The Information Technology (Security Procedure) Rules, 2004

Notification, New Delhi, the 29th October, 2004, G.S.R. 735(E).—In exercise of the powers conferred by clause (e) of sub-section (2) of Section 87, read with Section 16 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:—

1. Short title and commencement.—(1) These rules may be called the Information Technology (Security Procedure) Rules, 2004.

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

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

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

(b) "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 Act;

(c) "hardware token" means a token which can be connected to any computer system using, Universal Serial Bus (USB) port;

(d) "smart card" means a device containing one or more integrated circuit chips, which perform the functions of a computer's centre processor, memory and input or output interface;

(e) words and expressions used in these rules and not defined but defined in the Act shall have the meaning respectively assigned to them in the Act.

3. Secure electronic record.—An electronic record shall be deemed to be a secure electronic record for the purposes of the Act if it has been authenticated by means of a secure digital signature.

4. Secure digital signature.—A digital signature shall be deemed to be a secure digital signature for the purposes of the Act if the following procedure has been applied to it, namely:—

(a) that the smart card or hardware token, as the case may be, with cryptographic module, in it, is used to create the key pair;

(b) that the private key used to create the digital signature always remains in the smart card or hardware token as the case may be;

(c) that the hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system;

(d) that the information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature;

(e) that the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person;

(f) that the standards referred to in rule 6 of the information Technology (Certifying Authorities) Rules, 2000 have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and

(g) that the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated.