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. 530] नई दिल्ली, बुधवार, अगस्त 26, 2015/भाद्र 4, 1937
No. 530] NEW DELHI, WEDNESDAY, AUGUST 26, 2015/BHADRA 4, 1937

संचार और सूचना प्रौद्योगिकी मंत्रालय

(इलैक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग)

अधिसूचना

नई दिल्ली, 25 अगस्त, 2015

सा.का.नि. 660(अ).—केन्द्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 87 द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए निम्नलिखित नियम बनाती है, अर्थात् :--

1. **संक्षिप्त नाम और प्रारंभ.–**

(1) इन नियमों का संक्षिप्त नाम अंकीय हस्ताक्षर (अंतिम निकाय) नियम, 2015 है ।

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

परिभाषाएं–(1) इन नियमों में जब तक कि संदर्भ से अन्यथा अपेक्षित न हो,—

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

(ख) **"कैनोनिकैलाइजोशन",** किसी एक्सएमएल अंकीय हस्ताक्षर के संबंध किसी इलैक्ट्रोनिकी अभिलेख को जिसके एक से अधिक संभव अभ्यावेदन हो सकते हैं को मानक, सामान्य या कैनोनिकल प्ररूप में संपरीवर्तित करने की प्रक्रिया अभिप्रेत है जिसमें इलैक्ट्रोनिकी अभिलेख की प्रस्तुती में भिन्नताओं का संगत नियमों को लागू करके, मुख्यत: एक्सएमएल अंकीय हस्ताक्षर सृजन और सत्यापन प्रक्रियाओं के एक भाग के रूप में मानकीकरण किया जाएगा**;**

(ग) "प्रति हस्ताक्षर" से हस्ताक्षरों की श्रृंखला में पूर्ववर्ती हस्ताक्षर पर इलैक्ट्रानिकी अभिलेख पर हस्ताक्षर के सत्यापन के पश्चात् चस्पा किए गए और क्रम संख्यांक रूप से पूर्ववर्ती हस्ताक्षरों पर पश्चातवर्ती हस्ताक्षर अभिप्रेत हैं;

(घ) "असंबद्ध हस्ताक्षर" वे हस्ताक्षर अभिप्रेत हैं जिनका भंडारण हस्ताक्षर किए जा रहे इलैक्ट्रानिकी अभिलेख से स्वतंत्र किया गया है;

(ङ) "डायजेस्ट विधि एलीमेंट" से किसी एक्सएमएल अंकीय हस्ताक्षर के संबंध में मूल डाटा वस्तु के लिए उपयोग किया गया डायजेस्ट एल्गोरिथ्म या रूपांतरित अबजेक्ट, यदि एक्सएमएल रूपांतरण, विद्यमान है, कोई है अभिप्रेत है;

(च) "डायजेस्टिव एलीमेंट" से डायजेस्ट का मूल्य अभिप्रेत है;

(छ) "सीमांत निकाय" अंशदाता की ओर से अंशदाता या प्रणाली अभिप्रेत है जिसके नाम से इलैक्ट्रोनिकी हस्ताक्षर प्रमाणपत्र जारी किए जाते हैं;

(ज) " सीमांत निकाय हस्ताक्षर" से किसी सीमांत निकाय द्वारा अधिनियम की धारा 3 या 3क के उपबंधों के अनुसरण में अंकीय हस्ताक्षर, इलैक्ट्रानिकी विधि या प्रक्रिया के माध्यम से किसी इलैक्ट्रोनिकी अभिलेख का अधिप्रमाणन अभिप्रेत है;

(झ) "परिवेष्टित हस्ताक्षर" हस्ताक्षर और आरंभिक इलैक्ट्रानिकी अभिलेख का किसी अन्य इलैक्ट्रानिकी अभिलेख में परिवेष्टन अभिप्रेत है;

(ञ) "हस्ताक्षर का परिवेष्टन" से किसी हस्ताक्षर का परिवेष्टन अभिप्रेत है जिसको हस्ताक्षर तत्व के भीतर निर्दिष्ट और अंतर्विष्ट किया गया;

(ट) "आरंभिक इलैक्ट्रानिक अभिलेख", से किसी एक्सएमएल अंकीय हस्ताक्षर प्रक्रिया के संदर्भ में हस्ताक्षरित सूचना का कैनोनिकेलाइज्ड और रूपांतरित प्ररूप अभिप्रेत है;

(ठ) "कीइन्फो तत्व" से कोई तत्व अभिप्रेत है जो किसी की सूचना को हस्ताक्षर तत्व के साथ पैक करने में समर्थ बनाता है;

(ड) "दीर्घावधि हस्ताक्षर" से कोई हस्ताक्षर तत्व अभिप्रेत है जिसे हस्ताक्षरों में अप्राधिकृत परिवर्तनों का पता लगाने में समर्थ होने के लिए कार्यान्वियनकारी उपायों द्वारा दीर्घावधि के लिए सत्यापन के योग्य बनाया गया है;

(ढ) "प्रमुख तत्व", से किसी एक्सएमएल अंकीय हस्ताक्षर के संबंध में एक संदर्भ तत्वों के प्रसंस्करणकारी माडल को पूरा करने के लिए अनुप्रयोग द्वारा परिभाषित कोई ढांचा अभिप्रेत है ;

(ण) "वस्तु तत्व" से एक्सएमएल अंकीय हस्ताक्षर का कोई वैकल्पिक तत्व अभिप्रेत है जिसका उपयोग हस्ताक्षरों के परिवेष्टन के लिए वहां किया जाता है जहां हस्ताक्षर की जा रही डाटा वस्तु को एक्सएमएल में शामिल किया जाएगा;

(त) "ओसीएसपी रिस्पोंडम" से कोई ऑनलाइन सेवा अभिप्रेत है जो अंकीय हस्ताक्षर प्रमाण पत्र की प्रतिसंह्रण प्रास्थिति का उपबंध करती है;

(थ) "ऑनलाइन प्रमाण पत्र प्रास्थिति प्रोटोकॉल" से ऑनलाइन प्रमाण पत्र प्रतिसंह्रण जांच प्रोटोकॉल अभिप्रेत है जो परेषणकारी पक्षकारों को किसी पहचाने गए अंकीय हस्ताक्षर प्रमाण पत्र की प्रतिसंह्रण प्रास्थिति का अवधारण करने में सक्षम बनाता है ;

(द) "समानांतर हस्ताक्षरों" से उसी इलैक्ट्रानिकी अभिलेख के ऊपर एक या अधिक स्वतंत्र हस्ताक्षर अभिप्रेत हैं जिसमें हस्ताक्षरों का क्रम महत्वपूर्ण नहीं है;

(ध) किसी एक्सएमएल अंकीय हस्ताक्षर के संदर्भ में **"संदर्भ तत्व"**, से कोई तत्व अभिप्रेत है जो डाटा पदार्थों को, डाइजेस्ट से पूर्व अनुप्रयुक्त करने के लिए रूपांतरणों की वैकल्पिक सूची (एक्सएमएल रूपांतरण), डाइजेस्ट विधि और निर्दिष्ट किए गए डाटा पदार्थों का डाइजेस्ट मूल्य का वहन करता है;

