department/Agency/Authority

28. Particulars of Organisation: *

Name of Organisation _____

Administrative Ministry/Department _____

Under State/Central Government _____

Flat/Door/Block No. _____

Name of Premises/Building/Village _____

Road/Street/Lane/Post Office _____

Area/Locality/Taluka/Sub-Division _____

Town/City/District _____ Pin _____

State/Union Territory _____

Telephone No. _____

Fax No. _____

Web page URL Address _____

Name of the Head of Organisation _____

Designation _____

E-mail Address _____

29. Bank Details

Bank Name * _____

Branch * _____

Bank Account No. * _____

Type of Bank Account * _____

30. Whether bank draft/pay order for licence fee enclosed * : Y / N If yes,

Name of Bank _____

Draft/pay order No. _____

Date of Issue _____

Amount _____

31. Location of facility in India for generation
of Digital Signature Certificate * _____

32. Public Key @ _____

33. Whether undertaking for [15][performance bond in the form of banker's guarantee] attached * : Y / N

    (Not applicable if the applicant is a Government Ministry/Department/Agency/ Authority)

34. Whether Certification Practice Statement is enclosed * : Y / N

35. Whether certified copies of business registration document are enclosed : Y / N

    (For Company/ Firm/ Body of Individuals/ Association of Persons/ Local Authority)

    If yes, the documents attached:

    i. ……
    ii. ……
    iii. ……

36. Any other information

_____

_____

_____

Date: Signature of the Applicant

Instructions : 1. Columns marked with * are mandatory.

2. For the columns marked with #, details for at least one is mandatory.
3. Column No. 1 to 17 are to be filled up by individual applicant.
4. Column No. 18 to 27 are to be filled up if applicant is a Company/ Firm/ Body of Individuals/ Association of Persons/ Local Authority.
5. Column No. 28 is to be filled up if applicant is a Government organisation.
6. Column No. , 29, 30, 31 and 34 are to be filled up by all applicants.
7. Column No. 32 is applicable only for application for renewal of licence.
8. Column No. 33 is not applicable if the applicant is a Government organisation.

SCHEDULE-II

[*See* rule 19(2)]

Information Technology (IT) Security Guidelines

1. Introduction

This document provides guidelines for the implementation and management of Information Technology Security. Due to the inherent dynamism of the security requirements, this document does not provide an exact template for the organizations to follow. However, appropriate suitable samples of security process are provided for guidelines. It is the responsibility of the organizations to develop internal processes that meet the guidelines set forth in this document.

---

15. Substituted by G.S.R. 902(E), dated 22-11-2003, for the words "Bank Guarantee/Performance Bond" (w.e.f. 27-11-2003).

The following words used in the Information Technology Security Guidelines shall be interpreted as follows:

- shall: The guideline defined is a mandatory requirement, and therefore must be complied with.
- should: The guideline defined is a recommended requirement. Non-compliance shall be documented and approved by the management. Where appropriate, compensating controls shall be implemented.
- must: The guideline defined is a mandatory requirement, and therefore must be complied with.
- may: The guideline defined is an optional requirement. The implementation of this guideline is determined by the organisation's requirement.

2. Implementation of an Information Security Programme

Successful implementation of a meaningful Information Security Programme rests with the support of the top management. Until and unless the senior managers of the organization understand and concur with the objectives of the information security programme its ultimate success is in question.

The Information Security Programme should be broken down into specific stages as follows:

a. Adoption of a security policy;
b. Security risk analysis;
c. Development and implementation of a information classification system;
d. Development and implementation of the security standards manual;
e. Implementation of the management security self-assessment process;
f. On-going security programme maintenance and enforcement; and
g. Training.

The principal task of the security implementation is to define the responsibilities of persons within the organization. The implementation should be based on the general principle that the person who is generating the information is also responsible for its security. However, in order to enable him to carry out his responsibilities in this regard, proper tools, and environment need to be established.

When different pieces of information at one level are integrated to form higher value information, the responsibility for its security needs also should go up in the hierarchy to the integrator and should require higher level of authority for its access. It should be absolutely clear with respect to each information as to who is its owner, its custodian, and its users. It is the duty of the owner to assign the right classification to the information so that the required level of security can be enforced. The custodian of information is responsible for the proper implementation of security guidelines and making the information available to the users on a need to know basis.

3. Information Classification

Information assets must be classified according to their sensitivity and their importance to the organization. Since it is unrealistic to expect managers and employees to maintain absolute control over all information within the boundaries of the organization, it is necessary to advise them on which types of information are considered more sensitive, and how the organization would like the sensitive information handled and protected. Classification, declassification, labeling, storage, access, destruction and reproduction of classified data and the administrative overhead this process will create must be considered. Failure to maintain a balance between the value of the information classified and the administrative burden the classification system places on the organization will result in long-term difficulties in achieving success.

Confidential is that classification of information of which unauthorized disclosure/use could cause serious damage to the organization, *e.g.* strategic planning documents.

Restricted is that classification of information of which unauthorized disclosure/use would not be in the best interest of the organization and/or its customers, *e.g.* design details, computer software (programs, utilities), documentation, organization personnel data, budget information.

Internal use is that classification of information that does not require any degree of protection against disclosure within the company, *e.g.* operating procedures, policies and standards inter office memorandums.

Unclassified is that classification of information that requires no protection against disclosure *e.g.* published annual reports, periodicals.

While the above classifications are appropriate for a general organization view point, the following classifications may be considered :

Top Secret: It shall be applied to information unauthorized disclosure of which could be expected to cause exceptionally grave damage to the national security or national interest. This category is reserved for Nation's closest secrets and to be used with great reserve.

Secret: This shall be applied to information unauthorized disclosure of which could be expected to cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

Confidentiality: This shall be applied to information unauthorized disclosure of which could be expected to cause damage to the security of the organisation or could be prejudicial to the interest of the organisation, or could affect the organisation in its functioning. Most information will on proper analysis be classified no higher than confidential.

Restricted: This shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose.

Unclassified: This is the classification of information that requires no protection against disclosure.

4. Physical and Operational Security

4.1 Site Design

1. The site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions.
2. As per nature of the operations, suitable floor structuring, lighting, power and water damage protection requirements shall be provided.
3. Construction shall comply with all applicable building and safety regulations as laid down by the relevant Government agencies. Further, the construction must be tamper-evident.
4. Materials used for the construction of the operational site shall be fire-resistant and free of toxic chemicals.
5. External walls shall be constructed of brick or reinforced concrete of sufficient thickness to resist forcible attack. Ground level windows shall be fortified with sturdy mild steel grills or impact-resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper-evident.
6. Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All ducting holes of the air-conditioning system must be designed so as to prevent intrusion of any kind.

7. Automatic fire detection, fire suppression systems and equipment in compliance with requirement specified by the Fire Brigade or any other agencies of the Central or State Government shall be installed at the operational site.
8. Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.
9. Any facility that supports mission-critical and sensitive applications must be located and designed for repairability, relocation and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity/ disaster recovery plan.

4.2 Fire Protection

1. Combustible materials shall not be stored within hundred meters of the operational site.
2. Automatic fire detection, fire suppression systems and audible alarms as prescribed by the Fire Brigade or any other agency of the Central or State Government shall be installed at the operational site.
3. Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.
4. Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems shall be carried out.
5. Procedures for the safe evacuation of personnel in an emergency shall be visibly pasted/displayed at prominent places at the operational site. Periodic training and fire drills shall be conducted.
6. There shall be no eating, drinking or smoking in the operational site. The work areas shall be kept clean at all times.

4.3 Environmental Protection

1. Water detectors shall be installed under the raised floors throughout the operational site and shall be connected to audible alarms.
2. The temperature and humidity condition in the operational site shall be monitored and controlled periodically.
3. Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.
4. Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.

4.4 Physical Access

1. Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals.
2. Biometric physical access security systems shall be installed to control and audit access to the operational site.
3. Physical access to the operational site at all times shall be controlled and restricted to authorised personnel only. Personnel authorized for limited physical access shall not be allowed to gain unauthorized access to restricted area within operational site.

4. Dual control over the inventory and issue of access cards/keys during normal business hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for a period of three years.
5. Loss of access cards/keys must be immediately reported to the security supervisor of the operational site who shall take appropriate action to prevent unauthorised access.
6. All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.
7. Emergency exits shall be tested periodically to ensure that the access security systems are operational.
8. All opening of the Data Centre should be monitored round the clock by surveillance video cameras.

5. Information Management

5.1 System Administration

1. Each organization shall designate a properly trained "System Administrator" who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Depending upon the complexity and security needs of a system or application, the System Administrator may have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for information.
2. Organisations shall ensure that only a properly trained System Security Administrator is assigned the system security responsibilities.
3. The responsibility to create, classify, retrieve, modify, delete or archive information must rest only with the System Administrator.
4. Any password used for the system administration and operation of trusted services must not be written down (in paper or electronic form) or shared with any one. A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator (or System Security Administrator) leaving the organization. Every instance of usage of administrator's passwords must be documented.
5. Periodic review of the access rights of all users must be performed.
6. The System Administrator must promptly disable access to a user's account if the user is identified as having left the Data Centre, changed assignments, or is no longer requiring system access. Reactivation of the user's account must be authorized in writing by the System Administrator (Digitally signed e-mail may be acceptable).
7. The System Administrator must take steps to safeguards classified information as prescribed by its owner.
8. The System Administrator must authorize privileged access to users only on a need-to-know and need-to-do basis and also only after the authorization is documented.
9. Criteria for the review of audit trails/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented.

10. All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.
11. The System Administrator together with the system support staff, shall conduct a regular analysis of problems reported to and identify any weaknesses in protection of the information.
12. The System Administrator shall ensure that the data, file and Public Key Infrastructure (PKI) servers are not left unmonitored while these systems are powered on.
13. The System Administrator should ensure that no generic user is enabled or active on the system.

