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

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. 590] नई दिल्ली, मंगलवार, अक्तूबर 25, 2011/कार्तिक 3, 1933
No. 590] NEW DELHI, TUESDAY, OCTOBER 25, 2011/KARTIKA 3, 1933

संचार और सूचना प्रौद्योगिकी मंत्रालय

(सूचना प्रौद्योगिकी विभाग)

अधिसूचना

नई दिल्ली, 25 अक्तूबर, 2011

सा.का.नि. 782(अ).—केन्द्रीय सरकार सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 87 द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, सूचना प्रौद्योगिकी (प्रमाणकर्ता प्राधिकारी) नियम, 2000 का और संशोधन करने के लिए निम्नलिखित नियम बनाती है, अर्थात :-

1. (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (प्रमाणकर्ता प्राधिकारी) संशोधन नियम, 2011 है।

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

2. सूचना प्रौद्योगिकी (प्रमाणकर्ता प्राधिकारी) नियम, 2000 में :-

(क) नियम 4 में, "और अंकीय चिह्नक के साथ इलेक्ट्रॉनिक अभिलेख होगा तथा उसके इलेक्ट्रॉनिक अभिलेख के साथ भण्डारित या पारेषित किया जाएगा" शब्दों के स्थान पर,

"और इसके इलेक्ट्रॉनिक अभिलेख के साथ संलग्न अंकीय चिह्नक तथा अंकीय चिह्नक प्रमाण पत्र के साथ इसके इलेक्ट्रॉनिक अभिलेख के साथ भण्डारित या पारेसित किया जाएगा"

(ख) नियम 5 के पश्चात निम्नलिखित नियम अंत:स्थापित किया जाएगा, अर्थात् :-

"5 क. अंकीय चिह्नक प्रमाण पत्र का सत्यापन- (क) नियंत्रक द्वारा सृजित स्व-चिह्नक प्रमाण पत्र, जो सार्वजनिक लोक कुंजी अवसंरचना के लिए विश्वसनीय श्रृंखला प्रारंभ करता है, का उपयोग अनुज्ञप्ति प्राप्त प्रमाणकर्ता प्राधिकारी के लोक कुंजी प्रमाण पत्र की प्रामाणिकता के सत्यापन के लिए किया जाएगा।

(ख) अनुज्ञप्ति प्राप्त प्रमाणकर्ता प्राधिक्‍ारी की लोक कुंजी प्रमाण पत्र का उपयोग हस्ताक्षरकर्ता को जारी किए गए अंकीय चिह्नक प्रमाण पत्र की प्रामाणिकता का सत्यापन करने के लिए किया जाएगा।

(ग) अनुज्ञप्ति प्राप्त प्रमाणकर्ता प्राधिकारी द्वारा रखी गई प्रमाण पत्र प्रतिसंहरण सूची की जांच यह सुनिश्चित करने के लिए की जाएगी कि क्या प्रमाण पत्र विधिमान्य है अथवा इसका सूचनां अधिनियम की धारा 38 के अधीन प्रतिसंहरण कर लिया गया है।

(घ) किसी अंकीय चिह्नक की विधिमान्यता का सत्यापन करते समय तदस्थानी अंकीय चिह्नक प्रमाण पत्र जारीकर्ता प्रमाणकर्ता प्राधिकरी की लोक कुंजी प्रमाण पत्र के माध्यम से नियंत्रक के स्व-हस्ताक्षरित प्रमाण पत्र के साथ संलग्न किया जाना चाहिए और यदि विश्वसनीय श्रृंखला में कोई भी प्रमाण पत्र विश्वसनीय नहीं है, तो हस्ताक्षर सत्यापित नहीं किए जाएंगे।"

[फा. सं. 11(11)/2010-सीएलएफई]

एन. रवि शंकर, अपर सचिव

टिप्पणी : मूल नियम भारत के राजपत्र, असाधारण में अधिसूचना सं. सा.का.नि. 789(अ) तारीख 17 अक्तूबर, 2000 द्वारा प्रकाशित किए गए थे और पश्चातवर्ती संशोधन निम्नलिखित अधिसूचना संख्यायों द्वारा किए गए :-

सा.का.नि. 902(अ), तारीख 21.11.2003	सा.का.नि. 245(अ), तारीख 21.4.2005
सा.का.नि. 285(अ), तारीख 23.4.2004	सा.का.नि. 32(अ), तारीख 18.1.2006
सा.का.नि. 535(अ), तारीख 20.8.2004	सा.का.नि. 566(अ), तारीख 5.8.2009

MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY

(Department of Information Technology)

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 certificate 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.".