(न) किसी एक्सएमएल अंकीय हस्ताक्षर के संबंध में **"हस्ताक्षरित सूचना"**, से कोई तत्व अभिप्रेत है जिसमें किसी एक्सएमएल हस्ताक्षर का सृजन करने के लिए हस्ताक्षरित किए जाने के लिए सूचना का कोई सेट अंतर्विष्ट है, जहां इसमें किसी डाटा पदार्थ के लिए निर्देश अंतर्विष्ट है जिसमें कैनोनिकैलाइजेशन और हस्ताक्षर एल्गोरिथ्म शामिल हैं;

(प) **"हस्ताक्षर"** से अंकीय हस्ताक्षर या एक्सएमएल अंकीय हस्ताक्षर अभिप्रेत है;

(फ) **"हस्ताक्षर मूल्य"** से कोई तत्व अभिप्रेत है जो अंकीय हस्ताक्षर का वास्तविक मूल्य है;

(ब) **"हस्ताक्षर विधि "** से कोई तत्व अभिप्रेत है जिसमें हस्ताक्षर सृजन के लिए उपयोग किया गया एल्गोरिथ्म अंतर्विष्ट है और एल्गोरिथ्म हस्ताक्षर के सृजन में अंतवर्लित सभी कूटकारी कृत्यों की पहचान करता है;

(भ) **"हस्ताक्षर अभिलक्षण"** से कोई तत्व अभिप्रेत है जो हस्ताक्षर के विषय में अतिरिक्त सूचना जैसे समय स्टैंप या कोई अन्य सूचना जो अनुप्रयोग द्वारा परिभाषित है, को पूरा करने का उपबंध करता है;

(म) **"समय स्टैंप"** से केाई अंकन अभिप्रेत है जो किसी कार्रवाई की सही तारीख और समय को उपदर्शित करता है तथा उस व्यक्ति या युक्ति की पहचान करता है जिसमें समय स्टैंप को भेजा या प्राप्त किया है और समय स्टैंप टोकन को प्रवृत्त करता है;

(य) **"समय स्टैंप टोकन"** से किसी समय स्टैंप सेवा प्रदाता के अंकीय हस्ताक्षर का उपयोग करके सृजित कूट रूप से सुरक्षित पुष्टि अभिप्रेत है और इसके अंतर्गत वह समय भी है जब पुष्टि का सृजन किया गया था ;

(यक) **"समय स्टैंप सेवा प्रदाता"** से समय स्टैंप सृजित करने के लिए कोई विश्वसनीय निकाय अभिप्रेत है;

(यख) **"एक्सएमएल"** से एक्सटेंसीबल मार्कअप लैंग्वेज अभिप्रेत है जो एक औपचारिक सिंटैक्स के साथ सूचना के तत्वों की पहचान करने के लिए मानक विधि उपलब्ध कराती है, डाटा अवसंरचना का वर्णन करती है और एक स्वतंत्र रीति में डाटा का भंडारण भी करती है, इसकी निम्नलिखित विशेषताएं होंगी,—

(i) एक्सएमएल के साथ अंतर्वस्तु और प्रस्तुतीकरण पृथक् हैं;

(ii) किसी विशिष्ट संदर्भ में एक्सएमएल डाटा की अवसंरचना का वर्णन या तो एक्सएमएल स्कीम या दस्तावेज किस्म की परिभाषा का उपयोग करके किया जाता है ;

(iii) एक्सएमएल स्कीम या दस्तावेज किस्म की परिभाषा का भंडारण स्वयं एक्सएमएल दस्तावेज से पृथक् किया जाता है और इसका उपयोग पुष्टि के लिए किसी दिए गए एक्सएमएल दस्तावेज को विधिमान्य बनाने के लिए किया जा सकता है ;

(यग) **"एक्सएमएल अंकीय हस्ताक्षर तत्व"** से कोई तत्व अभिप्रेत है जिसको एक्सएमएल प्ररूप में एकपक्षीय डाटा को प्रयुक्त अंकीय हस्ताक्षर प्रचालन के परिणाम को कैप्चर करने के लिए मानक एक्सएमएल स्कीम को परिभाषित करता है, यह निम्नलिखित को पूरा करेगा,—

(i) एक्सएमएल अंकीय हस्ताक्षर तत्व एक मानक दस्तावेज के रूप में विद्यमान होगा या उस डाटा वस्तु को परावेष्टिक करेगा जिसे यह हस्ताक्षरित करता है ;

(ii) एक्सएमएल अंकीय हस्ताक्षर तत्व की हस्ताक्षरित सूचना, हस्ताक्षरित मूल्य, मुख्य सूचना, तत्व होगा और इसके उनके प्रकट होने वाले क्रम में टाइप चाइल्ड तत्व अभिलक्षण होंगे;

(यघ) **"एक्सएमएल अंकीय हस्ताक्षर"** से एक्सएमएल इलैक्ट्रानिकी अभिलेख पर अंकीय हस्ताक्षर अभिप्रेत हैं;

(यङ) **"एक्सएमएल दस्तावेज"** एक्सएमएल तर्क और भौतिक संरचना के साथ दस्तावेज अभिप्रेत है जिसका उपयोग डाटा तत्व के वहन के लिए घोषणाओं की संरचना, तत्वों, टिप्पणियों, विशेषता संदर्भों और अनुदेशों के प्रसंस्करण और निकायों से मिलकर बनने वाली भौतिक संरचना के लिए किया जाता है जो मूल या दस्तावेज प्रविष्टि से आरंभ होता है ;

(यच) **"एक्सएमएल स्कीम"** से पूर्व परिभाषित या उपयोगकर्ता द्वारा परिभाषित की वर्ड और अवसंरचनात्मक रीति में इकट्ठे किए गए उनके अभिलक्षण अभिप्रेत हैं, जो निम्नलिखित को पूरा करते हैं **,—**

(i) किसी विशिष्ट प्रयोजन के लिए इस्तेमाल किए जाने चाहिएं जहां एक स्कीम के रूप में किसी एक्सएमएल दस्तावेज की अवसंरचना का वर्णन करते हैं और तत्व नामों की विशिष्टियों का उपबंध करते हैं जो यह उपदर्शित करती हैं कि किसी एक्सएमएल दस्तावेज में किन तत्वों को और किन संयोजनों में अनुज्ञात किया जाएगा**;** और

(ii) उन्हें विस्तारित क्रियाशीलता जैसे डाटा किस्म, विरासत और प्रस्तुतीकरण नियम तथा अभिलक्षणों के लिए डिफाल्ट मूल्य **;**

(यछ) **"एक्सएमएल रूपांतरण"** से कोई तत्व अभिप्रेत है किसी डाटा वस्तु को उसको डाइजेस्ट करने से पूर्व प्रसंस्करण उपायों की कोई वैकल्पिक क्रमवार सूफी को विनिर्दिष्ट करता है जहां रूपांतरण में कैनोनिकैलाइजेशन, कूटकरण या कूटकरण को हटाने विस्तृत स्टाइल शीट भाषा रूपांतरण, एक्सपाथ फिल्टरीकरण और एक्सएमएल स्कीम विधिमान्यकरण शामिल है**;**

(यज) **"एक्सएमएल नेमस्पेस"** से यूनीफार्म रिसोर्स आइडेंटीफायर (यूआरआई) निर्देश अभिप्रेत है जहां विशिष्टि में वर्णित तंत्रों का उपयोग एक्सएमएल दस्तावेजों में तत्व किस्म और अभिलक्षण नाम के रूप में किया जाता है और नामों के टकराव के बिना विभिन्न एक्सएमएल शब्दकोशों का भी उपयोग किया जाता है ।

(2) वे शब्द और पद जो इसमें प्रयुक्त हैं, परिभाषित नहीं हैं किंतु अधिनियम में परिभाषित हैं का क्रमश: वही अर्थ होगा जो उनका उक्त अधिनियम में है ।

3. अंकीय हस्ताक्षर के माध्यम से सूचना के अधिप्रमाणन की रीति.—किसी अंकीय हस्ताक्षर**,—**

(क) का सृजन और सत्यापन कूटकरण द्वारा किया जाएगा जो किसी इलैक्ट्रानिकी अभिलेख को प्रत्यक्ष रूप से दुर्बोध प्ररूप में रूपांतरित करने से संबंधित है**;**

(ख) किसी लोक कुंजी कूटकरण का लोप करेगा जिसमें किसी दो भिन्न किंतु गणितीय रूप से संबंधित कुंजियों का उपयोग करते हुए किसी अल्गोरिदम का उपयोग किया जाता है **;** एक कुंजी (जिसे प्राइवेट कुंजी कहा जाता है) का उपयोग अंकीय हस्ताक्षर के सृजन के लिए और दूसरी कुंजी का उपयोग (जिसे पब्लिक कुंजी कहा जाता है) अंकीय हस्ताक्षरों के सत्यापन के लिए किया जाता है ।

(ग) किसी अंकीय हस्ताक्षर के सृजन और सत्यापन के लिए हैश कृत्य का उपयोग जो अंकीय हस्ताक्षर सृजन और सत्यापन फलोत्पादक अंकीय हस्ताक्षर बनाने के लिए अपेक्षित है ।

4. अंकीय हस्ताक्षर का सृजन.—(1) हस्ताक्षरकर्ता किसी इलैक्ट्रानिकी अभिलेख पर हस्ताक्षर करते समय या सूचना की किसी अन्य मद पर हस्ताक्षर करते समय प्रथमत: हस्ताक्षरकर्ता के हार्डवेयर या साफ्टवेयर में एक हैश फंक्शन को लागू करेगा।

(2) हैश फंक्शन एक हैश परिणाम प्रस्तुत करेगा ।

(3) हस्ताक्षरकर्ता का हार्डवेयर या साफ्टवेयर तब हैश परिणाम को हस्ताक्षकर्ता की प्राइवेट की और हस्ताक्षर एल्गोरिदम का उपयोग करते हुए एक अंकीय हस्ताक्षर में रूपांतरित कर देगा ।

(4) तारीख और समय जैसी परिप्रेक्ष्य जानकारी को तब अंकीय हस्ताक्षर का भाग बनाया जाए ।

(5) प्रति हस्ताक्षर या समानांतर हस्ताक्षर या दोनों को भी इलैक्ट्रोनिकी अभिलेख को लागू किया जा सकेगा ।

(6) निम्नलिखित सूचना भी हस्ताक्षर का भाग हो सकेगी,—

(क) हस्ताक्षरकर्ता के लोक की हस्ताक्षर प्रमाण पत्र**;**

(ख) अनुज्ञप्त प्रमाणीकरण प्राधिकारियों के लोक की प्रमाण पत्र जो हस्ताक्षरकर्ता को जारी अंकीय हस्ताक्षर प्रमाण पत्र की अधिप्रमाणत: का सत्यापन करते हैं**;**

(ग) नियंत्रक के स्वयं हस्ताक्षरित सृजित प्रमाण पत्र जिनका उपयोग अनुज्ञप्त प्रमाणीकरण प्राधिकारियों के लोक की प्रमाण पत्रों की अधिप्रमाणत: का सत्यापन करने के लिए किया जाता है **;**

(घ) अनुज्ञप्त प्रमाणीकरण प्राधिकारियों और नियंत्रक द्वारा अनुरक्षित प्रमाण पत्र प्रतिसंह्लण सूची (सूचियां) और जिनका उपयोग यह जांच करने के लिए किया जाता है कि अंकीय हस्ताक्षर प्रमाण पत्र का अधिनियम की धारा 38 के अधीन प्रतिसंह्लण कर लिया गया है;

(ड.) ऑनलाइन प्रमाण पत्र प्रास्थिति प्रोटोकॉल रेस्पोंडर प्रमाण पत्र और ऑनलाइन प्रमाण पत्र प्रास्थिति प्रोटोकॉल रिस्पोंसेस जिनका उपयोग प्रमाण पत्र प्रतिसंह्लण सूची के स्थान पर किया जाता है।

(7) दीर्घाविधि मान्य प्रमाण पत्र सृजित करने के लिए,-

(क) प्रारंभ में हस्ताक्षरित डाटा जिसके अंतर्गत प्रमाणपत्र और प्रतिसंह्लण सूचना है को समय स्टैंप लागू की जाएगी;

(ख) यह सुनिश्चय करना की समय स्टैंप सभी डाटा और हस्ताक्षर (रों) को कवर करती है ;

(ग) एक नेस्टड समय स्टैंप विकल्प का उपयोग समय स्टैंप सेवा प्रदाता (टीएसएसपी) कुंजी या एल्गोरिदम अवसान जहां समय स्टैंपों की नेस्टिंग यह दर्शाती है कि पश्चातवर्ती समय स्टैंप पूर्व समय स्टैंप को लागू की जाएगी के पश्चात् हस्ताक्षर की विधिमान्यता का सुनिश्चय करना

(घ) हस्ताक्षर और समय स्टैंप को स्वयं डाटा में ही रखा जाएगा या उनका पृथक् रूप से एक अलग के रूप में भंडारण किया जाएगा।

5. **अंकीय हस्ताक्षर का सत्यापन.—**(1) अंकीय हस्ताक्षर के सत्यापन को अंकीय हस्ताक्षर के सृजन के लिए हैश फंक्शन के माध्यम से मूल इलैक्ट्रानिकी अभिलेख के नए हैश परिणाम की संगणना करने के माध्यम से लोक कुंजी का उपयोग करके पूरा किया जाएगा, सत्यापनकर्ता निम्नलिखित की जांच करेगा—

(क) यदि अंकीय हस्ताक्षरों का सृजन तत्स्थानी प्राइवेट का उपयोग करते हुए किया गया था और वे इलैक्ट्रानिकी अभिलेख, यदि विद्यमान हो के लिए समानांतर और प्रति हस्ताक्षरों पर लागू होंगे।

(ख) वह समय जब अंकीय हस्ताक्षर का सृजन किया गया था।

(2) प्रतिहस्ताक्षर का सत्यापन करने के लिए इलैक्ट्रानिकी अभिलेख पर हस्ताक्षर और तत्पश्चात् पूर्ववर्ती हस्ताक्षर पर हस्ताक्षर को क्रमवर्ती रूप से सत्यापित किया जाएगा।

(3) समानांतर हस्ताक्षर का सत्यापन करने के लिए इलैक्ट्रानिकी अभिलेख पर हस्ताक्षर को स्वतंत्र रूप से सत्यापित किया जाएगा।

(4) दीर्घावधि हस्ताक्षर का सत्यापन करने के लिए आरंभिक समय स्टैंप और सभी पश्चातवर्ती समय स्टैंप जिसको प्रत्येक पूर्ववर्ती स्टैंप पर लागू किया गया था का सत्यापन लाग किया गया था।

6. अंकीय हस्ताक्षर प्रमाणपत्र .—(1) स्वयं द्वारा हस्ताक्षरित प्रमाणपत्र जिसका सृजन नियंत्रक द्वारा किया गया था, जो लोक कुंजी अवसंरचना के लिए विश्वास दावा आरंभ करता है, का उपयोग अनुज्ञप्त प्रमाणीकरण प्राधिकारियों के लोक कुंजी प्रमाणपत्र की अधिप्रमाणिता का सत्यापन करने के लिए किया जाएगा ।

(2) अनुज्ञप्त प्रमाणीकरण प्राधिकारियों के **लोक कुंजी** प्रमाणपत्र का उपयोग अंशदाताओं को जारी अंकीय हस्ताक्षर प्रमाणपत्र की अधिप्रमाणिता का सत्यापन करने के लिए किया जाएगा ।

(3) अनुज्ञप्त प्रमाणीकरण प्राधिकारियों द्वारा रखी गई प्रमाणपत्र प्रतिसंह्लण सूची की जांच या पुष्टि करने के लिए की जाएगी कि क्या अनुज्ञप्त प्रमाणीकरण प्राधिकारियों का प्रमाणपत्र विधिमान्य है या इसका अधिनियम की धारा 38 के अधीन प्रतिसंह्लण कर लिया गया है ।

(4) अंकीय हस्ताक्षर की विधिमान्यता का सत्यापन करते समय तत्स्थानी अंकीय हस्ताक्षर प्रमाणपत्र को जारी करने वाले प्रमाणीकरण प्राधिकारी के लोक कुंजी प्रमाणपत्र के माध्यम से स्वयं द्वारा हस्ताक्षरित नियंत्रक के प्रमाणपत्र को श्रृंखलाबद्ध करके और यदि विश्वसनीय श्रृंखला में कोई प्रमाणपत्र विश्वसनीय नहीं है तो हस्ताक्षर का सत्यापन नहीं किया जाएगा।

(5 अंकीय हस्ताक्षर प्रमाणपत्र का सत्यापन हस्ताक्षर के सृजन के समय की बाबत किया जाएगा ।

(6) प्रमाणपत्रों की श्रृंखला का सत्यापन नियम 7 में मानकों के अनुसार किया जाएगा ।

(7) यदि प्रमाणपत्र की विधिमान्यता एक घंटे से कम है तो प्रतिसंहरण सूची की जांच अपेक्षित नहीं है ।

7. अंकीय हस्ताक्षर मानक—सबसे महत्व मानक जो अंकीय हस्ताक्षर कृत्यों से संबंधित विभिन्न कार्यकलापों को लागू होंगे, नीचे दिए अनुसार हैं —

उत्पाद	**मानक**
कूट कृत हैश फंक्शन	एसएचए-2 जैसा एफआईपीएस 180-4 में विनिर्दिष्ट है
आरएसए लोक कुंजी प्रौद्योगिकी	पीकेसीएस#1 आरएसए कूटकरण मानक ([2048, 4096 बिट]); संस्करण 1.5
कूटकरण और अंकीय हस्ताक्षर	पीकेसीएस #7, सीएमएस
अंकीय हस्ताक्षर प्रमाणपत्र की विधिमान्यता	आरएफसी 5280
ईसीसी कर्व	एनआईएसटी पी-256, पी-384, या पी-521
दीर्घावधि हस्ताक्षर प्ररूप	1. CAdES आरएफसी 5126, 2. PAdES with CAdES
समय स्टैंप टोकन	जैसा आरएफसी 3161 में विनिर्दिष्ट है

8 **एक्सएमएल अंकीय हस्ताक्षर के माध्यम से सूचना के अधिप्रमाणन की रीति—**एक्सएमएल अंकीय हस्ताक्षर,—

(क) **का बीज लेखन के माध्यम से सृजन और सत्यापन किया जाएगा जो इलैक्ट्रानिकी अभिलेख को प्रत्यक्षत: अबोध्य प्ररूप में रूपांतरित करने से संबंधित है** ;

(ख) लोक कुंजी बीज लेखन का उपयोग जो दो भिन्न किंतु गणीतीय रूप से संबद्ध कुंजियों, एक कुंजी (जिसे प्राइवेट कुंजी कहा जाता है) का उपयोग एक्सएमएल अंकीय हस्ताक्षर और दूसरी कुंजी (जिसे लोक कुंजी कहा जाता है) का उपयोग एक्सएमएल अंकीय हस्ताक्षर का सत्यापन करने के लिए एक एल्गोरिदम का इस्तेमाल करता है;

(ग) बीज लेखन हैश फंक्शन का किसी एक्सएमएल अंकीय हस्ताक्षर के सृजन और सत्यापन के लिए उपयोग;

(घ) कैनोनिकैनाइजेशन और एक्सएमएल रूपांतरण का उपयोग मानक इलैक्ट्रानिकी अभिलेख का एक्सएमएल अंकीय हस्ताक्षर का सृजन और सत्यापन से पूर्व सृजन के लिए उपयोग;

(ङ) ऐसे एक्सएमएल दस्तावेजों का अधिप्रमाणन जिनमें डाटा एक निर्देश और तत्स्थानी हैश के रूप में अंतर्विष्ट है जो हैश एल्गोरिदम, कैनोनिकैनाइजेशन, एक्सएमएल रूपांतरण और लोक कुंजी एल्गोरिदम के उपयोग से प्रभावित होता है

9. एक्सएमएल अंकीय हस्ताक्षर का सृजन .—(1) किसी इलैक्ट्रानिकी अभिलेख या सूचना की किसी अन्य मद पर हस्ताक्षर करते समय हस्ताक्षरकर्ता पहले संदर्भ तत्वों, एक्सएमएल अंकीय हस्ताक्षर तत्व, हस्ताक्षरित सूचना, कुंजी सूचना और हस्ताक्षर मूल्य का संनिर्माण करेगा ।

(2) **संदर्भ तत्व के सृजन के लिए, हस्ताक्षाकारी साफ्टवेयर निम्नलिखित कृत्यों को करेगा**—

(क) सूचना की मद, एक्सएमएल रूपांतरण तत्व (वैकल्पिक), डाइजेस्ट एल्गोरिदम और डाइजेस्ट मूल्य के संदर्भ में संदर्भ तत्वों का सृजन करेगा ;

(ख) वैकल्पिक रूप से एक्सएमएल रूपांतरणों को प्रत्येक निर्दिष्ट वस्तु में क्रमवार रूप से लागू करेगा;

(ग) हस्ताक्षरकर्ता के हार्डवेयर या साफ्टवेयर में हैश फंक्शन को प्रत्येक निर्दिष्ट तत्व को लागू करेगा, हैश परिणाम को निर्दिष्ट तत्व में भंडारित करेगा;

(घ) यह सुनिश्चित करेगा कि यदि लक्षित तत्व का सृजन किया जाता है तो उसमें प्रमुख तत्व नहीं होगा ;

(ङ) यह सुनिश्चित करेगा कि विशिष्ट कैनोनिकलाइजेशन "बिना टिप्पाणियों के" को अनिवार्यत: किसी अन्य रूपांतरण के विनिर्दिष्ट किया गया है ।

