

**GOVERNMENT OF INDIA
MINISTRY OF INFORMATION TECHNOLOGY**

NOTIFICATION

New Delhi, the 9th July, 2001

G.S.R. 512(E):- In exercise of the powers conferred by clauses (c), (d), (e), and (g) of sub-section (2) of section 89 of the Information Technology Act, 2000 (21 of 2000), the Controller hereby, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, makes the following Regulations, namely: -

1. Short title and Commencement:- (1) These Regulations may be called the Information Technology (Certifying Authority) Regulations, 2001.

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

2. Definitions: - In these Regulations, unless the context otherwise requires,-

- (a) " Act" means the Information Technology Act, 2000 (21 of 2000) ;
- (b) "Certifying Authority " means a person who has been granted a licence to issue a Digital Signature Certificate under section 24 of the Act;
- (c) "Certificate Revocation List" means 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;

- (d) “Controller” means the Controller of Certifying Authorities appointed under sub-section (1) section 17 of the Act;
- (e) “Form” means the form appended to these Regulations;
- (f) “Public Key Certificate” means a Digital Signature Certificate issued by Certifying Authority.
- (g) “subscriber” means a person in whose name the Digital Signature Certificate is issued;
- (h) Words and expressions used herein and not defined, but defined in the Act, shall have the meanings respectively assigned to them in the Act.

3. Terms and conditions of licence to issue Digital Signature

Certificate: - Every licence to issue Digital Signature Certificates shall be granted under the Act subject to the following terms and conditions, namely: -

(i) *General-*

- (a) The licence shall be valid for a period of five years from the date of issue.
- (b) The licence shall not be transferable or heritable;
- (c) The Controller can revoke or suspend the licence in accordance with the provisions of the Act.
- (d) The Certifying Authority shall be bound to comply with all the parameters against which it was audited prior to issue of licence and shall consistently and continuously comply with those parameters during the period for which the licence shall remain valid.
- (e) The Certifying Authority shall subject itself to periodic audits to ensure that all conditions of the licence are consistently complied with by it. As the cryptographic components of the Certifying Authority systems are highly sensitive and critical, the components must be subjected to periodic expert review to ensure their integrity and assurance.
- (f) The Certifying Authority must maintain secure and reliable records and logs for activities that are core to its operations.

3

- (g) Public Key Certificates and Certificate Revocation Lists must be archived for a minimum period of seven years to enable

verification of past transactions.

- (h) The Certifying Authority shall provide Time Stamping Service for its subscribers. Error of the Time Stamping clock shall not be more than 1 in 10^9 .
- (i) The Certifying Authority shall use methods, which are approved by the Controller, to verify the identity of a subscriber before issuing or renewing any Public Key Certificate.
- (j) The Certifying Authority shall publish a notice of suspension or revocation of any certificate in the Certificate Revocation List in its repository immediately after receiving an authorised request of such suspension or revocation.
- (k) The Certifying Authority shall always assure the confidentiality of subscriber information.
- (l) All changes in Certificate Policy and certification practice statement shall be published on the web site of the Certifying Authority and brought to the notice of the Controller well in advance of such publication. However any change shall not contravene any provision of the Act, rule or regulation or made there under.
- (m) The Certifying Authority shall comply with every order or direction issued by the Controller within the stipulated period.

(ii) *Overall Management and Obligations-*

- (a) The Certifying Authority shall manage its functions in accordance with the levels of integrity and security approved by the Controller from time to time.
- (b) The Certifying Authority shall disclose information on the assurance levels of the certificates that it issues and the limitations of its liabilities to each of its subscribers and relying parties.
- (c) The Certifying Authority shall as approved, in respect of security and risk management controls continuously ensure that security policies and safeguards are in place. Such controls include personnel security and incident handling measures to prevent fraud and security breaches.

(iii) *Certificate and Key Management-*

4

- (a) To ensure the integrity of its digital certificates, the Certifying Authority shall ensure the use of approved security controls in the certificate management processes, i.e. certificate registration, generation, issuance, publication, renewal, suspension, revocation and archival.

- (b) The method of verification of the identity of the applicant of a Public Key Certificates shall be commensurate with the level of assurance accorded to the certificate.
- (c) The Certifying Authority shall ensure the continued accessibility and availability of its Public Key Certificates and Certificate Revocation Lists in its repository to its subscribers and relying parties.
- (d) In the event of a compromise of the private key the Certifying Authority shall follow the established procedures for immediate revocation of the affected subscribers' certificates.
- (e) The Certifying Authority shall make available the information relating to certificates issued and/or revoked by it to the Controller for inclusion in the National Repository.
- (f) The private key of the Certifying Authority shall be adequately secured at each phase of its life cycle, i.e. key generation, distribution, storage, usage, backup, archival and destruction.
- (g) The private key of the Certifying Authority shall be stored in high security module in accordance with FIPS 140-1 level 3 recommendations for Cryptographic Modules Validation List.
- (h) Continued availability of the private key be ensured through approved backup measures in the event of loss or corruption of its private key.
- (i) All submissions of Public Key Certificates and Certificate Revocation Lists to the National Repository of the Controller must ensure that subscribers and relying parties are able to access the National Repository using LDAP ver 3 for X.500 Directories.
- (j) The Certifying Authority shall ensure that the subscriber can verify the Certifying Authority's Public Key Certificate, if he chooses to do so, by having access to the Public Key Certificate of the Controller.

(iv) *Systems and Operations-*

- (a) The Certifying Authority shall prepare detailed manuals for performing all its activities and shall scrupulously adhere to them.
- (b) Approved access and integrity controls such as intrusion detection, virus scanning, prevention of denial-of service attacks and physical security measures shall be followed by the

5

Certifying Authority for all its systems that store and process the subscribers' information and certificates.

- (c) The Certifying Authority shall maintain records of all activities and review them regularly to detect any anomaly in the system.

(v) *Physical, procedural and personnel security-*

- (a) Every Certifying Authority shall get an independent periodic

audit done through an approved auditor. Such periodic audits shall focus on the following issues among others: -

- (i) changes/additions in physical controls such as site location, access, etc ;
 - (ii) re-deployment of personnel from an approved role/task to a new one;
 - (iii) appropriate security clearances for outgoing employees such as deletion of keys and all access privileges;
 - (iv) thorough background checks, etc. during employment of new personnel.
- (b) The Certifying Authority shall follow approved procedures to ensure that all the activities referred to in (i) to (iv) in sub-regulation (a) are recorded properly and made available during audits.

(vi) *Financial-*

- (a) Every Certifying Authority shall comply with all the financial parameters during the period of validity of the licence, issued under the Act.
- (b) Any loss to the subscriber, which is attributable to the Certifying Authority, shall be made good by the Certifying Authority.

(vii) *Compliance Audits-*

- (a) The Certifying Authority shall subject itself to Compliance Audits that shall be carried out by one of the empanelled Auditors duly authorized by the Controller for the purpose. Such audits shall be based on the Internet Engineering Task Force document RFC 2527 – Internet X.509 PKI Certificate Policy and Certification Practices Framework.
- (b) If a Digital Signature Certificate issued by the Certifying Authority is found to be fictitious or that proper identification

6

procedures have not been followed by the Certifying Authority while issuing such certificate, the Certifying Authority shall be liable for any losses resulting out of this lapse and shall be liable to pay compensation as decided by the Controller.

4. The standards followed by the Certifying Authority for carrying out its functions: –

- (1) Every Certifying Authority shall observe the following standards for carrying out different activities associated with its functions.
 - (a) **PKIX (Public Key Infrastructure)**
Public Key Infrastructure as recommended by Internet

Engineering Task Force (IETF) document draft-ietf-pkix-roadmap-05 for “Internet X.509 Public Key Infrastructure” (March 10, 2000);

(b) Public-key cryptography based on the emerging Institute of Electrical and Electronics Engineers (IEEE) standard P1363 for three families:

Discrete Logarithm (DL) systems
 Elliptic Curve Discrete Logarithm (EC) systems
 Integer Factorization (IF) systems;

(c) Public-key Cryptography Standards (PKCS)