[F. No. 11(11)/2010-CLFE]

N. RAVI SHANKER, Addl. Secy.

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 subsequently amended vide notification numbers :-

G.S.R. 902(E), dated 21-11-2003
G.S.R. 285(E), dated 23-4-2004
G.S.R. 535(E), dated 20-8-2004
G.S.R. 245(E), dated 21-4-2005
G.S.R. 32(E), dated 18-1-2006
G.S.R. 566(E), dated 5-8-2009

अधिसूचना

नई दिल्ली, 25 अक्तूबर, 2011

सा.का.नि. 783(अ).—केन्द्रीय सरकार सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 87 की उप-धारा (i) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, सूचना प्रौद्योगिकी (प्रमाणकर्ता प्राधिकारी) नियम, 2000 का और संशोधन करने के लिए निम्नलिखित नियम बनाती है, अर्थात :-

1. (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (प्रमाणकर्ता प्राधिकारी) संशोधन नियम, 2011 है।

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

2. सूचना प्रौद्योगिकी (प्रमाणकर्ता प्राधिकारी) नियम, 2000 में, (जिसे इसमें इसके पश्चात् उक्त नियम कहा गया है), नियम 6 में, -

(क) "एसएचए-1 और एसएच-2" अक्षरों, अंकों और शब्दों के स्थान पर "एसएचए-2" अक्षर, अंक रखे जाएंगे;

(ख) "512,1024, 2048 बिट" अंकों और शब्दों के स्थान पर, "2048, 4096 बिट" अंक और शब्द रखे जाएंगे ;

(ग) "अंकीय चिह्नक अनुरोध प्रारूप -पीकेसीएस#10" के पश्चात निम्नलिखित अंत:स्थापित किया जाएगा, अर्थात्:-

"स्पष्टीकरण – एसएचए-1 अंकीय हैश कार्य मानक का उपयोग जारी रखते हुए, सूचना प्रौद्योगिकी (प्रमाणकर्ता प्राधिकारी) संशोधन नियम, 2011 प्रारंभ किए जाने से पूर्व दिए गए अंकीय चिह्नक प्रमाण पत्र में ऐसे प्रमाण पत्रों की समाप्ति की तारीख तक वैध बने रहेंगे।

3. उक्त नियम की अनुसूची 3 के पैरा 21 के लिए मार्ग दर्शन के स्थान पर निम्नलिखित पैरा रखा जाएगा,अर्थात्:-

"21. कुंजियों के लिए प्रचलन की अवधि –

(1) प्रमाणकर्ता प्राधिकारी और हस्ताक्षरकर्ता द्वारा कुंजियों को नियतकालिक रूप से परिवर्तित किया जाएगा।

(2) कुंजी में परिवर्तन कुंजी उत्पादन मार्गदर्शन के अनुसार संसाधित होंगे।

(3) प्रमाणकर्ता प्राधिकारी हस्ताक्षरकर्ता का आश्रय लेने वाले पक्षकारों को अंकीय चिह्नक प्रमाणपत्र पर हस्ताक्षर करने के लिए प्रमाणकर्ता प्राधिकारी द्वारा प्रयुक्त नए कुंजी युग्म में किसी परिवर्तन के बारे में युक्तियुक्त सूचना उपलब्ध कराएगा।

(4) सभी प्रमाणकर्ता प्राधिकारी कुंजी युग्मों और सहबद्ध प्रमाण-पत्रों की विधिमान्यता की अवधि 10 वर्ष से अधिक नहीं होनी चाहिए।

(5) सभी हस्ताक्षरकर्ता कुंजियों के युग्मों और सहबद्ध प्रमाण-पत्रों की विधिमान्यता की अवधि तीन वर्ष से अधिक नहीं होनी चाहिए।"

[फा. सं. 11(4)/2011-सीएलएफई]

एन. रवि शंकर, अपर सचिव

टिप्पणी : मूल नियम भारत के राजपत्र, असाधारण में अधिसूचना सं. सा.का.नि. 789(अ) तारीख 17 अक्तूबर, 2000 द्वारा प्रकाशित किए गए थे और पश्चातवर्ती संशोधन निम्नलिखित अधिसूचना संख्याओं द्वारा किए गए :-

सा.का.नि. 902(अ), तारीख 21.11.2003	सा.का.नि. 245(अ), तारीख 21.4.2005
सा.का.नि. 285(अ), तारीख 23.4.2004	सा.का.नि. 32(अ), तारीख 18.1.2006
सा.का.नि. 535(अ), तारीख 20.8.2004	सा.का.नि. 566(अ), तारीख 5.8.2009

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 Technology 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 Subscriber's 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."

[F. No. 11(4)/2011-CLFE]

N. RAVI SHANKER, Addl. Secy.

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. 285(E), dated 23-4-2004
G.S.R. 535(E), dated 20-8-2004
G.S.R. 245(E), dated 21-4-2005
G.S.R. 32(E), dated 18-1-2006
G.S.R. 566(E), dated 5-8-2009

Printed by the Manager, Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.