(3) **एक्सएमएल अंकीय हस्ताक्षर** सृजन के प्रयोजन के लिए, हस्ताक्षरकर्ता साफ्टवेयर निम्नलिखित कृत्य करेगा—

(क) हस्ताक्षर विधि, कैनोनिकेलाजेशन विधि और निर्देशों के साथ हस्ताक्षर सूचना का सृजन करेगा ;

(ख) हस्ताक्षर सूचना को कैनोनिकेलाजेशन लागू करेगा और कैनोनिकेलाइजड सूचना के हैस मूल्य का हैसिंग एल्गोरिदम का उपयोग करते हुए हस्ताक्षर विधि से संगणना करेगा ;

(ग) सुनिश्चित करेगा कि,—

(i) हस्ताक्षरकर्ता के पास हस्ताक्षर करने से पूर्व दस्तावेज की सभी अंतर्वस्तु है ;

(ii) स्वचालित हस्ताक्षर करने की प्रक्रिया की दशा में अंतर्वस्तु प्रदर्शन अपेक्षाओं की अपेक्षा नहीं है ;

(iii) एक साथ बहुसंसाधनों पर हस्ताक्षर करने के लिए,—

(क) प्रत्येक संसाधन को सक्रिन पर डाला जाएगा ;

(ख) प्रत्येक एक्सएमएल संदर्भ संसाधन को एक्सएलटी का उपयोग करते हुए डाला जाएगा और एक्सएलटी संसाधन को सक्रिन पर डालने के लिए किया गया अंतिम रूपांतरण होगा ;

(ग) प्रत्येक गैर एक्सएमएल संसाधन को माइम किस्म अभिलक्षण, जो आबजेक्ट में वर्णित है, का उपयोग करते हुए डाला जाएगा ;

(घ) हस्ताक्षर एल्गोरिवदम हैस, हस्ताक्षकर्ता की प्राइवेट कुंजी और पब्लिक कुंजी पैरामीटर (यदि लागू हों) का उपयोग करते हुए, हस्ताक्षर का सृजन किया जाएगा और कार्यकरण आधारित हस्ताक्षर परिणाम का 64 मूल कूटकरण परिणाम और उसका उपयोग हस्ताक्षर मूल्य के प्ररूपण के लिए किया जाएगा ;

(ङ) हस्ताक्षर तत्वों का संनिर्माण, जिसके अंतर्गत हस्ताक्षरित सूचना, सूचना की मद्दे एक्स 509 प्रमाणपत्र तत्व के साथ कुंजी सूचना और हस्ताक्षर मूल्य तथा एक्स 509 प्रमाणपत्र तत्व हस्ताक्षरकर्ता की एक्स 509 लोक कुंजी प्रमाणपत्र को कैरी करेंगे ।

(4) संदर्भिक सूचना, जैसे तारीख और समय को तब एक्सएमएल अंकीय हस्ताक्षर का भाग बनाया जाएगा ।

(5) प्रति हस्ताक्षर या समानांतर हस्ताक्षर या दोनों को भी इलैक्ट्रानिक अभिलेख में लागू किया जा सकेगा ।

(6) निम्नलिखित सूचना भी हस्ताक्षर का भाग हो सकेगी—

(क) हस्ताक्षरित प्रमाणीकरण प्राधिकारियों के लोक कुंजी प्रमाणपत्र, जो हस्ताक्षकर्ता को जारी अंकीय हस्ताक्षर प्रमाणपत्र की अनुप्रमाणिता का सत्यापन करते हैं ;

(ख) नियंत्रक द्वारा सृजित स्वय: द्वारा हस्ताक्षरित प्रमाणपत्र, जो अनुज्ञप्त प्रमाणीकरण प्राधिकारियों की लोक कुंजी प्रमाणपत्रों की अनुप्रमाणिकता का सत्यापन करने के लिए उपयोग किए जाते हैं ;

(ग) अनुज्ञप्त प्रमाणीकरण प्राधिकारियों और नियंत्रक द्वारा रखी गई प्रमाणपत्र प्रतिसंहरण सूची, जिसका उपयोग यह जांच करने के लिए किया जाता है कि क्या अंकीय हस्ताक्षर प्रमाणपत्र का अधिनियम की धारा 38 के अधीन प्रतिसंहरण कर लिया गया है ;

(घ) ऑनलाइन प्रमाणपत्र प्रास्थिति प्रोटोकाल रिस्पोंडर प्रमाणपत्र और ऑनलाइन प्रमाणपत्र प्रास्थिति अनुक्रियाओं का उपयोग प्रमाणपत्र प्रतिसंहरण सूची के स्थान पर किया जा सकेगा ।

(7) दीर्घावधि विधिमान्य एक्सएमएल अंकीय हस्ताक्षर का सृजन करने के लिए निम्नलिखित कृत्य किए जाएंगे—

(क) प्रारंभ में हस्ताक्षरित दस्तावेज पर एक समय स्टॉप लगाई जाएगी, जहां आरंभिक समय स्टॉप सभी इलैक्ट्रानिक अभिलेख और हस्ताक्षरों को कवर करेगी ;

(ख) एक नेस्टेड समय स्टॉप विकल्प का उपयोग समय स्टाम्पिंग सेवा प्रदात्ता (टीएसएसपी) के कुंजी या एल्गोरिदम के अवसान के पश्च हस्ताक्षर की विधिमान्यता का सुनिश्चय करने के लिए किया जाएगा, जहां समय स्टॉपों की नेस्टिंग का यह अर्थ है कि पश्चातवर्ती समय स्टॉप पूर्व समय स्टॉप को लागू की जाएगी ;

(ग) हस्ताक्षर और समय स्टॉपों को डाटा में ही रखा जा सकेगा या पृथक् रूप में एकल के रूप में भंडारित किया जाएगा ।

10. एक्सएमएल अंकीय हस्ताक्षर का सत्यापन.—(1) एक्सएमएल अंकीय हस्ताक्षर के सत्यापन को हस्ताक्षर के विधिमान्यकरण, संदर्भ विधिमान्यकरण और प्रमाणपत्र विधिमान्यकरण के द्वारा पूरा किया जाएगा और एक्सएमएल अंकीय हस्ताक्षर को केवल तभी विधिमान्य माना जाएगा यदि हस्ताक्षर विधिमान्यकरण, संदर्भ विधिमान्यकरण और प्रमाणपत्र विधिमान्यकरण जैसा नीचे विनिर्दिष्ट किया गया है, का अनुपालन किया गया हो ।

(2) हस्ताक्षर विधिमान्यकरण को निम्नलिखित के माध्यम से पूरा किया जाएगा—

(क) संदर्भ विधिमान्यकरण के दौरान तैयार की गई हस्ताक्षर सूचना का कैनोनिकल प्ररूप का उपयोग किया जाएगा ;

(ख) कैनोनिकलाइजेशन विधि का उपयोग करते हुए हस्ताक्षर पद्धति के कैनोनिकल प्ररूप को अभिप्राप्त किया जाएगा ;

(ग) हस्ताक्षरकर्ता के एक्स 509 प्रमाणपत्र में अंतर्विष्ट लोक कुंजी, जिसे एक्सएमएल अंकीय हस्ताक्षर में सम्मिलित किया गया है, हस्ताक्षर सूचना, हस्ताक्षर मूल्य का कैनोनिकलाइजेड प्ररूप और हस्ताक्षर पद्धति के कैनोनिकलाइजेड प्ररूप का हस्ताक्षर का सत्यापन करने के लिए उपयोग किया जाएगा ;