PKCS#1 RSA Encryption Standard (512, 1024, 2048 bit)
 PKCS#3 Diffie-Hellman Key Agreement Standard
 PKCS#5 Password Based Encryption Standard
 PKCS#6 Extended-Certificate Syntax 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#11 Cryptographic Token Interface Standard
 PKCS#12 Portable format for storing/transporting a user's private keys and certificates
 PKCS#13 Elliptic Curve Cryptography Standard
 PKCS#15 Cryptographic Token Information Format Standard;

(d) Federal Information Processing Standards (FIPS)

FIPS 180-1, Secure Hash Standard
 FIPS 186-1, Digital Signature Standard (DSS)
 FIPS 140-1 level 3, Security Requirement for Cryptographic Modules;

(e) Discrete Logarithm (DL) systems

Diffie-Hellman, MQV key agreement
 DSA, Nyberg-Rueppel signatures;

7

(f) Elliptic Curve (EC) systems

Elliptic curve analogs of DL systems;

(g) Integer Factorization (IF) systems

RSA encryption
 RSA, Rabin-Williams signatures;

(h) Key agreement schemes

(i) Signature schemes

DL/EC scheme with message recovery
 PSS, FDH, PKCS #1 encoding methods for IF family
 PSS-R for message recovery in IF family;

(ii) Encryption schemes

Abdalla-Bellare-Rogaway DHAES for DL/EC family;

(i) Form and size of the key pairs

- (1) The minimum key length for Asymmetric cryptosystem (RSA Algorithm) shall be 2048 for the Certifying Authority's key pairs and 1024 for the key pairs used by subscribers.
- (2) The Certifying Authority's key pairs shall be changed every three to five years (except during exigencies as in the case of key compromise when the key shall be changed immediately). The Certifying Authority shall take appropriate steps to ensure that key changeover procedures as mentioned in the approved Certificate Practice Statements are adhered to.
- (3) The subscriber's key pairs shall be changed every one to two years;

(j) Directory Services (LDAP ver 3)

X.500 for publication of Public Key Certificates and Certificate Revocation Lists

X.509 version 3 Certificates as specified in ITU RFC 1422

X.509 version 2 Certificate Revocation Lists;

(i) Publication of Public Key Certificate.

The Certifying Authority shall, on acceptance of a Public Key Certificate by a subscriber, publish it on its web site for access by the subscribers and relying parties. The Certifying Authority shall be responsible and shall ensure the transmission of Public Key Certificates and Certificate Revocation Lists to the National Repository of the Controller, for access by subscribers and relying parties. The National Repository shall conform to X.500 Directory Services and provide for access through LDAP Ver 3. The Certifying Authority shall be responsible for ensuring that Public Key Certificates and Certificate Revocation Lists integrate seamlessly with the National Repository on their transmission;

8

k) Public Key Certificate Standard

All Public Key Certificates issued by the Certifying Authorities shall conform to International Telecommunication Union X.509 version 3 standard. X.509 v3 certificate basic syntax is as follows.

tbsCertificate

```
{
  Version
  Serial Number
  Signature
  Issuer
  Validity
  Subject
  Subject Public Key Information
  Issuer Unique ID [1] IMPLICIT Unique Identifier optional,
    -- If present, version shall be v2 or v3
  Subject Unique ID [2] IMPLICIT Unique Identifier optional,
    -- If present, version shall be v2 or v3
  Extensions [3] EXPLICIT Extensions optional
    -- If present version shall be v3
```

```

{
    Authority Key Identifier
    {
        Key Identifier optional,
        Authority Certificate Issuer optional,
        Authority Certificate Serial Number optional
    }
    Subject Key Identifier
    Key Usage
    {
        Digital Signature
        Non Repudiation
        Key Encipherment
        Data Encipherment
        Key Agreement
        Key Cert Sign
        cRLSign
        Encipher Only
        Decipher Only
    }
    Private Key Usage Period
    {
        Not Before optional,
        Not After optional
    }
    Certificate Policies
    {
        Policy Information
        {
            Policy Identifier
            9

            Policy Qualifiers optional
        }
        Certificate Policy Id
        {
            Policy Qualifier Info
            {
                Policy Qualifier Id
                Qualifier
                {
                    cPSuri
                    User Notice
                    {
                        Notice Reference optional
                        {
                            Organization
                            Notice Numbers
                        }
                        Display Text optional
                        {
                            visibleString
                            bmpString
                            utf8String
                        }
                    }
                }
            }
        }
    }
}

