रजिस्ट्री सं० डी० एल०-33004/99 REGD. NO. D. L.-33004/99

सत्यमेव जयते

भारत का राजपत्र
The Gazette of India

असाधारण

EXTRAORDINARY

भाग II—खण्ड 3—उप-खण्ड (i)
PART II—Section 3—Sub-section (i)

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 492] नई दिल्ली, शुक्रवार, नवम्बर 5, 2004/कार्तिक 14, 1926
No. 492] NEW DELHI, FRIDAY, NOVEMBER 5, 2004/KARTIKA 14, 1926

IndiaCode

संचार और सूचना प्रौद्योगिकी मंत्रालय

(सूचना प्रौद्योगिकी विभाग)

अधिसूचना

नई दिल्ली, 29 अक्तूबर, 2004

सा.का.नि. 735(अ).—केन्द्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 16 के साथ पठित धारा 87 की उपधारा (2) के खंड (ङ) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, निम्नलिखित नियम बनाती है, अर्थात् :—

1. **संक्षिप्त नाम और प्रारंभ.**—(1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (सुरक्षा प्रक्रिया) नियम, 2004 है।

(2) ये राजपत्र में प्रकाशन की तारीख को प्रवृत्त होंगे।

2. **परिभाषाएं.**—इन नियमों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो,—

(क) "अधिनियम" से सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अभिप्रेत है;

(ख) "अंकीय हस्ताक्षर" से अभिदाता द्वारा अधिनियम की धारा 3 के उपबंधों के अनुसार किसी इलैक्ट्रानिक पद्धति या प्रक्रिया के साधनों द्वारा किसी इलैक्ट्रानिक अभिलेख का अधिप्रमाणन अभिप्रेत है;

(ग) "हार्डवेयर टोकन" से ऐसा कोई टोकन अभिप्रेत है जिसे यूनिवर्सल सीरियल बस पोर्ट का उपयोग करके किसी भी कंप्यूटर प्रणाली से जोड़ा जा सकता है;

(घ) "स्मार्ट कार्ड" से ऐसी युक्ति अभिप्रेत है, जिसमें एक या अधिक एकीकृत परिपथ चिप अंतर्विष्ट हैं, जो किसी कंप्यूटर के केन्द्रीय प्रसंस्कारक, मेमोरी और इनपुट या आउटपुट इंटरफेस कृत्यों का निष्पादन करती है;

(ङ) उन शब्दों और पदों के, जो इन नियमों में प्रयुक्त हुए हैं, और परिभाषित नहीं हैं, किंतु अधिनियम में परिभाषित है, वही अर्थ होंगे, जो अधिनियम में है।

3. **सुरक्षित इलैक्ट्रानिक अभिलेख.**—इस अधिनियम के प्रयोजनों के लिए किसी इलैक्ट्रानिक अभिलेख को तब सुरक्षित इलैक्ट्रानिक अभिलेख समझा जाएगा जब उसका अधिप्रमाणन किसी सुरक्षित अंकीय हस्ताक्षर द्वारा किया गया हो।

4. **सुरक्षित अंकीय हस्ताक्षर.**—इस अधिनियम के प्रयोजनों के लिए कोई अंकीय हस्ताक्षर तब सुरक्षित अंकीय हस्ताक्षर समझा जाएगा जब उसके लिए निम्नलिखित प्रक्रिया को लागू किया गया हो, अर्थात् :—

(क) यह कि यथास्थिति स्मार्ट कार्ड या हार्डवेयर टोकन इसमें क्राईटोग्राफिक मोडयूल के साथ की पेयर सृजित करने के लिए उपयोग किया जाता है;

(ख) यह कि अंकीय हस्ताक्षर सृजित करने के लिए उपयोग की गई निजी कुंजी सदैव यथास्थिति स्मार्ट कार्ड या हार्डवेयर टोकन में रहती है;

(ग) यह कि हस्ताक्षर की जाने वाली अंतर्वस्तु का हैश स्मार्ट कार्ड या हार्डवेयर टोकन की हॉस्ट प्रणाली से लिया जाता है और निजी कुंजी का उपयोग अंकीय हस्ताक्षर सृजित करने के लिए किया जाता है और हस्ताक्षरित हैश को हॉस्ट प्रणाली में वापस कर दिया जाता है;

(घ) यथास्थिति स्मार्ट कार्ड या हार्डवेयर टोकन में अंतर्विष्ट सूचना एकमात्र ऐसे व्यक्ति के नियंत्रण में है, जो अंकीय हस्ताक्षर सृजित करने के लिए तात्पर्यित है;

(ङ) यह कि अंकीय हस्ताक्षर का सत्यापन उस व्यक्ति को जारी किए गए अंकीय हस्ताक्षर प्रमाणपत्र में सूचीबद्ध लोक कुंजी का उपयोग करके किया जा सकेगा;

(च) यह कि सूचना प्रौद्योगिकी (प्रमाणन प्राधिकारी) नियम, 2000 के नियम 6 में निर्दिष्ट मानकों का संबंध जहां तक उनके अंकीय हस्ताक्षर के सृजन, भंडारण और पारेषण से है, का अनुपालन किया गया है;

(छ) यह कि अंकीय हस्ताक्षर को इलैक्ट्रानिक अभिलेख से ऐसी रीति में जोड़ा जाता है यदि इलैक्ट्रानिक अभिलेख को परिवर्तित किया जाता है तो अंकीय हस्ताक्षर अविधिमान्य हो जाएगा।

[फा. सं. 9(8)/2003-ईसी]

एस. लक्ष्मीनारायणन, अपर सचिव

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

(Department of Information Technology)

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 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) "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.

[F. No. 9(8)/2003-EC]

S. LAKSHMINARAYANAN, Addl. Secy.

IndiaCode