5.2 Sensitive Information Control

1. Information assets shall be classified and protected according to their sensitivity and criticality to the organization.
2. Procedures in accordance with para 8.3 of these Guidelines must be in place to handle the storage media, which has sensitive and classified information.
3. All sensitive information stored in any media shall bear or be assigned an appropriate security classification.
4. All sensitive material shall be stamped or labeled accordingly.
5. Storage media (*i.e.* floppy diskettes, magnetic tapes, portable hard disks, optical disks, *etc.*) containing sensitive information shall be secured according to their classification.
6. Electronic communication systems, such as router, switches, network device and computers, used for transmission of sensitive information should be equipped or installed with suitable security software and if necessary with an encryptor or encryption software. The appropriate procedure in this regard should be documented.
7. Procedures shall be in place to ensure the secure disposal of sensitive information assets on all corrupted/damaged or affected media both internal (*e.g.* hard disk/optical disk) and external (*e.g.* diskette, disk drive, tapes *etc.*) to the system. Preferably such affected/corrupted/damaged media both internal and external to the system shall be destroyed.

5.3 Sensitive Information Security

1. Highly sensitive information assets shall be stored on secure removable media and should be in an encrypted format to avoid compromise by unauthorized persons.
2. Highly sensitive information shall be classified in accordance with para 3.
3. Sensitive information and data, which are stored on the fixed disk of a computer shared by more than one person, must be protected by access control software (*e.g.*, password). Security packages must be installed which partition or provide authorization to segregated directories/files.
4. Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.
5. Removable electronic storage media containing sensitive information and data must be clearly labeled and secured.
6. Hard disks containing sensitive information and data must be securely erased prior to giving the computer system to another internal or external department or for maintenance.

5.4 Third Party Access

1. Access to the computer systems by other organisations shall be subjected to a similar level of security protection and controls as in these Information Technology security guidelines.
2. In case the Data Centre uses the facilities of external service/facility provider (outsourcer) for any of their operations, the use of external service/facility providers (*e.g.* outsourcer) shall be evaluated in light of the possible security exposures and risks involved and all such agreements shall be approved by the information asset owner. The external service or facility provider shall also sign non-disclosure agreements with the management of the Data Centre/operational site.
3. The external service/facility provider (*e.g.* outsourcer) shall provide an equivalent level of security controls as required by these Information Technology Security Guidelines.

5.5 Prevention of Computer Misuse

1. Prevention, detection, and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.
2. Each organization shall provide adequate information to all persons, including management, systems developers and programmers, end-users, and third party users warning them against misuse of computers.
3. Effective measures to deal expeditiously with breaches of security shall be established within each organisation. Such measures shall include :
    i. Prompt reporting of suspected breach;
    ii. Proper investigation and assessment of the nature of suspected breach;
    iii. Secure evidence and preserve integrity of such material as relates to the discovery of any breach;
    iv. Remedial measures.
4. All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence.
5. Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence. Such procedures shall include:
    i. The role of the System Administrator, System Security Administrator and management;
    ii. Procedure for investigation;
    iii. Areas for security review; and
    iv. Subsequent follow-up action.

6. System integrity and security measures

6.1 Use of Security Systems or Facilities

1. Security controls shall be installed and maintained on each computer system or computer node to prevent unauthorised users from gaining entry to the information system and to prevent unauthorised access to data.
2. Any system software or resource of the computer system should only be accessible after being authenticated by access control system.

6.2 System Access Control

1. Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorise issuance of user identification (ID) and resource privileges.
2. Access to information system resources like memory, storage devices *etc.*, sensitive utilities and data resources and programme files shall be controlled and restricted based on a "need-to-use" basis with proper segregation of duties.
3. The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as "administrator" or "president" or "game" *etc.* to protect access to the system and data resources represent a security exposure and shall be avoided. All passwords used must be resistant to dictionary attacks.
4. Appropriate approval for the request to access system resources shall be obtained from the System Administrator. Guidelines and procedures governing access authorisations shall be developed, documented and implemented.
5. An Access Control System manual documenting the access granted to different level of users shall be prepared to provide guidance to the System Administrator for grant of access.
6. Each user shall be assigned a unique user ID. Adequate user education shall be provided to help users in password choice and password protection. Sharing of user IDs shall not be allowed.
7. Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorised disclosure and modification.
8. Stored passwords shall be protected by access controls from unauthorised disclosure and modification.
9. Automatic time-out for terminal inactivity should be implemented.
10. Audit trail of security-sensitive access and actions taken shall be logged.
11. All forms of audit trail shall be appropriately protected against unauthorised modification or deletion.
12. Where a second level access control is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.
13. Activities of all remote users shall be logged and monitored closely.
14. The facility to login as another user from one user's login shall be denied. However, the system should prohibit direct login as a trusted user (*e.g.* root in Unix, administrator in Windows NT or Windows 2000). This means that there must be a user account configured for the trusted administrator. The system requires trusted users to change their effective username to gain access to root and to re-authenticate themselves before requesting access to privileged functions.
15. The startup and shutdown procedure of the security software must be automated.
16. Sensitive Operating System files, which are more prone to hackers must be protected against all known attacks using proven tools and techniques. That is to say no user will be able to modify them except with the permission of System Administrator.

6.3 Password Management

(1) Certain minimum quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords:—

i. Minimum of eight characters without leading or trailing blanks;

ii. Shall be different from the existing password and the two previous ones;

iii. Shall be changed at least once every ninety days; for sensitive system, password shall be changed at least once every thirty days; and

iv. Shall not be shared, displayed or printed.

(2) Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.

(3) Passwords which are easy-to-guess (*e.g.* user name, birth date, month, standard words *etc.*) should be avoided.

(4) Initial or reset passwords must be changed by the user upon first use.

(5) Passwords shall always be encrypted in storage to prevent unauthorized disclosure.

(6) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

6.4 Privileged User's Management

1. System privileges shall be granted to users only on a need-to-use basis.
2. Login privileges for highly privileged accounts should be available only from Console and terminals situated within Console room.
3. An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by operator who is independent of System Administrator.
4. Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.
5. Separate user IDs shall be allowed to the user for performing privileged and normal (non-privileged) activities.
6. The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

6.5 User's Account Management

(1) Procedures for user account management shall be established to control access to application systems and data. The procedures shall include the following:

i. Users shall be authorised by the computer system owner to access the computer services.

ii. A written statement of access rights shall be given to all users.

iii. All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.

iv. Where access to computer services is administered by service providers, ensure that the service providers do not provide access until the authorization procedures have been completed. This includes the acknowledgement of receipt of the accounts by the users.

v. A formal record of all registered users of the computer services shall be maintained.

vi. Access rights of users who have been transferred, or left the organisation shall be removed immediately.

vii. A periodic check shall be carried out for redundant user accounts and access rights that are no longer required.

viii. Ensure that redundant user accounts are not re-issued to another user.

(2) User accounts shall be suspended under the following conditions:

(i) when an individual is on extended leave or inactive use of over thirty days. In case of protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator.

(ii) immediately upon the termination of the services of an individual.

(iii) suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.

6.6 Data and Resource Protection

1. All information assets shall be assigned an "owner" responsible for the integrity of that data/resource. Custodians shall be assigned and shall be jointly responsible for information assets by providing computer controls to assist owners.
2. The operating system or security system of the computer system shall:
   (i) Define user authority and enforce access control to data within the computer system;
   (ii) Be capable of specifying, for each named individual, a list of named data objects (*e.g.* file, programme) or groups of named objects, and the type of access allowed.
3. For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks.
4. Access controls for any data and/or resources shall be determined as part of the systems analysis and design process.
5. Application Programmer shall not be allowed to access the production system.

7. Sensitive Systems Protection

1. Security tokens/smart cards/bio-metric technologies such as Iris recognition, finger print verification technologies *etc.* shall be used to complement the usage of passwords to access the computer system.
2. For computer system processing sensitive data, access by other organisations shall be prohibited or strictly controlled.
3. For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

8. Data Centre Operations Security

8.1 Job Scheduling

1. Procedures shall be established to ensure that all changes to the job schedules are appropriately approved. The authority to approve changes to job schedules shall be clearly assigned.
2. As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.

8.2 System Operations Procedure

1. Procedures shall be established to ensure that only authorised and correct job stream and parameter changes are made.

2. Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent independent party for indications of dubious activities. Appropriate retention periods shall be set for such logs.
3. Procedures shall be established to ensure that people other than well-trained computer operators are prohibited from operating the computer equipment.
4. Procedures shall be implemented to ensure the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owners for each system.

8.3 Media Management

1. Responsibilities for media library management and protection shall be clearly defined and assigned.
2. All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of toxic chemicals.
3. Access to the media library (both on-site and off-site) shall be restricted to the authorized persons only. A list of personnel authorised to enter the library shall be maintained.
4. The media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached in few hours.
5. A media management system shall be in place to account for all media stored on-site and off-site.
6. All incoming/outgoing media transfers shall be authorised by management and users.
7. An independent physical inventory check of all media shall be conducted at least every six months.
8. All media shall have external volume identification. Internal labels shall be fixed, where available.
9. Procedures shall be in place to ensure that only authorised addition/removal of media from the library is allowed.
10. Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

8.4 Media Movement

1. Proper records of all movements of computer tapes/disks between on-site and off-site media library must be maintained.
2. There shall be procedures to ensure the authorized and secure transfer to media to/from external parties and the off-site location. A means to authenticate the receipt shall be in place.
3. Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation.

9. Data Backup and Off-site Retention

1. Back-up procedures shall be documented, scheduled and monitored.
2. Up-to-date backups of all critical items shall be maintained to ensure the continued provision of the minimum essential level of service. These items include:
   i. Data files
   ii. Utilities programmes

iii. Databases
iv. Operating system software
v. Applications system software
vi. Encryption keys
vii. Pre-printed forms
viii. Documentation (including a copy of the business continuity plans)

3. One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.
4. Backups of the system, application and data shall be performed on a regular basis. Backups should also be made for application under development and data conversion efforts.
5. Data backup is required for all systems including personal computers, servers and distributed systems and databases.
6. Critical system data and file server software must have full backups taken weekly.
7. The backups must be kept in an area physically separate from the server. If critical system data on the LAN represents unique versions of the information assets, then the information backups must be rotated on a periodic basis to an off-site storage location.
8. Critical system data and file server software must have incremental backups taken daily.
9. Systems that are completely static may not require periodic backup, but shall be backed up after changes or updates in the information.
10. Each LAN/system should have a primary and backup operator to ensure continuity of business operations.
11. The business recovery plan should be prepared and tested on an annual basis.