```



```

Policy Mappings
{
  Issuer Domain Policy
  Subject Domain Policy
}
Subject Alternative Name
{
  General Name
  {
    Other Name
    {
      type-id
      value
    }
    Rfc822Name
    DNS Name
    X400 Address
    Directory Name
    edi Party Name
    {
      Name Assigner optional,
      Party Name
    }
    Uniform Resource Identifier
    IP Address
    Registered ID
  }
}

```

10

```

Issuer Alternative Names
Subject Directory Attributes
Basic Constraints
{
  cA
  path Len Constraint optional
}
Name Constraints
{
  Permitted Subtrees optional
  Excluded Subtrees optional
}
Policy Constraints
{
  Require Explicit Policy optional
  Inhibit Policy Mapping optional
}
Extended key usage field
{
  Extended Key Usage Syntax
  Key Purpose Id
  {
    Server Authentication
    Client Authentication
    Code Signing
    Email Protection

```

```

        Time Stamping
    }
}
CRL Distribution Points
{
    CRL Distribution Points Syntax
    Distribution Point
    {
        Distribution Point optional
        {
            full Name
            name Relative To CRL Issuer
        }
    }
    Reasons optional
    {
        Unused
        Key Compromise
        CA Compromise
        Affiliation Changed
        Superseded
        Cessation Of Operation
        Certificate Hold
    }
    cRL Issuer optional
}
Authority Information Access
{
    Authority Information Access Syntax
    Access Description
    {
        Access Method
        Access Location
    }
}
Signature Algorithm
Signature Value
}

```

11

(i) Certificate

TBSCertificate is certificate “to be signed”. The field contains the names of the subject and issuer, a public key associated with the subject, a validity period, and other associated information. The fields are described in detail.

(ii) Version

This field describes the version of the encoded certificate. When extensions are used, as expected in this profile, use X.509 version 3 (value is 2). If no extensions are present, but a Unique Identifier is present, use version 2 (value is 1). If only basic fields are present, use version 1 (the value is omitted from the certificate as the default value).

(iii) Serial number

The serial number is an integer assigned by the Certifying Authority to each certificate. It shall be unique for each certificate issued by a given Certifying Authority (i.e., the issuer name and serial number identify a unique certificate).

(iv) Signature

This field contains the algorithm identifier for the algorithm used by the Certifying Authority to sign the certificate.

(v) Issuer

The issuer field identifies the entity who has signed and issued the certificate. The issuer field shall contain a non-empty distinguished name.

(vi) Validity

The certificate validity period is the time interval during which the Certifying Authority warrants that it will maintain information about the status of the certificate.

12

(vii) Subject

The subject field identifies the entity associated with the public key stored in the subject public key field. The subject name may be carried in the subject field and/or the subjectAltName extension. If the subject is a Certifying Authority (e.g., the basic constraints extension, is present and the value of cA is TRUE,) then the subject field shall be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject Certifying Authority.

(viii) Subject Public Key Information

This field is used to carry the public key and identify the algorithm with which the key is used.

(ix) Unique Identifiers

These fields may only appear if the version is 2 or 3. The subject and issuer unique identifiers are present in the certificate to handle the possibility of reuse of subject and/or issuer names over time.

(x) Extensions

This field may only appear if the version is 3. The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with users or public keys and for managing the certification hierarchy. The X.509 v3 certificate format also allows communities to define private extensions to carry information unique to those communities. If present, this field is a sequence of one or more certificate extensions. The content of certificate extensions in the Internet Public Key Infrastructure is defined as follows, namely:-

(a) *Authority Key Identifier*

The authority key identifier extension provides a means of

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover). The identification may be based on either the key identifier (the subject key identifier in the issuer's certificate) or on the issuer name and serial number.