(3) संदर्भ विधिमान्यकरण को प्राप्त करने के लिए निम्नलिखित का उपयोग किया जाएगा—

(क) हस्ताक्षर सूचना में कैनोनिकलाइजेशन विधि के आधार पर हस्ताक्षर सूचना तत्व के कैनोनिकलाइज का उपयोग किया जाएगा ;

(ख) हस्ताक्षर सूचना में प्रत्येक संदर्भ के लिए--

(i) यदि हस्ताक्षरकर्ता द्वारा रूपांतरणों को लागू किया जाता है, तब सत्यापनकर्ता साफ्टवेयर यूनिफोर्म रिसोस आइडेन्टीफायर (यूआरआई) को डीरेफरेंस कर देगा और रेफरेंस तत्व में हस्ताक्षरकर्ता द्वारा उपबंधित रूपांतरणों को निष्पादित करेगा ;

(ii) रेफरेंस तत्व में विनिर्दिष्ट डाइजेस्ट पद्धति का उपयोग करते हुए रेफरेंस्ड मद के डाइजेस्ट की संगणना करेगा ;

(iii) हस्ताक्षरित सूचना रेफरेंस में डाइजेस्ट मूल्य के विरुद्ध संगणित डाइजेस्ट मूल्य की तुलना करेगा ।

(4) एक्सएमएल अंकीय हस्ताक्षर में सम्मिलित अंकीय हस्ताक्षर प्रमाणपत्र का नियम 6 में विनिर्दिष्ट उपबंधों के अनुसार सत्यापन किया जाएगा ।

(5) प्रति हस्ताक्षर का सत्यापन करने के लिए इलैक्ट्रानिक अभिलेख पर पहले हस्ताक्षर और पूर्ववर्ती हस्ताक्षर पर हस्ताक्षरों का क्रम संख्यंक रूप से सत्यापन किया जाएगा ।

(6) समानातर हस्ताक्षरों का सत्यापन करने के लिए इलैक्ट्रानिक अभिलेख पर हस्ताक्षर का स्वतंत्र रूप से सत्यापन किया जाएगा ।

(7) दीर्घावधि हस्ताक्षर का सत्यापन करने के लिए आरंभिक समय स्टॉप और प्रत्येक पूर्ववर्ती समय स्टॉप पर सभी पश्चातवर्ती लागू समय स्टॉप का सत्यापन किया जाएगा ।

11. एक्सएमएल अंकीय हस्ताक्षर मानक.—सबसे महत्वपूर्ण मानक, जिन्हें एक्सएमएल अंकीय हस्ताक्षर कृत्यों के साथ सहबद्ध विभिन्न कार्यकलापों के लिए लागू किया जाएगा, नीचे दिए अनुसार है—

उत्पाद	मानक
एक्सएमएल अंकीय हस्ताक्षर मानक	आरएफसी 3275 निम्नलिखित कन्सट्रेंट्स के साथ ○ किसी ओबजेक्ट के अंदर मेनीफिस्ट अनुज्ञात नहीं है, ○ एक्स 509 प्रमाणपत्र को अंतर्विष्ट करते हुए कुंजी सूचना आज्ञापक है ○ रेफरेंस प्रक्रिया अनन्य कैनोनिकलाइजेशन का (बिना टिप्पणियों के) अन्य रूपांतरणों के अतिरिक्त उपयोग करेगी ○ एक्सएमएल स्रोत के लिए एक्सएसएलटी स्क्रीन पर दस्तावेज को रखने में समर्थ बनाने के लिए किया गया अंतिम रूपांतर होगा ○ स्क्रीन पर दस्तावेज को रखने के लिए ○ प्रत्येक संदर्भित एक्सएमएल संसाधन का एक्सएसएलटी का उपयोग करते हुए कार्यान्वयन किया जाएगा ○ प्रत्येक गैर एक्सएमएल संसाधन का माइम किस्म के ओबजेक्ट में वर्णित अभिलक्षणों का उपयोग करते हुए कार्यान्वयन किया जाएगा
एक्सएमएल नाम स्थान	आरएफसी 3986
हस्ताक्षर कूटकरण	यूटीएफ-8 आरएफसी 3629
हस्ताक्षर मूल्य कूटकरण	बेस64 आरएफसी 4648
सदंर्भ ऐलीमेंट डाइजेस्ट	एसएचए256 एफआईपीएस 180-4
हस्ताक्षर एल्गोरिदम	आरएसए पीकेसीएस-1 संस्करण 1.5 के साथ एसएचए 256
हस्ताक्षर खंड कैनोनिकलाइजेशन	○ अनन्य (बिना टिप्पणियों के), एक्सएमएल-ईएक्ससी-सी14एन, आरएफसी 3741 ○ कैनोनिकल एक्सएमएल 1. कैनोनिकल एक्सएमएल 1.0 (टिप्पणियों का लोप करता है) http://www.w3.org/TR/2001/REC-xml-c14n-20010315 2. कैनोनिकल एक्सएमएल 1.1 (टिप्पणियों का लोप करता है) http://www.w3.org/2006/12/xml-c14n11
रूपांतर एल्गोरिदम	अनन्य (बिना टिप्पणियों के), एक्सएमएल-ईएक्ससी-सी14एन, आरएफसी 3741 कैनोनिकल एक्सएमएल 1. कैनोनिकल एक्सएमएल 1.0 (टिप्पणियों का लोप करता है) http://www.w3.org/TR/2001/REC- xml -c14n-20010315 2. कैनोनिकल एक्सएमएल 1.1 (टिप्पणियों का लोप करता है)

	http://www.w3.org/2006/12/ xml-c14n11 एक्सएसएलटी-एक्सएसएल रूपांतर (एक्सएसएलटी) संस्करण 1.0. डब्ल्यू3सी http://www.w3.org/TR/1999/REC-xslt-19991116 XPath – RFC 3653
हस्ताक्षर किस्म	परावेष्टित या परावेष्टित किया जा रहा या असंलग्न
अंकीय हस्ताक्षर प्रमाणपत्र	(डीइआर) एक्स.509 वी3 अंर्तकार्यकारी मार्गदर्शक सिद्धांतों के अनुसार जारी
लोक कुंजी एल्गोरिदम	आरएसए पीकेसीएस-1 संस्करण 1.5
इसीसी कर्व	एनआईएसटी पी-256, पी-384, या पी-521
दीर्घावधि हस्ताक्षर प्रारूप	1. एक्सएमएलइआरएस आरएफसी 6283 और XAdES 2. एक्सएमएलइआरएस आरएफसी 6283 और PAdES XAdES के साथ
समय स्टॉप टोकन	जैसा कि एक्सएमएल नोटेशन में विनिर्दिष्ट आरएफसी 3161

12. एक्सएमएल अंकीय हस्ताक्षर का मूल सिन्टेक्स और नियम में इस्तेमाल किए गए पद निम्नानुसार होंगे, अर्थात् :—

```
<Signature  ID?>
<Signed Info>
<canonicalization Method/>
<Signature Method/>
(<Reference  URI?>
(<Transforms>)?
<Digest Method>
<Digest Value>
</Reference>+
</Signed Info>
<Signature Value>
(<KeyInfo>
(Key Name)
(Key Value)
(Retrieval Method)
(<X509 Data>
(X509 SKI)
```

