The Information Technology (Certifying Authorities) Amendment Rules, 2011

Notification, New Delhi, the 25th October, 2011 G.S.R. 782(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 further to amend the Information Technology (Certifying Authorities) Rules, 2000, namely:—

1. (1) These rules may be called the Information Technology (Certifying Authorities) Amendment Rules, 2011.

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

2. In the Information Technology (Certifying authorities) Rules, 2000,-

(a) in rule 4, for the words "and the Digital Signature shall be attached to its electronic record and stored or transmitted with its electronic record", the words "*the Digital Signature and the digital signature Certificate attached to its electronic record shall be stored or transmitted along with its electronic record*" shall be substituted;

(b) after rule 5, the following rule shall be inserted, namely:—

"**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 authenticity 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by the licensed Certifying Authorities shall be checked to confirm whether the certificate is valid or whether it has been revoked under Section 38 of the Act;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."

Note: The principal rules were published in the Gazette of India, Extraordinary, vide notification G.S.R.789(E), dated the 17th October, 2000 and subsequent amendment vide notification numbers:—

G.S.R. 902(E), dated 21-11-2003; G.S.R. 245(E), dated 21-4-2005.

G.S.R. 285(E), dated 23-4-2004; G.S.R. 32(E), dated 18-1-2006.

G.S.R. 535(E), dated 20-8-2004; G.S.R. 566(E), dated 5-8-2009.

Notification

Notification, New Delhi, the 25th October, 2011 G.S.R. 783(E).—In exercise of the powers conferred by sub section (1) of Section 87 of the Information Terminology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules to further amend the Information Technology (Certifying Authorities) Rules, 2000, namely:—

1. (1) These rules may be called the Information Technology (Certifying Authorities Amendment) Rules, 2011.

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

2. In the Information Technology (Certifying Authorities) Rules, 2000, (hereinafter referred to as the said rules), in rule 6,—

(a) for the letters, figure and word "SHA-1 and SHA-2" the letters, figure and word "SHA-2" shall be substituted;

(b) for the figures and words "512, 1024, 2048 bit", the figures and words "2048 4096 bit" shall be substituted;

(c) after "Digital Signature Request Format-PKCS#10" the following shall be inserted, namely:—

"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."

3. In Schedule-(iii) to the said rules, in the guidelines, for paragraph 21, the following paragraph shall be substituted namely:—

"21. Usage period 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."

Note:— The principal rules were published in the Gazette of India, Extraordinary, vide notification number G.S.R.789(E), dated the 17th October, 2000 and subsequently amended vide notification numbers:—

G.S.R. 902(E), dated 21-11-2003; G.S.R. 245(E), dated 21-4-2005.

G.S.R. 285(E), dated 23-4-2004; G.S.R. 32(E), dated 18-1-2006.

G.S.R. 535(E), dated 20-8-2004; G.S.R. 566(E), dated 5-8-2009.