(b) Subject Key Identifier

The subject key identifier extension provides a means of identifying certificates that contain a particular public key.

(c) Key Usage

The key usage extension defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate. The usage restriction might be employed when a key that could be used for more than one operation is to be restricted.

13

For example, when an RSA key should be used only for signing, the digital Signature and/or non-Repudiation bits would be asserted. Likewise, when an RSA key should be used only for key management, the key Encipherment bit would be asserted.

(d) Private Key Usage Period

The private key usage period extension allows the certificate issuer to specify a different validity period for the private key than the certificate. This extension is intended for use with digital signature keys. This extension consists of two optional components, not Before and not After. (This profile recommends against the use of this extension. Certifying Authorities conforming to this profile MUST NOT generate certificates with critical private key usage period extensions.)

(e) Certificate Policies

The certificate policies extension contains a sequence of one or more policy information terms, each of which consists of an object identifier and optional qualifiers. These policy information terms indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used. Optional qualifiers, which may be present, are not expected to change the definition of the policy.

(f) Policy Mappings

This extension is used in Certifying Authority certificates. It lists one or more pairs of object identifiers; each pair includes an issuer Domain Policy and a subject Domain Policy. The pairing indicates the issuing Certifying Authority considers its issuer Domain Policy equivalent to the subject Certifying Authority's subject Domain Policy.

(g) Subject Alternative Name

The subject alternative names extension allows additional identities to be bound to the subject of the certificate. Defined options include an Internet electronic mail address, a Directory Naming Service name, an IP address, and a uniform resource identifier (URI).

(h) *Issuer Alternative Names*

This extension is used to associate Internet style identities with the certificate issuer.

(i) *Subject Directory Attributes*

The subject directory attributes extension is not recommended as

14

an essential part of this profile, but it may be used in local environments.

(j) *Basic Constraints*

The basic constraints extension identifies whether the subject of the certificate is a Certifying Authority and how deep a certification path may exist through that Certifying Authority.

(k) *Name Constraints*

The name constraints extension, which MUST be used only in a Certifying Authority certificate, indicates a name space within which all subject names in subsequent certificates in a certification path shall be located. Restrictions may apply to the subject distinguished name or subject alternative names. Restrictions apply only when the specified name form is present. If no name of the type is in the certificate, the certificate is acceptable.

(l) *Policy Constraints*

The policy constraints extension can be used in certificates issued to Certifying Authorities. The policy constraints extension constrains path validation in two ways. It can be used to prohibit policy mapping or require that each certificate in a path contain an acceptable policy identifier.

(m) *Extended key usage field*

This field indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension field.

(n) *CRL Distribution Points*

The CRL distribution points extension identifies how CRL information is obtained.

(o) *Private Internet Extensions*

This extension may be used to direct applications to identify an on-line validation service supporting the issuing Certifying Authority.

(p) Authority Information Access

The authority information access extension indicates how to access Certifying Authority information and services for the issuer of the certificate in which the extension appears. Information and services may include on-line validation services and Certifying Authority policy data.

(xi) Signature Algorithm

15

The Signature Algorithm field contains the identifier for the cryptographic algorithm used by the Certifying Authority to sign this certificate. The algorithm identifier is used to identify a cryptographic algorithm.

(xii) Signature Value

The Signature Value field contains a digital signature computed upon the Abstract Syntax Notation (ASN.1) DER encoded tbsCertificate. The ASN.1 DER encoded tbsCertificate is used as the input to the signature function. This signature value is then ASN.1 encoded as a BIT STRING and included in the Certificate's signature field.