10. Audit Trails and Verification

1. Transactions that meet exception criteria shall be completely and accurately high-lighted and reviewed by personnel independent of those that initiate the transaction.
2. Adequate audit trails shall be captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (*e.g.* repeated unsuccessful logons, access attempts over a series of days) shall be analyzed. This information includes such information as who, what, when, where, and any special information such as:
   i. Success or failure of the event
   ii. Use of authentication keys, where applicable
3. Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of-pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include:
   (i) Significant computer system events (*e.g.* configuration updates, system crashes)
   (ii) Security profile changes
   (iii) Actions taken by computer operations, system administrators, system programmers, and/or security administrators

4. The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.
5. The real time clock of the computer or communications device shall be set to Indian Standard Time (IST). Further there shall be a procedure that checks and corrects drift in the real time clock.
6. Computer system access records shall be kept for a minimum of two years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behaviour, shall be retained as per laws of the land.
7. Computer records of applications transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements.

11. Measures to Handle Computer Virus

(1) Responsibilities and duties shall be assigned to ensure that all file servers and personal computers are equipped with up-to-date virus protection and detection software.

(2) Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis.

(3) All diskettes and software shall be screened and verified by virus detection software before being loaded onto the computer system. No magnetic media like tape cartridge, floppies *etc.* brought from outside shall be used on the data, file, PKI or computer server or personal computer on Intranet and Internet without proper screening and verification by virus detection software.

(4) A team shall be designated to deal with reported or suspected incidents of computer virus. The designated team shall ensure that latest version of anti-virus software is loaded on all data, file, PKI servers and personal computers.

(5) Procedures shall be established to limit the spread of viruses to other organization information assets. Such procedures *inter alia* shall include:

i. Communication to other business partners and users who may be at risk from an infected resource
ii. Eradication and recovery procedures
iii. Incident report must be documented and communicated per established procedures.

(6) An awareness and training programme shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities.

12. Relocation of Hardware and Software

Whenever computers or computer peripherals are relocated (*e.g.* for maintenance, installation at different sites or storage), the following guidelines shall apply:

i. All removable media will be removed from the computer system and kept at secure location.
ii. Internal drives will be overwritten, reformatted or removed as the situation may be.
iii. If applicable, ribbons will be removed from printers.
iv. All paper will be removed from printers.

13. Hardware and Software Maintenance

Whenever, the hardware and software maintenance of the computer or computer network is being carried out, the following should be considered:

1. Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.
2. Maintenance of an inventory and configuration chart of hardware.
3. Identification and use of security features implemented within hardware.
4. Authorization, documentation, and control of change made to the hardware.
5. Identification of support facilities including power and air conditioning.
6. Provision of an uninterruptible power supply.
7. Maintenance of equipment and services.
8. Organisation must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them. It shall be the responsibility of the officer in charge of the operational site to ensure that contract for annual maintenance of hardware is always in place.
9. Organisation must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.
10. Maintenance personnel will sign non-disclosure agreements.
11. The identities of all hardware and software vendor maintenance staff should be verified before allowing them to carry out maintenance work.
12. All maintenance personnel should be escorted within the operational site/computer system and network installation room by the authorized personnel of the organisation.
13. After maintenance, any exposed security parameters such as passwords, user IDs, and accounts will be changed or reset to eliminate any potential security exposures.
14. If the computer system, computer network or any of its devices is vulnerable to computer viruses as a result of performing maintenance, system managers or users shall scan the computer system and its devices and any media affected for viruses as a result of maintenance.

14. Purchase and Licensing of Hardware and Software

1. Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organisation system or network, must be verified to comply with these Information Technology Security Guidelines prior to the signing of any contract, purchase or lease.
2. Software, which is capable of bypassing or modifying the security system or operating system, integrity features, must be verified to determine that they conform to these Information Technology Security Guidelines. Where such compliance is not possible, then procedures shall be in place to ensure that the implementation and operation of that software does not compromise the security of the system.
3. There shall be procedures to identify, select, implement and control software (system and application software) acquisition and installation to ensure compliance with the Indian Copyright Act and Information Technology Security Guidelines.
4. It is prohibited to knowingly install on any system whether test or production, any software which is not licensed for use on the specific systems or networks.
5. No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which the user has documented permission to install and test the software under evaluation.
6. Illegally acquired or unauthorized software must not be used on any computer, computer network or data communication equipment. In the event that any illegally

acquired or unauthorized software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

15. System Software

1. All system software options and parameters shall be reviewed and approved by the management.
2. System software shall be comprehensively tested and its security functionality validated prior to implementation.
3. All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.
4. Versions of system software installed on the computer system and communication devices shall be regularly updated.
5. All changes proposed in the system software must be appropriately justified and approved by an authorised party.
6. A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.
7. Procedures to control changes initiated by vendors shall be in accordance with para 21 pertaining to "Change Management".
8. There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.
9. System Programmers shall not be allowed to have access to the application system's data and programme files in the production environment.
10. Procedures to control the use of sensitive system utilities and system programmes that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities.

16. Documentation Security

1. All documentation pertaining to application software and sensitive system software and changes made therein shall be updated to the current time, accurately and stored securely. An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.
2. All documentation and subsequent changes shall be reviewed and approved by an independent authorised party prior to issue.
3. Access to application software documentation and sensitive system software documentation shall be restricted to authorised personnel on a "need-to-use" basis only.
4. Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals shall be stored off-site.
5. Documentation shall be classified according to the sensitivity of its contents/ implications.
6. Organisations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorised access, loss of and damage to information outside normal working hours.

17. Network Communication Security

1. All sensitive information on the network shall be protected by using appropriate techniques. The critical network devices such as routers, switches and modems should be protected from physical damage.
2. The network configuration and inventories shall be documented and maintained.

3. Prior authorization of the Network Administrator shall be obtained for making any changes to the network configuration. The changes made in the network configuration shall be documented. The threat and risk assessment of the network after changes in the network configuration shall be reviewed. The network operation shall be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.
4. Physical access to communications and network sites shall be controlled and restricted to authorized individuals only in accordance with para 4.4 pertaining to "Physical Access".
5. Communication and network systems shall be controlled and restricted to authorized individuals only in accordance with para 6.2 – System Access Control.
6. As far as possible, transmission medium within the Certifying Authority's operational site should be secured against electro magnetic transmission. In this regard, use of Optical Fibre Cable and armoured cable may be preferred as transmission media as the case may be.
7. Network diagnostic tools, *e.g.*, spectrum analyzer, protocol analyzer should be used on a need basis.

18. Firewalls

1. Intelligent devices generally known as "Firewalls" shall be used to isolate organisation's data network with the external network. Firewall device should also be used to limit network connectivity for unauthorized use.
2. Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls. The internal network of the organization shall be physically and logically isolated from the internet and any other external connection by a firewall.
3. All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.
4. All web servers for access by internet users shall be isolated from other data and host servers.

19. Connectivity

1. Organisation shall establish procedure for allowing connectivity of their computer network or computer system to non-organisation computer system or networks. The permission to connect other networks and computer system shall be approved by the Network Administrator and documented.
2. All unused connections and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an organisation's host system must adhere to the general system security and access control guidelines.
3. The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organisation's network.
4. As far as possible, no internet access should be allowed to database server/file server or server hosting sensitive data.
5. The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

20. Network Administrator

1. Each organization shall designate a properly trained "Network Administrator" who will be responsible for operation, monitoring security and functioning of the network.

2. Network Administrator shall regularly undertake the review of network and also take adequate measures to provide physical, logical and procedural safeguards for its security. Appropriate follow up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator.
3. System must include a mechanism for alerting the Network Administrator of possible breaches in security, *e.g.*, unauthorized access, virus infection and hacking.
4. Secure Network Management System should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimized.
5. Only authorized and legal software shall be used on the network.
6. Shared computer systems, network devices used for business applications shall comply with the requirement established in para 6 – System Integrity and Security Measures.

21. Change Management

21.1 Change Control

1. Procedures for tracking and managing changes in application software, system software, hardware and data in the production system shall be established. Organisational responsibilities for the change management process shall be defined and assigned.
2. A risk and impact analysis, classification and prioritisation process shall be established.
3. No changes to a production system shall be implemented until such changes have been formally authorised. Authorisation procedures for change control shall be defined and documented.
4. Owners/Users shall be notified of all changes made to production system which may affect the processing of information on the said production system.
5. Fall-back procedures in the event of a failure in the implementation of the change process shall be established and documented.
6. Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation shall be documented and implemented.
7. Version changes of application software and all system software installed on the computer systems and all communication devices shall be documented. Different versions of application software and system software must be kept in safe custody.

21.2 Testing Of Changes To Production System

1. All changes in computer resource proposed in the production system shall be tested and the test results shall be reviewed and accepted by all concerned parties prior to implementation.
2. All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment which includes: (i) Test objectives, (ii) A documented test plan, and (iii) acceptance criteria.

21.3 Review Of Changes

1. Procedures shall be established for an independent review of programme changes before they are moved into a production environment to detect unauthorised or malicious codes.

2. Procedures shall be established to schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning.
3. All emergency changes/fixes in computer resource in the production system shall be reviewed and approved.
4. Periodic management reports on the status of the changes implemented in the computer resource in the production system shall be submitted for management review.