(X509 Subject Name)

(X509 Certificate)

(X509 CRL)

(X509 Digest)

</x509 Data>)

</Keyinfo>)

(<Object ID?>)*

</Signature>

जहां "?" शून्य या एक बार उपदर्शित होने को दर्शाता है ; "+" एक या अधिक बार उपदर्शित होने को दर्शाता है ; और "*" शून्य या अधिक बार उपदर्शित होने को दर्शाता है ।

13. अंकीय हस्ताक्षर कृत्य मानक.— हस्ताक्षर प्रोफाइल और हस्ताक्षर प्ररूप की बाबत अंकीय हस्ताक्षर सृजन और सत्यापन की रीति नियंत्रक द्वारा जारी निम्नलिखित मार्गदर्शक सिद्धांतों के भी अनुरूप होगी, अर्थात् :-

(i) अंकीय हस्ताक्षर प्रमाणपत्र के लिए सूचना प्रौद्योगिकी अधिनियम के अधीन जारी अंर्तकार्यकारी मार्गदर्शक सिद्धांत ;

(ii) भारत पीकेआई के लिए एक्स.509 प्रमाणपत्र नीति ;

(iii) हस्ताक्षर प्रोफाइल ;

(iv) प्रमाणीकरण प्राधिकारियों (सीए) के लिए ऑनलाइन प्रमाणपत्र प्रास्थिति प्रोटोकाल (ओसीएसपी) सेवा मार्गदर्शक सिद्धांत ;

(v) प्रमाणपत्र प्राधिकारियों (सीए) के लिए समय स्टॉप सेवा मार्गदर्शक सिद्धांत ।

[फा. सं. 19/26/2015-सीसीए]

तपन राय, अपर सचिव

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY

(Department of Electronics and Information Technology)

NOTIFICATION

New Delhi, the 25th August, 2015

G.S.R. 660(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, namely:—

1. Short title and commencement.—

(1) These rules may be called the Digital Signature (End entity) Rules, 2015.

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

Definitions-—(1)In these rules, unless the context otherwise requires,—

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

(b) "canonicalisation", in relation to a xml digital signature, means the process of converting electronic record that has more than one possible representation into a 'standard', 'normal', or 'canonical form' in which the variations

in representation of electronic record shall be standardised by applying consistent rules, primarily as part of the xml digital signature creation and verification processes;

(c) “counter signature” means a signature on a previous signature in a series of signatures, affixed after the verification the signature on electronic record and subsequent signatures on previous signatures serially;

(d) “detached signature” means the signature that is stored independent of electronic record being signed;

(e) “digestmethod element”, in relation to a xml digital signature, means the digest algorithm to be used for the original data object or transformed, if any ‘xml transforms’ exists;

(f) “digestvalue element” means the value of the digest;

(g) "end entity**”** means the subscriber or system on behalf of the subscriber in whose name the Electronic Signature Certificate is issued;

(h) "end entity signature" means authentication of any electronic record by an end entity by means of a digital signature, electronic method or procedure in accordance with the provisions of sections 3 or 3A of the Act;

(i) “enveloped signature” means enveloping of the signature and the initial electronic record into another electronic record;

(j) “enveloping signature” means a signature over a electronic record that is referenced and contained within the signature element;

(k) “initial electronic record”, in the context of xml digital signature process, means canonicalised and transformed form of signedInfo;

(l) “keyinfo element” means an element that enables key information to be packaged along with the signature element;

(m) "long term signature" means a signature element that is made verifiable for a long term by implementing measures to enable the detection of unauthorised alterations of signature;

(n) “manifest element”, in relation to a xml digital signature, means a structure to carry a list of reference elements processing model defined by the application;

(o) “object element” means an optional element of xml digital signature, which is used for enveloping signature where the data object being signed is included in the xml;

(p) "ocsp responder" means an online service that provides revocation status of a digital signature certificate;

(q) "online certificate status protocol" means an online certificate-revocation checking protocol that enables relying-parties to determine the revocation status of an identified digital signature certificate;

(r) “parallel signatures” means one or more independent signature over the same electronic record in which the ordering of the signatures is not important;

(s) “reference element”**,** in relation to a xml digital signature, means an element that carries a references to data objects, an optional list of transforms to be applied prior to digest (xml transforms), digestmethod and digestvalue value of referenced data objects;

(t) “signedinfo”, in relation to a xml digital signature, means an element that contains a set of information to be signed for creating an xml signature, where it shall contains references to the data object that includes the canonicalisation and signature algorithms;

(u) “signature” means digital signature or xml digital signature;

(v) “signaturevalue” means an element that the actual value of the digital signature;

(w) “signaturemethod ” means an element that contains the algorithm used for signature generation and this algorithm identifies all cryptographic functions involved in the signature generation;

(x) "signatureproperties" means an element that provides a way to carry additional information about the signature, such as a time stamp or any other information which are defined by application;

(y) "time stamp" means a notation that indicates the correct date and time of an action and identity of the person or device that sent or received the time stamp and is enforced using time stamp token;

(z) "time stamp token " means a cryptographically secure confirmation generated by applying digital signature of a time stamping service provider that includes the time when the confirmation was generated;

(za) "time stamping service provider " means a trusted entity authorised to generate time stamps;

(zb) "xml" means Extensible Markup Language that provides a standard methodology with formal syntax to identify elements of information, describe the structure of data and also to store data in an independent manner, shall have the following properties,—

(i) with xml, content and presentation are separate;

(ii) the structure of xml data in a particular context is described using either xml schema or a document type definition;

(iii) xml schema or a document type definition are stored separately from the xml document itself and can be used to validate a given xml document for conformance;

(zc) "xml digital signature element" means an element that defined by standard xml schema for capturing the result of a digital signature operation applied to arbitrary data in xml format, shall satisfy the following,—

(i) xml digital signature element shall exist as a standalone document or envelop the data object that it signs;

(ii) xml digital signature element shall have signedinfo, signaturevalue, keyinfo, object and has id attribute of type child elements in order in which they appear;

(zd) "xml digital signature" means the digital signature on xml electronic record;

(ze) "xml document" means a document with xml logical and physical structure that is used to carry data elements, composed of declarations, elements, comments, character references, and processing instructions and a physical structure composed of entities, starting with the root, or document entity;

(zf) "xml schema" means a set of pre-defined or user defined keywords and their attributes arranged in a structured manner, shall satisfy the following,—

(i) should be used for a particular purpose where as a schema describes the structure of an xml document and provides specification of element names that indicates which elements are allowed in an xml document, and in what combinations; and

(ii) should provide extended functionality such as data types, inheritance, and presentation rules and default values for attributes;

(zg) "xml transform" means an element that specify an optional ordered list of processing steps applied to the data objects before it was digested where the transforms include canonicalization, encoding or decoding, extensible style sheet language transformations, xpath filtering, and xml schema validation;

(zh) "xml namespace" means a uniform resource identifier (uri) reference where the mechanisms described in the specification are used in xml documents as element types and attribute names and also to use various xml vocabularies without having name collision.

(2) Words and expressions used herein and not defined but defined in the Act shall have the meanings respectively assigned to them in the said Act.