(I) Certificate Revocation List Standard –

CRL and CRL Extensions Profile - The CRL contents as per International Telecommunications Union standard ver 2 are as follows

CertificateList

```

{
  TBSCertList
  {
    Version
    Signature
    Issuer
    This Update
    Next Update
    Revoked Certificates
    {
      User Certificate
      Revocation Date
      Certificate Revocation List Entry Extensions
      {
        Reason Code
        {
          Unspecified
          Key Compromise
          CA Compromise
          Affiliation Changed
          Superseded
          Cessation Of Operation
          Certificate Hold
          Remove From Certificate Revocation List
        }
      }
      Hold Instruction Code
      Invalidity Date
    }
  }
}

```

```

    Issuance Date
    Certificate Issuer
  } optional
Certificate Revocation List Extensions
{
  Authority Key Identifier
  Issuer Alternative Name
    16

  Certificate Revocation List Number
  Delta Certificate Revocation List Indicator
  Issuing Distribution Point
  {
    Distribution Point
    Only Contains User Certs
    Only Contains CA Certs
    Only Some Reasons
    Indirect Certificate Revocation List
  }
} optional
Signature Algorithm
Signature Value
}

```

(i) **tbsCertList**

The certificate list to be signed, or TBSCertList, is a sequence of required and optional fields. The required fields identify the Certificate Revocation List issuer, the algorithm used to sign the Certificate Revocation List, the date and time the Certificate Revocation List was issued, and the date and time by which the Certifying Authority will issue the next Certificate Revocation List.

Optional fields include lists of revoked certificates and Certificate Revocation List extensions. The Revoked Certificate List is optional to support the case where a Certifying Authority has not revoked any unexpired certificates that it has issued. The profile requires conforming Certifying Authorities to use the Certificate Revocation List extension cRLNumber in all Certificate Revocation Lists issued.

The first field in the sequence is the tbsCertList. This field is itself a sequence containing the name of the issuer, issue date, issue date of the next list, the list of revoked certificates, and optional Certificate Revocation List extensions. Further, each entry on the revoked certificate list is defined by a sequence of user certificate serial number, revocation date, and optional Certificate Revocation List entry extensions. The fields are described in detail, as follows namely:-

(ii) **Version**

This optional field describes the version of the encoded Certificate Revocation List. When extensions are used, as required by this profile, this field **MUST** be present and **MUST** specify version 2 (the integer value is 1).

(iii) Signature

This field contains the algorithm identifier for the algorithm used to sign the Certificate Revocation List. This field shall contain the same

17

algorithm identifier as the signature Algorithm field in the sequence Certificate List.

(iv) Issuer Name

The issuer name identifies the entity who has signed and issued the Certificate Revocation List. The issuer identity is carried in the issuer name field. Alternative name forms may also appear in the issuer Alternate Name extension. The issuer name field **MUST** contain an X.500 distinguished name (DN). The issuer name field is defined as the X.501 type Name, and **MUST** follow the encoding rules for the issuer name field in the certificate.

(v) This Update

This field indicates the issue date of this Certificate Revocation List. This Update may be encoded as UTC Time or Generalized Time. Certifying Authorities conforming to this profile that issue Certificate Revocation Lists **MUST** encode This Update as UTCTime for dates through the year 2049. Certifying Authorities conforming to this profile that issue Certificate Revocation Lists **MUST** encode This Update as Generalized Time for dates in the year 2050 or later.

(vi) Next Update

This field indicates the date by which the next Certificate Revocation List will be issued. The next Certificate Revocation List could be issued before the indicated date, but it will not be issued any later than the indicated date. Certifying Authorities should issue Certificate Revocation Lists with a Next Update time equal to or later than all previous Certificate Revocation Lists. Next Update may be encoded as UTCTime or GeneralizedTime.

(vii) Revoked Certificates

Revoked certificates are listed. The revoked certificates are named by their serial numbers. Certificates revoked by the Certifying Authority are uniquely identified by the certificate serial number. The date on which the revocation occurred is specified. Additional information may be supplied in Certificate Revocation List entry extensions;

(viii) CRL Entry Extensions

The Certificate Revocation List entry extensions already defined by American National Standards Institute X9 and International Standards Organisation /IEC /International Telecommunication Union for X.509 v2 Certificate Revocation Lists provide methods for associating additional attributes with Certificate Revocation List entries [X.509] [X9.55]. The X.509 v2 Certificate Revocation List format also allows communities to define private Certificate Revocation List entry extensions to carry information unique to those communities. All

Certificate Revocation List entry extensions used in this specification are non-critical.