22. Problem Management and Reporting

1. Procedures for identifying, reporting and resolving problems, such as non-functioning of Certifying Authority's system; breaches in Information Technology security; and hacking, shall be established and communicated to all personnel concerned. It shall include emergency procedures. Periodic reports shall be submitted for management review.
2. A help desk shall be set up to assist users in the resolution of problems.
3. A system for recording, tracking and reporting the status of reported problems shall be established to ensure that they are promptly managed and resolved with minimal impact on the user of the computing resource.

23. Emergency Preparedness

1. Emergency response procedures for all activities connected with computer operation shall be developed and documented. These procedures should be reviewed periodically.
2. Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.

24. Contingency Recovery Equipment and Services

1. Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility.
2. The business continuity plan shall be developed which inter alia include the procedures for emergency ordering of the equipment and availability of the services.
3. The need for backup hardware and other peripherals should be evaluated in accordance to business needs.

25. Security Incident Reporting and Response

1. All security related incidents must be reported to a central coordinator, appointed by the management to coordinate and handle security related incidents. This central coordinator shall be the single point of contact at the organization.
2. All incidents reported, actions taken, follow-up actions, and other related information shall be documented.
3. Procedures shall be defined for dealing with all security related incidents, including malicious software, break-ins from networks, software bugs which compromised the security of the system.

26. Disaster Recovery/Management

(1) Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the facility, essential level of service will be provided. The disaster recovery framework should include:

(a) emergency procedures, describing the immediate action to be taken in case of a major incident

(b) fall back procedure, describing the actions to be taken to relocate essential activities or support services to a backup site

(c) restoration procedures, describing the action to be taken to return to normal operation at the original site

(2) The documentation should include:

(a) definition of a disaster;

(b) condition for activating the plan;

(c) stages of a crisis;

(d) who will make decisions in the crisis;

(e) role of individuals for each component of the plan;

(f) composition of the recovery team; and

(g) decision making process for return to normal operation.

(3) Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.

(4) Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster.

(5) Each component/aspect of the plan should have a person and a backup assigned to its execution.

(6) Periodic training of personnel and users associated with computer system and network should be conducted defining their roles and responsibilities in the event of a disaster.

(7) Test plan shall be developed, documented and maintained. Periodic tests shall be carried out to test the effectiveness of the procedures in the plan. The results of the tests shall be documented for management review.

(8) Disaster recovery plan should be updated regularly to ensure its continuing effectiveness.

SCHEDULE-III

[*See* rule 19(2)]

Security Guidelines for Certifying Authorities

1. Introduction

This document prescribes security guidelines for the management and operation of Certifying Authorities (CAs) and is aimed at protecting the integrity, confidentiality and availability of their services, data and systems. These guidelines apply to Certifying Authorities that perform all the functions associated with generation, issue and management of Digital Signature Certificate such as:

1. Verification of registration, suspension and revocation request;
2. Generation, issuance, suspension and revocation of Digital Signature Certificates; and
3. Publication and archival of Digital Signature Certificates, suspension and revocation of information.

2. Security Management

The Certifying Authority shall define Information Technology security policies for its operation on the lines defined in Schedule-II and Schedule-III. The policy shall be

communicated to all personnel and widely published throughout the organisation to ensure that the personnel follow the policies.

3. Physical controls – site location, construction and physical access

1. The site location, design, construction and physical security of the operational site of Certifying Authority shall be in accordance with para 4 of the Information Technology Security Guidelines given at Schedule-II.
2. Physical access to the operational site housing computer servers, PKI server, communications and network devices shall be controlled and restricted to the authorized individuals only in accordance with para 4.4 of the Information Technology Security Guidelines given at Schedule-II.
3. A Certifying Authority must:
    i. ensure that the operational site housing PKI servers, communications and networks is protected with fire suppression system in accordance with para 4.2 of the Information Technology Security Guidelines given at Schedule-II.
    ii. ensure that power and air-conditioning facilities are installed in accordance with para 4.1 of the Information Technology Security Guidelines given at Schedule-II.
    iii. ensure that all removable media and papers containing sensitive or plain text information are listed, documented and stored in a container properly identified.
    iv. ensure unescorted access to Certifying Authority's server is limited to those personnel identified on an access list.
    v. ensure that the exact location of Digital Signature Certification System shall not be publicly identified.
    vi. ensure that access security system is installed to control and audit access to the Digital Signature Certification System.
    vii. ensure that dual control over the inventory and access cards/keys are in place.
    viii. ensure that up-to-date list of personnel who possess the access cards/keys is maintained at the Certifying Authority's operational site. Loss of access cards/keys shall be reported immediately to the Security Administrator; who shall take appropriate actions to prevent unauthorised access.
    ix. ensure personnel not on the access list are properly escorted and supervised.
    x. ensure a site access log is maintained at the Certifying Authority's operational site and inspected periodically.
4. Multi-tiered access mechanism must be installed at the Certifying Authority's operational site. The facility should have clearly laid out security zones within its facility with well-defined access rights to each security zone. Each security zone must be separated from the other by floor to ceiling concrete reinforced walls. Alarm and intrusion detection system must be installed at every stage with adequate power backup capable of continuing operation even in the event of loss of main power. Electrical/Electronic circuits to external security alarm monitoring service (if used) must be supervised. No single person must have complete access to PKI Server, root keys or any computer system or network device on his/her own.
5. Entrance to the main building where the Certifying Authority's facilities such as Data Centre, PKI Server and Network devices are housed and entrance to each security zone must be video recorded round the clock. The recording should be carefully scrutinized and maintained for at least one year.

6. A Certifying Authority site must be manually or electronically monitored for unauthorised intrusion at all times in accordance with the Information Technology Security Guidelines given at Schedule-II.
7. Computer System/PKI Server performing Digital Signature Certification function shall be located in a dedicated room or partition to facilitate enforcement of physical access control. The entry and exit of the said room or partition shall be automatically locked with time stamps and shall be reviewed daily by the Security Administrator.
8. Access to infrastructure components essential to operation of Certifying Authority such as power control panels, communication infrastructure, Digital Signature Certification system, cabling, etc. shall be restricted to authorised personnel.
9. By-pass or deactivation of normal physical security arrangements shall be authorised and documented by security personnel.
10. Intrusion detection systems shall be used to monitor and record physical access to the Digital Signature Certification system during and after office hours.
11. Computer System or PKI Server performing the Digital Signature Certification functions shall be dedicated to those functions and should not be used for any other purposes.
12. System software shall be verified for integrity in accordance with para 15 of the Information Technology Security Guidelines given at Schedule-II.

4. Media Storage

A Certifying Authority must ensure that storage media used by his system are protected from environment threats such as temperature, humidity and magnetic and are transported and managed in accordance with para 8.3 and para 8.4 of the Information Technology Security Guidelines given at Schedule-II.

5. Waste Disposal

All media used for storage of information pertaining to all functions associated with generation, production, issue and management of Digital Signature Certificate shall be scrutinized before being destroyed or released for disposal.

6. Off-site Backup

A Certifying Authority must ensure that facility used for off-site backup, if any, shall be within the country and shall have the same level of security as the primary Certifying Authority site.

7. Change and Configuration Management

1. The components of the Certifying Authority infrastructure (*e.g.* cryptographic algorithm and its key parameters, operating system, system software, computer system, PKI server, firewalls, physical security, system security *etc.*) shall be reviewed every year for new technology risks and appropriate action plan shall be developed to manage the risks identified for each component.
2. The application software, system software and hardware, which are procured from questionable sources, shall not be installed and used for any function associated with generation and management of Digital Signature Certificate.
3. Software updates and patches shall be reviewed for security implications before being implemented on Certifying Authority's system.
4. Software updates and patches to rectify security vulnerability in critical systems used for Certifying Authority's operation shall be promptly reviewed and implemented.

5. Information on the software updates and patches and their implementation on Certifying Authority's system shall be clearly and properly documented.

8. Network and Communications Security

1. Certifying Authority's systems shall be protected to ensure network access control to critical systems and services from other systems in accordance with para 17, para 18, para 19 and para 20 of the Information Technology Security Guidelines given at Schedule-II.
2. Network connections from the Certifying Authority's system to external networks shall be restricted to only those connections which are essential to facilitate Certifying Authority's functional processes and services. Such network connections to the external network shall be properly secured and monitored regularly.
3. Network connections should be initiated by the systems performing the functions of generation and management of Digital Signature Certificate to connect those systems performing the registration and repository functions but not *vice versa*. If this is not possible, compensating controls (*e.g.* use of proxy servers) shall be implemented to protect the systems performing the function of generation and management of Digital Signature Certificate from potential attacks.
4. Systems performing the Digital Signature Certification function should be isolated to minimise their exposure to attempts to compromise the confidentiality, integrity and availability of the certification function.
5. Communication between the Certifying Authority systems connected on a network shall be secure to ensure confidentiality and integrity of the information. For example, communications between the Certifying Authority's systems connected on a network should be encrypted and digitally signed.
6. Intrusion detection tools should be deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner.

9. System Security Audit Procedures

9.1 Types of event recorded

(1) The Certifying Authority shall maintain record of all events relating to the security of his system. The records should be maintained in audit log file and shall include such events as:

i. System start-up and shutdown;
ii. Certifying Authority's application start-up and shutdown;
iii. Attempts to create, remove, set passwords or change the system privileges of the PKI Master Officer, PKI Officer, or PKI Administrator;
iv. Changes to keys of the Certifying Authority or any of his other details;
v. Changes to Digital Signature Certificate creation policies, *e.g.* validity period;
vi. Login and logoff attempts;
vii. Unauthorised attempts at network access to the Certifying Authority's system;
viii. Unauthorised attempts to access system files;
ix. Generation of own keys;
x. Creation and revocation of Digital Signature Certificates;

xi. Attempts to initialize remove, enable, and disable subscribers, and update and recover their keys;

xii. Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) directory.

(2) Monitoring and Audit Logs

(i) A Certifying Authority should consider the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time. Records of the following application transactions shall be maintained:

a. Registration;

b. Certification;

c. Publication;

d. Suspension; and

e. Revocation.