(a) *Reason Code*

The reason Code is a non-critical Certificate Revocation List entry extension that identifies the reason for the certificate revocation. Certifying Authorities are strongly encouraged to include meaningful reason codes in Certificate Revocation List entries; however, the reason code Certificate Revocation List entry extension should be absent instead of using the unspecified (0) Reason Code value.

(b) *Hold Instruction Code*

The hold instruction code is a non-critical Certificate Revocation List entry extension that provides a registered instruction identifier, which indicates the action to be taken after encountering a certificate that has been placed on hold.

(c) *Invalidity Date*

The invalidity date is a non-critical Certificate Revocation List entry extension that provides the date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid. This date may be earlier than the revocation date in the Certificate Revocation List entry, which is the date at which the Certifying Authority processed the revocation.

(d) *Certificate Issuer*

This Certificate Revocation List entry extension identifies the certificate issuer associated with an entry in an indirect Certificate Revocation List, i.e. a Certificate Revocation List that has the indirect Certificate Revocation List indicator set in its issuing distribution point extension. If this extension is not present on the first entry in an indirect Certificate Revocation List, the certificate issuer defaults to the Certificate Revocation List issuer. On subsequent entries in an indirect Certificate Revocation List, if this extension is not present, the certificate issuer for the entry is the same as that for the preceding entry.

(ix) Issuing Distribution Point

The issuing distribution point is a critical Certificate Revocation List extension that identifies the Certificate Revocation List distribution point for a particular Certificate Revocation List, and it indicates whether the Certificate Revocation List covers revocation for end entity certificates only, Certifying Authority certificates only, or a limited set

or reason codes. Although the extension is critical, conforming implementations are not required to support this extension.

(x) Signature Algorithm

The signature Algorithm field contains the algorithm identifier for the algorithm used by the Certifying Authority to sign the Certificate List. This field **MUST** contain the same algorithm identifier as the signature field in the sequence tbsCertList.

(xi) Signature Value

The signature Value field contains a digital signature computed upon the ASN.1 DER encoded to be signed CertList. The ASN.1 DER encoded tbsCertList is used as the input to the signature function. This signature value is then ASN.1 encoded as a BIT STRING and included in the Certificate Revocation List's signature Value field.

- (2) The list of standards specified in sub-regulation (1) shall be updated at least once a year to include new standards that may emerge from the international bodies. In addition, if any Certifying Authority or a group of Certifying Authorities brings a set of standards to the Controller for a specific user community, the Controller shall examine the same and respond to them within ninety days.

5. (1) Every Certifying Authority shall disclose:-

- (a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;
- (b) any Certification Practice Statement relevant thereto;
- (c) notice of the revocation or suspension of its Certifying Authority Certificate, if any; and
- (d) any other fact that materially or adversely affect either the reliability of a Digital Signature Certificate, which that Authority has issued by it or the Authority's ability to perform its services

- (2) The above disclosure shall be made available to the Controller through filling up of online forms on the Web site of the Controller on the date and time the information is made public. The Certifying Authority shall digitally sign the information.

6. Communication of compromise of Private Key:-

- (1) Where the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, the subscriber shall communicate the same without any delay to the Certifying Authority.

20

- (2) An application for revocation of the key pair shall be made in Form online on the web site of the concerned Certifying Authority to enable revocation and publication in the Certificate Revocation List. The Subscriber shall encrypt this transaction by using the public key of the Certifying Authority.

The transaction shall be further authenticated with the private key of the subscriber even though it may have already been compromised.

[1(6)/2001 – CCA]

(K N GUPTA)
Controller of Certifying Authorities

21

FORM

[See Regulation 6]

Communication of compromise of Private Key

- 1. Name of Holder : _____
- 2. Public Key of Holder : (Attach PKC)
- 3. Category of Certificate : Individual/Organisation/Web Server
...../Other (please specify)
- 4. e-mail address : _____
- 5. Distinguished Name : _____
- 6. Serial No. of Certificate : _____
- 7. Certificate Fingerprint : _____

- 8. Date & Time of communication : _____

(Digital Signature of Holder)