(ii) Records and log files shall be reviewed regularly for the following activities:

a. Misuse;

b. Errors;

c. Security violations;

d. Execution of privileged functions;

e. Change in access control lists;

f. Change in system configuration.

(3) All logs, whether maintained through electronic or manual means, should contain the date and time of the event, and the identity of the subscriber/subordinate/entity which caused the event.

(4) A Certifying Authority should also collect and consolidate, either electronically or manually, security information which may not be generated by his system, such as:

i. Physical access logs;

ii. System configuration changes and maintenance;

iii. Personnel changes;

iv. Discrepancy and compromise reports;

v. Records of the destruction of media containing key material, activation data, or personal subscriber information.

(5) To facilitate decision-making, all agreements and correspondence relating to services provided by Certifying Authority should be collected and consolidated, either electronically or manually, at a single location.

9.2 Frequency of Audit Log Monitoring

The Certifying Authority must ensure that its audit logs are reviewed by its personnel at least once every two weeks and all significant events are detailed in an audit log summary. Such reviews should involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken following these reviews must be documented.

9.3 Retention Period for Audit Log

The Certifying Authority must retain its audit logs onsite for at least twelve months and subsequently retain them in the manner described in para 10 of the Information Technology Security Guidelines as given in Schedule-II.

9.4 Protection of Audit Log

The electronic audit log system must include mechanisms to protect the log files from unauthorized viewing, modification, and deletion.

Manual audit information must be protected from unauthorised viewing, modification and destruction.

9.5 Audit Log Backup Procedures

Audit logs and audit summaries must be backed up or copied if in manual form.

9.6 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The Certifying Authority must ensure that a vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.

10. Records Archival

1. Digital Signature Certificates stored and generated by the Certifying Authority must be retained for at least seven year after the date of its expiration. This requirement does not include the backup of private signature keys.
2. Audit information as detailed in para 9, subscriber agreements, verification, identification and authentication information in respect of subscriber shall be retained for at least seven years.
3. A second copy of all information retained or backed up must be stored at three locations within the country including the Certifying Authority site and must be protected either by physical security alone, or a combination of physical and cryptographic protection. These secondary sites must provide adequate protection from environmental threats such as temperature, humidity and magnetism. The secondary site should be reachable in few hours.
4. All information pertaining to Certifying Authority's operation, Subscriber's application, verification, identification, authentication and Subscriber agreement shall be stored within the country. This information shall be taken out of the country only with the permission of Controller and where a properly constitutional warrant or such other legally enforceable document is produced.
5. The Certifying Authority should verify the integrity of the backups at least once every six months.
6. Information stored off-site must be periodically verified for data integrity.

11. Compromise and Disaster Recovery

11.1 Computing Resources, Software and/or Data are Corrupted

The Certifying Authority must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing and networking resources, nominated website, repository, software and/or data. Where a repository is not under the control of the Certifying Authority, the Certifying Authority must ensure that any agreement with the repository provides for business continuity procedures.

11.2 Secure facility after a natural or other type of disaster

The Certifying Authority must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of

disaster. Where a repository is not under the control of the Certifying Authority, the Certifying Authority must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

11.3 Incident Management Plan

An incident management plan shall be developed and approved by the management. The plan shall include the following areas:

i. Certifying Authority's certification key compromise;
ii. Hacking of systems and network;
iii. Breach of physical security;
iv. Infrastructure availability;
v. Fraudulent registration and generation of Digital Signature Certificates; and
vi. Digital Signature Certificate suspension and revocation information.

An incident response action plan shall be established to ensure the readiness of the Certifying Authority to respond to incidents. The plan should include the following areas:

i. Compromise control;
ii. Notification to user community; (if applicable)
iii. Revocation of affected Digital Signature Certificates; (if applicable)
iv. Responsibilities of personnel handling incidents;
v. Investigation of service disruption;
vi. Service restoration procedure;
vii. Monitoring and audit trail analysis; and
viii. Media and public relations.

12. Number of Persons Required Per Task

The Certifying Authority must ensure that no single individual may gain access to the Digital Signature Certificate server and the computer server maintaining all information associated with generation, issue and management of Digital Signature Certificate and private keys of the Certifying Authority. Minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, must perform any operation associated with generation, issue and management of Digital Signature Certificate and application of private key of the Certifying Authority.

13. Identification and Authentication for Each Role

All Certifying Authority personnel must have their identity and authorization verified before they are:

i. included in the access list for the Certifying Authority's site;
ii. included in the access list for physical access to the Certifying Authority's system;
iii. given a certificate for the performance of their Certifying Authority role;
iv. given an account on the PKI system.

Each of these certificates and accounts (with the exception of Certifying Authority's signing certificates) must:

i. be directly attributable to an individual;
ii. not be shared;
iii. be restricted to actions authorized for that role; and
iv. procedural controls.

Certifying Authority's operations must be secured using techniques of authentication and encryption, when accessed across-a shared network.

14. Personnel Security Controls

The Certifying Authority must ensure that all personnel performing duties with respect to its operation must:

i. be appointed in writing;

ii. be bound by contract or statute to the terms and conditions of the position they are to fill;

iii. have received comprehensive training with respect to the duties they are to perform;

iv. be bound by statute or contract not to disclose sensitive Certifying Authority's security related information or subscriber information;

v. not be assigned duties that may cause a conflict of interest with their Certifying Authority's duties; and

vi. be aware and trained in the relevant aspects of the Information Technology Security Policy and Security Guidelines framed for carrying out Certifying Authority's operation.

15. Training Requirements

A Certifying Authority shall ensure that all personnel performing duties with respect to its operation, must receive comprehensive training in:

i. relevant aspects of the Information Technology Security Policy and Security Guidelines framed by the Certifying Authority;

ii. all PKI software versions in use on the Certifying Authority's system;

iii. all PKI duties they are expected to perform; and

iv. disaster recovery and business continuity procedures.

16. Retraining Frequency and Requirements

The requirements of para 15 must be kept current to accommodate changes in the Certifying Authority's system. Refresher training must be conducted as and when required, and the Certifying Authority must review these requirements at least once a year.

17. Documentation Supplied to Personnel

A Certifying Authority must make available to his personnel the Digital Signature Certificate policies it supports, its Certification Practice Statement, Information Technology Security Policy and any specific statutes, policies or contracts relevant to their position.

18. Key Management

18.1 Generation

1. The subscriber's key pair shall be generated by the subscriber or on a key generation system in the presence of the subscriber.
2. The key generation process shall generate statistically random key values that are resistant to known attacks.

18.2 Distribution of Keys

Keys shall be transferred from the key generation system to the storage device (if the keys are not stored on the key generation system) using a secure mechanism that ensures confidentiality and integrity.

18.3 Storage

1. Certifying Authority's keys shall be stored in tamper-resistant devices and can only be activated under split-control by parties who are not involved in the set-up and maintenance of the systems and operations of the Certifying Authority. The key of the Certifying Authority may be stored in a tamper-resistant cryptographic module or split into sub-keys stored in tamper-resistant devices under the custody of the key custodians.
2. The Certifying Authority's key custodians shall ensure that the Certifying Authority's key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the Certifying Authority's management and documented.

18.4 Usage

1. A system and software integrity check shall be performed prior to Certifying Authority's key loading.
2. Custody of and access to the Certifying Authority's keys shall be under split control. In particular, Certifying Authority's key loading shall be performed under split control.

18.5 Certifying Authority's Public Key Delivery to Users

The Certifying Authority's public verification key must be delivered to the prospective Digital Signature Certificate holder in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or *via* an equally secure manner.

19. Private Key Protection and Backup

1. The Certifying Authority must protect its private keys from disclosure.
2. The Certifying Authority must back-up its private keys. Backed-up keys must be stored in encrypted form and protected at a level no lower than those followed for storing the primary version of the key.
3. The Certifying Authority's private key backups should be stored in a secure storage facility, away from where the original key is stored.

20. Method of Destroying Private Key

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over-writing. Private key destruction procedures must be described in the Certification Practice Statement or other publicly available document.

[16]**[21. Usage Periods for keys**–

(1) Certifying Authority and subscriber keys shall be changed periodically).

(2) Key change shall be processed as per Key Generation guidelines.

(3) The Certifying Authority shall provide reasonable notice to the Subscribers relying parties of any change to a new key pair used by the Certifying authority to sign Digital Signature Certificates.

(4) All Certifying Authorities key pairs and associated certificates must have validity period of no more than ten years.

(5) All subscriber's key pairs and associated certificates must have validity period of no more than three years.]

22. Confidentiality of Subscriber's Information

---

16. Substituted by G.S.R. 783(E), dated 25-10-2011 (w.e.f. 25-10-2011).

1. Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the Certifying Authority's custody shall be implemented. Confidential information provided by the subscriber must not be disclosed to a third party without the subscribers' consent, unless the information is required to be disclosed under the law or a court order.
2. Data on the usage of the Digital Signature Certificates by the subscribers and other transactional data relating to the subscribers' activities generated by the Certifying Authority in the course of its operation shall be protected to ensure the subscribers' privacy.
3. A secure communication channel between the Certifying Authority and its subscribers shall be established to ensure the authenticity, integrity and confidentiality of the exchanges (*e.g.* transmission of Digital Signature Certificate, password, private key) during the Digital Signature Certificate issuance process.

SCHEDULE-IV

[*See* rule 23].

[17][FORM A

APPLICATION FORM FOR ISSUE OF DIGITAL CERTIFICATE FOR SUBSCRIBER OF GOVERNMENT AND BANKING SECTOR

Class of certificate applied : Certificate

Individual/Server/Web server Required

Certificate Validity :

Name : _____

Email Address : _____

Office Address (with Designation : _____

and Department) (optional) : _____

Telephone : _____

Identification Details : Employee Identification No _____

Passport No. : _____

Any other

(Passport No./PAN Card No./Voter's ID Card No./ Driving License No./PF No.)

In case the application is for a device, then _____ Web Server _____

details of Server/De vice for which the _____ Services _____

certificate is being applied for must IP address _____

be filled: URL/Domain Name _____

Physical Location _____

Date:

17. Amended by G.S.R. 285(E), dated 23-4-2004

Place:

(Signature of the Applicant)

For Head of Office or JS (Admn.) for Government Sector /Superior Authority for Banking Sector of Applicant

This is to certify that Mr./Ms. _____has provided correct information in the "Application form for issue of Digital Certificate for subscriber of Government and Banking Sector" to the best of my knowledge and belief. I hereby authorize him/her, on behalf of my organization to apply for obtaining Digital Certificate from CA for the purpose specified above.

Date:

Place:

Name of Officer with Designation:

(Signature of Officer with stamp of Org./Office)

Office Email:

Important Notice:

- This application form is (o be filled by the applicant.
- All subscribers are advised to read Certificate Practice Statement of CA
- All document specified in CPS for each Certificate Class should be submitted with this application form.'
- Application form must be submitted in person.
- Incomplete/Inconsistent application is liable to be rejected.

FORM - B

APPLICATION FORM FOR ISSUE OF DIGITAL SIGNATURE CERTIFICATE FOR SUBSCRIBERS OTHER THAN GOVERNMENT AND BANKING SECTOR

Class of Certificate applied for Certificate Required : Individual/Server/Web Server

Certificate validity : _____

Name : _____

E-mail Address : _____

Office Address (with Designation and Department) (optional) : _____

Telephone : _____

Residential Address : _____

Telephone:

In case the application is for a device, then details of Server/Device for which the certificate is being applied for must

Web Server _____

Services _____

IP address _____

be filled.

URL/Domain Name _____

Physical Location _____

Date:

Place:

(Signature of the applicant)

Authentication of Identity and Proof of Residence

Copies of one or more of the following must be provided, as required by the Certifying Authority. Identity verification methods for the certificate applicant will be as per the procedure specified in the Certification Practice Statement (CPS) of the CA.

1. Passport
2. Election card (Voter's ID)
3. Ration Card
4. Bank Account Details
5. Driving Licence
6. Any Other

Important Notice:

— This application form is to be filled by the applicant.

— All subscribers are advised to read Certificate Practice Statement of CA

— All document specified in CPS for each Certificate Class must be accompanied with this application form.

— Application form must be submitted in person.

— Incomplete/Inconsistent application is liable to be rejected.]

SCHEDULE—V

Glossary

ACCEPT (A DIGITAL SIGNATURE CERTIFICATE)

To demonstrate approval of a Digital Signature Certificate by a Digital Signature Certificate applicant while knowing or having notice of its informational contents.

ACCESS

Gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

ACCESS CONTROL

The process of limiting access to the resources of a computer system only to authorized users, programs or other computer systems.

ACCREDITATION

A formal declaration by the Controller that a particular information system, professional or other employee or contractor, or organization is approved to perform certain duties and to operate in a specific security mode, using a prescribed set of safeguards.

AUTHORITY REVOCATION LIST (ARL)

A list of revoked Certifying Authority certificates. An ARL is a CRL for Certifying Authority cross-certificates.

ADDRESSEE

A person who is intended by the originator to receive the electronic record but does not include any intermediary.

AFFILIATED CERTIFICATE

A certificate issued to an affiliated individual. (See also affiliated individual)

AFFIRM / AFFIRMATION

To state or indicate by conduct that data is correct or information is true.

AFFIXING DIGITAL SIGNATURE

With its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

ALIAS–A PSEUDONYM.

APPLICANT (*see* CA APPLICANT; CERTIFICATE APPLICANT)

APPLICATION SOFTWARE

A software that is specific to the solution of an application problem. It is the software coded by or for an end user that performs a service or relates to the user's work.

APPLICATION SYSTEM

A family of products designed to offer solutions for commercial data processing, office, and communications environments, as well as to provide simple, consistent programmer and end user interfaces for businesses of all sizes.

ARCHIVE

To store records and associated journals for a given period of time for security, backup, or auditing purposes.

ASSURANCES

Statements or conduct intended to convey a general intention, supported by a good-faith effort, to provide and maintain a specified service. "Assurances" does not necessarily imply a guarantee that the services will be performed fully and satisfactorily. Assurances are distinct from insurance, promises, guarantees, and warranties, unless otherwise expressly indicated.

ASYMMETRIC CRYPTO SYSTEM

A system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

AUDIT

A procedure used to validate that controls are in place and adequate for their purposes. Includes recording and analyzing activities to detect intrusions or abuses into an information system. Inadequacies found by an audit are reported to appropriate management personnel.

AUDIT TRAIL

A chronological record of system activities providing documentary evidence of processing that enables management staff to reconstruct, review, and examine the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

AUTHENTICATED RECORD

A signed document with appropriate assurances of authentication or a message with a digital signature verified by a relying party. However, for suspension and revocation

notification purposes, the digital signature contained in such notification message must have been created by the private key corresponding to the public key contained in the Digital Signature Certificate.

AUTHENTICATION

A process used to confirm the identity of a person or to prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit. (*See also* verify (a digital signature))

AUTHORIZATION

The granting of rights, including the ability to access specific information or resources.

AVAILABILITY

The extent to which information or processes are reasonably accessible and usable, upon demand, by an authorized entity, allowing authorized access to resources and timely performance of time-critical operations.

BACKUP

The process of copying critical information, data and software for the purpose of recovering essential processing back to the time the backup was taken.

BINDING

An affirmation by a Certifying Authority of the relationship between a named entity and its public key.

CERTIFICATE

A Digital Signature Certificate issued by Certifying Authority.

CERTIFICATE CHAIN

An ordered list of certificates containing an end-user subscriber certificate and Certifying Authority certificates (See valid certificate).

CERTIFICATE EXPIRATION

The time and date specified in the Digital Signature Certificate when the operational period ends, without regard to any earlier suspension or revocation.

CERTIFICATE EXTENSION

An extension field to a Digital Signature Certificate which may convey additional information about the public key being certified, the certified subscriber, the Digital Signature Certificate issuer, and/or the certification process. Standard extensions are defined in Amendment 1 to ISO/IEC 9594-8:1995 (X.509). Custom extensions can also be defined by communities of interest.

CERTIFICATE ISSUANCE

The actions performed by a Certifying Authority in creating a Digital Signature Certificate and notifying the Digital Signature Certificate applicant (anticipated to become a subscriber) listed in the Digital Signature Certificate of its contents.

CERTIFICATE MANAGEMENT [MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE]

Certificate management includes, but is not limited to, storage, distribution, dissemination, accounting, publication, compromise, recovery, revocation, suspension and administration of Digital Signature Certificates. A Certifying Authority undertakes Digital Signature Certificate management functions by serving as a registration authority for subscriber Digital Signature

Certificates. A Certifying Authority designates issued and accepted Digital Signature Certificates as valid by publication.

CERTIFICATE POLICY

A specialized form of administrative policy tuned to electronic transactions performed during Digital Signature Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

CERTIFICATE REVOCATION (*see* REVOKE A CERTIFICATE)

CERTIFICATE REVOCATION LIST (CRL)

A periodically (or exigently) issued list, digitally signed by a Certifying Authority, of identified Digital Signature Certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked Digital Signature Certificates' serial numbers, and the specific times and reasons for suspension and revocation.

CERTIFICATE SERIAL NUMBER

A value that unambiguously identifies a Digital Signature Certificate generated by a Certifying Authority.

CERTIFICATE SIGNING REQUEST (CSR)

A machine-readable form of a Digital Signature Certificate application.

CERTIFICATE SUSPENSION (*see* SUSPEND A CERTIFICATE)

CERTIFICATION / CERTIFY

The process of issuing a Digital Signature Certificate by a Certifying Authority.

CERTIFYING AUTHORITY (CA)

A person who has been granted a licence to issue a Digital Signature Certificate under Section 24 of Information Technology Act, 2000.

CERTIFYING AUTHORITY SOFTWARE

The cryptographic software required to manage the keys of end entities.

CERTIFYING AUTHORITY SYSTEM

All the hardware and software system (*e.g.* Computer, PKI servers, network devices *etc.*) used by the Certifying Authority for generation, production, issue and management of Digital Signature Certificate.

CERTIFICATION PRACTICE STATEMENT (CPS)

A statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates.

CERTIFIER (*see* ISSUING AUTHORITY)

CHALLENGE PHRASE

A set of numbers and/or letters that are chosen by a Digital Signature Certificate applicant, communicated to the Certifying Authority with a Digital Signature Certificate application, and used by the Certifying Authority to authenticate the subscriber for various purposes as

required by the Certification Practice Statement. A challenge phrase is also used by a secret share holder to authenticate himself, herself, or itself to a secret share issuer.

CERTIFICATE CLASS

A Digital Signature Certificate of a specified level of trust.

CLIENT APPLICATION

An application that runs on a personal computer or workstation and relies on a server to perform some operation.

COMMON KEY

Some systems of cryptographic hardware require arming through a secret-sharing process and require that the last of these shares remain physically attached to the hardware in order for it to stay armed. In this case, "common key" refers to this last share. It is not assumed to be secret as it is not continually in an individual's possession.

COMMUNICATION/NETWORK SYSTEM

A set of related, remotely connected devices and communications facilities including more than one computer system with the capability to transmit data among them through the communications facilities (covering ISDN, lease lines, dial-up, LAN, WAN, *etc.*).

COMPROMISE

A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. (Cf., data integrity)

COMPUTER

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

COMPUTER CENTRE (*See* DATA CENTRE)

COMPUTER DATA BASE

Means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network.

COMPUTER NETWORK

Interconnection of one or more computers through—

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

COMPUTER PERIPHERAL

Means equipment that works in conjunction with a computer but is not a part of the main computer itself, such as printer, magnetic tape reader, *etc.*

COMPUTER RESOURCE

Means computer, computer system, computer network, data, computer database or software.

COMPUTER SYSTEM

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

COMPUTER VIRUS (*see* VIRUS)

CONFIDENTIALITY

The condition in which sensitive data is kept secret and disclosed only to authorized parties.

CONFIRM

To ascertain through appropriate inquiry and investigation. (*See also* authentication; verify a digital signature)

CONFIRMATION OF DIGITAL SIGNATURE CERTIFICATE CHAIN

The process of validating a Digital Signature Certificate chain and subsequently validating an end-user subscriber Digital Signature Certificate.

CONTINGENCY PLANS

The establishment of emergency response, back up operation, and post-disaster recovery processes maintained by an information processing facility or for an information system.

Establish the strategy for recovering from unplanned disruption of information processing operations. The strategy includes the identification and priority of what must be done, who performs the required action, and what tools must be used.

A document, developed in conjunction with application owners and maintained at the primary and backup computer installation, which describes procedures and identifies the personnel necessary to respond to abnormal situations such as disasters. Contingency plans help managers ensure that computer application owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.

CONTROLS

Measures taken to ensure the integrity and quality of a process.

CORRESPOND

To belong to the same key pair. (*See also* public key; private key)

CRITICAL INFORMATION

Data determined by the data owner as mission critical or essential to business purposes.

CROSS-CERTIFICATE

A Certificate used to establish a trust relationship between two Certifying Authorities.

CRYPTOGRAPHIC ALGORITHM

A clearly specified mathematical process for computation; a set of rules that produce a prescribed result.

CRYPTOGRAPHY (*see also* PUBLIC KEY CRYPTOGRAPHY)

i. The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.

ii. A discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized uses.

DAMAGE

Means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

DATA

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

DATA BASE (*see* COMPUTER DATABASE)

DATA CENTRE (*as also* COMPUTER CENTRE)

The facility covering the computer room, media library, network area, server area, programming and administration areas, other storage and support areas used to carry out the computer processing functions. Usually refers to the computer room and media library.

DATA CONFIDENTIALITY (*see* CONFIDENTIALITY)

DATA INTEGRITY

A condition in which data has not been altered or destroyed in an unauthorized manner. (See also threat; compromise)

DATA SECURITY

The practice of protecting data from accidental or malicious modification, destruction, or disclosure.

DEMO CERTIFICATE

A Digital Signature Certificate issued by a Certifying Authority to be used exclusively for demonstration and presentation purposes and not for any secure or confidential communications. Demo Digital Signature Certificates may be used by authorized persons only.

DIGITAL CERTIFICATE APPLICANT

A person that requests the issuance of a public key Digital Signature Certificate by a Certifying Authority. (See also CA applicant; subscriber)

DIGITAL CERTIFICATE APPLICATION

A request from a Digital Signature Certificate applicant (or authorized agent) to a Certifying Authority for the issuance of a Digital Signature Certificate. (*See also* certificate applicant; certificate signing request)

DIGITAL SIGNATURE

Means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3 of the Information Technology Act, 2000.

DIGITAL SIGNATURE CERTIFICATE

Means a Digital Signature Certificate issued under sub-section (4) of Section 35 of the Information Technology Act, 2000.

DISTINGUISHED NAME

A set of data that identifies a real-world entity, such as a person in a computer-based context.

DOCUMENT

A record consisting of information inscribed on a tangible medium such as paper rather than computer-based information. (See also message; record)

ELECTRONIC FORM

With reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro-film, computer generated micro fiche or similar device.

ELECTRONIC MAIL ("E-MAIL")

Messages sent, received or forwarded in digital form via a computer-based communication mechanism.

ELECTRONIC RECORD

Means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated micro-fiche.

ENCRYPTION

The process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).

EXTENSIONS

Extension fields in X.509 v3 certificates. (See X.509)

FIREWALL/DOUBLE FIREWALL

One of several types of intelligent devices (such as routers or gateways) used to isolate networks. Firewalls make it difficult for attackers to jump from network to network. A double firewall is two firewalls connected together. Double firewalls are used to minimise risk if one firewall gets compromised or provide address translation functions.

FILE TRANSFER PROTOCOL (FTP)

The application protocol that offers file system access from the internet suite of protocols.

FUNCTION

In relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer.

GATEWAY

Hardware or software that is used to translate protocols between two or more systems.

GENERATE A KEY PAIR

A trustworthy process of creating private keys during Digital Signature Certificate application whose corresponding public keys are submitted to the applicable Certifying Authority during Digital Signature Certificate application in a manner that demonstrates the applicant's capacity to use the private key.

HARD COPY

A copy of computer output that is printed on paper in a visually readable form; *e.g.* printed reports, listing, and documents.

HASH (HASH FUNCTION)

An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that :

i. A message yields the same result every time the algorithm is executed using the same message as input.

ii. It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.

iii. It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

HIGH-SECURITY ZONE

An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors. High-Security Zones should be accessible only from Security Zones, and are separated from Security Zones and Operations Zones by a perimeter. High-Security Zones are monitored 24 hours a day a week by security staff, other personnel or electronic means.

IDENTIFICATION / IDENTIFY

The process of confirming the identity of a person. Identification is facilitated in public key cryptography by means of certificates.

IDENTITY

A unique piece of information that marks or signifies a particular entity within a domain. Such information is only unique within a particular domain.

INFORMATION

Includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro-film or computer generated micro fiche.

INFORMATION ASSETS

Means all information resources utilized in the course of any organisation's business and includes all information, application software (developed or purchased), and technology (hardware, system software and networks).

INTERMEDIARY

With respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.

INFORMATION TECHNOLOGY SECURITY

All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.

INFORMATION TECHNOLOGY SECURITY POLICY

Rules, directives and practices that govern how information assets, including sensitive information, are managed, protected and distributed within an organization and its Information Technology systems.

KEY

A sequence of symbols that controls the operation of a cryptographic transformation (*e.g.* encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

KEY GENERATION

The trustworthy process of creating a private key/public key pair.

KEY MANAGEMENT

The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

KEY PAIR

In an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

LICENCE

Means a licence granted to a Certifying Authority.

LOCAL AREA NETWORK (LAN)

A geographically small network of computers and supporting components used by a group or department to share related software and hardware resources.

LOW-SENSITIVE

Applies to information that, if compromised, could reasonably be expected to cause injury outside the national interest, for example, disclosure of an exact salary figure.

MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE [*See* CERTIFICATE MANAGEMENT]

MEDIA

The material or configuration on which data is recorded. Examples include magnetic taps and disks.

MESSAGE

A digital representation of information; a computer-based record. A subset of record. (See also record)

NAME

A set of identifying attributes purported to describe an entity of a certain type.

NETWORK

A set of related, remotely connected devices and communications facilities including more than one computer system with the capability to transmit data among them through the communications facilities.

NETWORK ADMINISTRATOR

The person at a computer network installation who designs, controls, and manages the use of the computer network.

NODE

In a network, a point at which one or more functional units connect channels or data circuits.

NOMINATED WEBSITE

A website designated by the Certifying Authority for display of information such as fee schedule, Certification Practice Statement, Certificate Policy etc.

NON-REPUDIATION

Provides proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent.

Note: Only a trier of fact (someone with the authority to resolve disputes) can make an ultimate determination of non-repudiation. By way of illustration, a digital signature verified pursuant to this Certification Practice Statement can provide proof in support of a determination of non-repudiation by a trier of fact, but does not by itself constitute non-repudiation.

NOTARY

A natural person authorized by an executive governmental agency to perform notarial services such as taking acknowledgments, administering oaths or affirmations, witnessing or attesting signatures, and noting protests of negotiable instruments.

ON-LINE

Communications that provide a real-time connection.

OPERATIONS ZONE

An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a threat risk assessment (TRA), and should preferably be accessible from a Reception Zone.

OPERATIONAL CERTIFICATE

A Digital Signature Certificate which is within its operational period at the present date and time or at a different specified date and time, depending on the context.

OPERATIONAL MANAGEMENT

Refers to all business/service unit management (*i.e.* the user management) as well as Information Technology management.

OPERATIONAL PERIOD

The period starting with the date and time a Digital Signature Certificate is issued (or on a later date and time certain if stated in the Digital Signature Certificate) and ending with the date and time on which the Digital Signature Certificate expires or is earlier suspended or revoked.

ORGANIZATION

An entity with which a user is affiliated. An organization may also be a user.

ORIGINATOR

A person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

PASSWORD (PASS PHRASE; PIN NUMBER)

Confidential authentication information usually composed of a string of characters used to provide access to a computer resource.

PARTICULARLY SENSITIVE

Applies to information that, if compromised, could reasonably be expected to cause serious injury outside the national interest, for example loss of reputation or competitive advantage.

PC CARD (*See* ALSO SMART CARD)

A hardware token compliant with standards promulgated by the Personal Computer Memory Card International Association (PCMCIA) providing expansion capabilities to computers, including the facilitation of information security.

PERSON

Means any company or association or individual or body of individuals, whether incorporated or not.

PERSONAL PRESENCE

The act of appearing (physically rather than virtually or figuratively) before a Certifying Authority or its designee and proving one's identity as a prerequisite to Digital Signature Certificate issuance under certain circumstances.

PKI (PUBLIC KEY INFRASTRUCTURE) / PKI SERVER

A set of policies, processes, server platforms, software and workstations used for the purpose of administering Digital Signature Certificates and public-private key pairs, including the ability to generate, issue, maintain, and revoke public key certificates.

PKI HIERARCHY

A set of Certifying Authorities whose functions are organized according to the principle of delegation of authority and related to each other as subordinate and superior Certifying Authority.

PLEDGE (*See* SOFTWARE PUBLISHER'S PLEDGE)

POLICY

A brief document that states the high-level organization position, states the scope, and establishes who is responsible for compliance with the policy and the corresponding standards. Following is an abbreviated example of what a policy may contain:

— Introduction

— Definitions

— Policy Statement identifying the need for "something" (*e.g.* data security)

— Scope

— People playing a role and their responsibilities

— Statement of Enforcement, including responsibility

PRIVATE KEY

The key of a key pair used to create a digital signature.

PROCEDURE

A set of steps performed to ensure that a guideline is met.

PROGRAM

A detailed and explicit set of instructions for accomplishing some purpose, the set being expressed in some language suitable for input to a computer, or in machine language.

PROXY SERVER

A server that sits between a client application such as a web browser and a real server. It intercepts all requests to the real server to see if it can fulfill the request itself. If not, it forwards the request to the real server.

PUBLIC ACCESS ZONE

Generally surrounds or forms part of a government facility. Examples include the grounds surrounding a building, and public corridors and elevator lobbies in multiple-occupancy buildings. Boundary designators such as signs and direct or remote surveillance may be used to discourage unauthorized activity.

PUBLIC KEY

The key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

PUBLIC KEY CERTIFICATE (*See* CERTIFICATE)

PUBLIC KEY CRYPTOGRAPHY (*See* CRYPTOGRAPHY)

A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

PUBLIC KEY INFRASTRUCTURE (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. It includes a set of policies, processes, server platforms, software and workstations, used for the purpose of administering Digital Signature Certificates and keys.

PUBLIC/PRIVATE KEY PAIR (*See* PUBLIC KEY; PRIVATE KEY; KEY PAIR)

RECIPIENT (OF A DIGITAL SIGNATURE)

A person who receives a digital signature and who is in a position to rely on it, whether or not such reliance occurs. (*See also* relying party)

RECORD

Information that is inscribed on a tangible medium (a document) or stored in an electronic or other medium and retrievable in perceivable form. The term "record" is a superset of the two terms "document" and "message". (*See also* document; message)

RE-ENROLLMENT (*See also* RENEWAL)

RELY / RELIANCE (ON A CERTIFICATE AND DIGITAL SIGNATURE)

To accept a digital signature and act in a manner that could be detrimental to oneself were the digital signature to be ineffective. (See also relying party; recipient)

RELYING PARTY

A recipient who acts in reliance on a certificate and digital signature. (*See also* recipient; rely or reliance (on a certificate and digital signature))

RENEWAL

The process of obtaining a new Digital Signature Certificate of the same class and type for the same subject once an existing Digital Signature Certificate has expired.

REPOSITORY

A database of Digital Signature Certificates and other relevant information accessible on-line.

REPUDIATION (*See also* NON-REPUDIATION)

The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.

REVOKE A CERTIFICATE

The process of permanently ending the operational period of a Digital Signature Certificate from a specified time forward.

RISK

The potential of damage to a system or associated assets that exists as a result of the combination of security threat and vulnerability.

RISK ANALYSIS

The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards.

RISK ASSESSMENT

An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events.

RISK MANAGEMENT

The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect Information Technology system resources.

RSA

A public key cryptographic system invented by Rivest, Shamir & Adelman.

SECRET SHARE

A portion of a cryptographic secret split among a number of physical tokens.

SECRET SHAREHOLDER

An authorized holder of a physical token containing a secret share.

SECURE CHANNEL

A cryptographically enhanced communications path that protects messages against perceived security threats.

SECURE SYSTEM

Means computer hardware, software, and procedure that—

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

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

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

(d) adhere to generally accepted security procedures.

SECURITY PROCEDURE

Means the security procedure prescribed under Section 16 of the Information Technology Act, 2000.

SECURITY

The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific “state” to be preserved under various operations.

SECURITY POLICY

A document which articulates requirements and good practices regarding the protections maintained by a trustworthy system.

SECURITY SERVICES

Services provided by a set of security frameworks and performed by means of certain security mechanisms. Such services include, but are not limited to, access control, data confidentiality, and data integrity.

SECURITY ZONE

An area to which access is limited to authorised personnel and to authorised and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 week by security staff, other personnel or electronic means.

SELF-SIGNED PUBLIC KEY

A data structure that is constructed the same as a Digital Signature Certificate but that is signed by its subject. Unlike a Digital Signature Certificate, a self-signed public key cannot be used in a trustworthy manner to authenticate a public key to other parties.

SERIAL NUMBER (*See* CERTIFICATE SERIAL NUMBER)

SERVER

A computer system that responds to requests from client systems.

SIGN

To create a digital signature for a message, or to affix a signature to a document, depending upon the context.

SIGNATURE (*See* DIGITAL SIGNATURE)

SIGNER

A person who creates a digital signature for a message, or a signature for a document.

SMART CARD

A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

S/MIME

A specification for E-mail security exploiting a cryptographic message syntax in an internet mime environment.

SUBJECT (OF A CERTIFICATE)

The holder of a private key corresponding to a public key. The term “subject” can refer to both the equipment or device that holds a private key and to the individual person, if any, who controls that equipment or device. A subject is assigned an unambiguous name, which is bound to the public key contained in the subject’s Digital Signature Certificate.

SUBJECT NAME

The unambiguous value in the subject name field of a Digital Signature Certificate, which is bound to the public key.

SUBSCRIBER

A person in whose name the Digital Signature Certificate is issued.

SUBSCRIBER AGREEMENT

The agreement executed between a subscriber and a Certifying Authority for the provision of designated public certification services in accordance with this Certification Practice Statement.

SUBSCRIBER INFORMATION

Information supplied to a certification authority as part of a Digital Signature Certificate application. (*See also* certificate application)

SUSPEND A CERTIFICATE

A temporary "hold" placed on the effectiveness of the operational period of a Digital Signature Certificate without permanently revoking the Digital Signature Certificate. A Digital Signature Certificate suspension is invoked by, *e.g.*, a CRL entry with a reason code. (*See also* revoke a certificate)

SYSTEM ADMINISTRATOR

The person at a computer installation who designs, controls, and manages the use of the computer system.

SYSTEM SECURITY

A system function that restricts the use of objects to certain users.

SYSTEM SOFTWARE

Application-independent software that supports the running of application software. It is a software that is part of or made available with a computer system and that determines how application programs are run; for example, an operating system.

TEST CERTIFICATE

A Digital Signature Certificate issued by a Certifying Authority for the limited purpose of internal technical testing. Test certificates may be used by authorized persons only.

THREAT

A circumstance or event with the potential to cause harm to a system, including the destruction, unauthorized disclosure, or modification of data and/or denial of service.

TIME-OUT

A security feature that logs off a user if any entry is not made at the terminal within a specified period of time.

TIME STAMP

A notation that indicates (at least) the correct date and time of an action, and identity of the person or device that sent or received the time stamp.

TOKEN

A hardware security token containing a user's private key(s), public key certificate, and, optionally, a cache of other certificates, including all certificates in the user's certification chain.

TRANSACTION

A computer-based transfer of business information, which consists of specific processes to facilitate communication over global networks.

TRUST

Generally, the assumption that an entity will behave substantially as expected. Trust may apply only for a specific function. The key role of this term in an authentication framework is to describe the relationship between an authenticating entity and a Certifying Authority. An authenticating entity must be certain that it can trust the Certifying Authority to create only valid and reliable Digital Signature Certificates, and users of those Digital Signature Certificates rely upon the authenticating entity's determination of trust.

TRUSTED POSITION

A role that includes access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of Digital Signature Certificates, including operations that restrict access to a repository.

TRUSTED THIRD PARTY

In general, an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers. A trusted third party does not connote the existence of a trustor-trustee or other fiduciary relationship. (Cf., trust)

TRUSTWORTHY SYSTEM

Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.

TYPE (OF CERTIFICATE)

The defining properties of a Digital Signature Certificate, which limit its intended purpose to a class of applications uniquely, associated with that type.

UNAMBIGUOUS NAME (*See* DISTINGUISHED NAME)

UNIFORM RESOURCE LOCATOR (URL)

A standardized device for identifying and locating certain records and other resources located on the World Wide Web.

USER

An authorized entity that uses a certificate as applicant, subscriber, recipient or relying party, but not including the Certifying Authority issuing the Digital Signature Certificate. (*See also* certificate applicant; entity; person; subscriber)

VALID CERTIFICATE

A Digital Signature Certificate issued by a Certifying Authority and accepted by the subscriber listed in it.

VALIDATE A CERTIFICATE (*i.e.*, OF AN END-USER SUBSCRIBER CERTIFICATE)

The process performed by a recipient or relying party to confirm that an end-user subscriber Digital Signature Certificate is valid and was operational at the date and time a pertinent digital signature was created.

VALIDATION (OF CERTIFICATE APPLICATION)

The process performed by the Certifying Authority or its agent following submission of a Digital Signature Certificate application as a prerequisite to approval of the application and the issuance of a Digital Signature Certificate. (*See also* authentication; software validation)

VALIDATION (OF SOFTWARE) (*See* SOFTWARE VALIDATION)

VERIFY (A DIGITAL SIGNATURE)

In relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether —

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

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

VIRUS

Means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

VULNERABILITY

A weakness that could be exploited to cause damage to the system or the assets it contains.

WEB BROWSER

A software application used to locate and display web pages.

WORLD WIDE WEB (WWW)

A hypertext-based, distributed information system in which users may create, edit, or browse hypertext documents. A graphical document publishing and retrieval medium; a collection of linked documents that reside on the internet.

WRITING

Information in a record that is accessible and usable for subsequent reference.

X.509

The ITU-T (International Telecommunications Union-T) standard for Digital Signature Certificates. X.509 v3 refers to certificates containing or capable of containing extensions.

ACRONYMS

ARL Authority Revocation List

CA Certification Authority

CP Certificate Policy

CPS Certification Practice Statement

CRL Certificate Revocation List

CSR Certificate Signing Request

DN Distinguished Name

e-mail Electronic Mail

FTP File Transfer Protocol

ISDN Integrated Service Digital Network

ITU International Telecommunications Union

LAN Local Area Network

PIN Personal Identification Number

PKI Public Key Infrastructure

PKIX Public Key Infrastructure X.509

URL Uniform Resource Locator

WAN Wide Area Network