3. **Manner of authentication of information by means of digital signature.—**A digital signature shall,—

(a) be created and verified by cryptography which concerns with transforming electronic record into seemingly unintelligible forms;

(b) use Public Key Cryptography, which employs an algorithm using two different but mathematical related keys; one key (called the private key) for creating a digital signature and another key (called the public key) for verifying a digital signature;

(c) use an hash function for creating and verifying a digital signature which required to make digital signature generation and verification efficient.

4. **Creation of digital signature.—**(1) The signatory shall, while signing an electronic record or any other item of information, first apply an hash function in the signatory's hardware or software.

(2) The hash function shall produce a hash result.

(3) The signatory's hardware or software shall then transform the hash result into a digital signature using signatory's private key and signature algorithm.

(4) The contextual information like date and time, shall be then made part of the digital signature.

(5) The counter signatures or parallel signatures or both may also be applied to electronic record.

(6) The following information may also be a part of signature,—

(a) the signatory's public key signature certificate(s);

(b) the public key certificate(s) of the licensed Certifying Authorities which used to verify the authenticity of the digital signature certificate issued to the signatory;

(c) the self signed certificate generated by the Controller used to verify the authenticity of the public key certificate of the licensed Certifying Authorities;

(d) the certificate revocation list(s) maintained by the licensed Certifying Authorities, and the controller which is used to check whether the digital signature certificate has been revoked under section 38 the Act;

(e) online certificate status protocol responder certificates and online certificate status protocol responses that may be used in lieu of certificate revocation list.

(7) To create long term valid digital signature,—

(a) a timestamp shall be applied initially to the signed data including the certificates and revocation information;

(b) ensure that initial time stamp shall cover all the data and signature(s);

(c) a nested time stamp option shall be used to ensure signature validity past the time stamping service provider's (tssp) key or algorithm expiry where the nesting of time stamps implies that a subsequent time stamp shall be applied to the prior time stamp;

(d) signature(s) and time stamps may be embedded in the data itself or stored separately as standalone.

5. Verification of digital signature.—(1)The verification of a digital signature shall be accomplished by computing a new hash result of the original electronic record by means of the hash function used to create a digital signature and by using the public key and the new hash result, the verifier shall check—

(a) if the digital signature was created using the corresponding private key and shall be applicable for parallel and counter signatures applied on the electronic record, if present;

(b) the time when the digital signature was created.

(2) To verify counter signature, the signature on electronic record and thereafter signature on previous signature serially shall be verified.

(3) To verify parallel signature, signature on electronic record shall be verified independently.

(4) To verify long term signature, the initial timestamp and all subsequent time stamp applied on the each prior timestamp shall be verified.

6. Verification of Digital Signature Certificate.—(1) 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.

(2) 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.

(3) The certificate revocation list maintained by the licensed Certifying Authorities shall be checked to confirm whether the certificate of the licensed Certifying Authorities is valid or whether it has been revoked under section 38 the Act.

(4) While verifying the validity of a digital signature the corresponding digital signature certificate shall 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 shall not be verified.

(5) The Digital Signature Certificate shall be verified with respect to time of signature created.

(6) The chain of certificates shall be verified in accordance with the standards specified in rule 7.

(7) If the certificate validity is less than one hour, the checking of revocation list shall not be required.

7. Digital signature standards.—The most important standards that shall be applicable for different activities associated with digital signature functions are as under—

Products	**Standards**
Cryptographic hash function	SHA-2 as specified in FIPS 180-4
RSA Public Key Technology	PKCS#1 RSA Encryption Standard ([2048, 4096 bit]); Version 1.5
Encryption and digital signature	PKCS#7, CMS
Validation of Digital Signature Certificate	RFC 5280
ECC curve	NIST P-256, P-384, or P-521
Long term signature formats	1. CAdES RFC 5126, 2. PAdES with CAdES
Time stamp token	As specified RFC 3161

8. **Manner of authentication of information by means of xml digital signature.—** A xml digital signature shall,—

(a) be created and verified by cryptography which concerns with transforming electronic record into seemingly unintelligible forms;

(b) use Public Key Cryptography, which employs an algorithm using two different but mathematical related keys, one key (called the private key) for creating a xml digital signature and another key (called the public key) for verifying a xml digital signature;

(c) use an cryptographic hash function for creating and verifying a xml digital signature;

(d) use canonicalization and xml transformation to create standard electronic record prior to creation and verification of xml digital signature;

(e) authenticate xml documents which contain data as references and corresponding hashes, which is affected by the use of hash algorithm, canonicalization, xml transformation and public key algorithm.

9. Creation of xml digital signature.—(1) To sign an electronic record or any other item of information, the signatory shall first constructs reference elements, xml digital signature element, signedinfo, keyinfo and signaturevalue.

(2) For the purpose of reference element generation, the signing software shall—

(a) create reference(s) element(s) with reference to the item of information, xml transform element(s) (optional), digest algorithms and digest value;

(b) optionally apply xml transform(s) to each referenced object in a sequential order;

(c) apply the hash function in the signatory's hardware or software to each reference elements, store the hash result in the reference element;

(d) ensure that if the object element is created, it shall not have a manifest element;

(e) ensure that exclusive canonicalization "without comments" has been mandatorily specified in addition to any other transforms.

(3) For the purpose xml digital signature generation, the signing software shall—

(a) create signedinfo element with signaturemethod, canonicalisation method and reference(s);

(b) apply canonicalisation to signedinfo and calculate the hash value of canonicalised signedinfo using the hashing algorithms implied by the signaturemethod;

(c) ensure that,—

(i) the signatory has seen all the contents of the document before signing;

(ii) the contents display requirements, in the case of automated signing process, is not required;

(iii) to sign multiple resources together,—

(a) each resource shall be rendered on the screen;

(b) each referenced xml resource shall be rendered using xslt and the xslt shall be the last transform done to render the resource on the screen;

(c) each non xml resource shall be rendered using mimetype attribute mentioned in the object;

(d) generate the signature using the signature algorithm and the hash, the signatory's private key, and the public key parameters (if applicable) and perform base64 encoding of the signature result and use it to form signaturevalue;

(e) construct the signature element that includes signedinfo, items of information, keyinfo with ×509 certificate element and signaturevalue and the x509 certificate element shall carry the signatory's ×509 public key certificate.

(4) The contextual information like date and time, shall be then made part of the xml digital signature.

(5) The counter signatures or parallel signatures or both may also be applied to electronic record.

(6) The following information may also be a part of signature—

(a) the public key certificate(s) of the licensed Certifying Authorities which used to verify the authenticity of the digital signature certificate issued to the signatory;

(b) the self signed certificate generated by the Controller used to verify the authenticity of the public key certificate of the licensed Certifying Authorities;

(c) the certificate revocation list(s) maintained by the licensed Certifying Authorities and controller which is used check whether the digital signature certificate has been revoked under section 38 the Act;

(d) online certificate status protocol responder certificates and online certificate status protocol responses may be used in lieu of certificate revocation list.

(7) To create long term valid xml digital signature—

(a) a timestamp shall be applied initially to the signed document, where the Initial time stamp shall cover all the electronic record and signature(s);

(b) a nested time stamp option shall be used to ensure signature validity past the time-stamping service provider (tssp)'s key or algorithm expiry where as nesting of time stamps implies that a subsequent time stamp shall be applied to the prior time stamp;

(c) signature(s) and time stamps may be embedded in the data itself or stored separately as standalone.

10. Verification of xml digital signature.—(1) The verification of the xml digital signature shall be accomplished by signature validation, reference validation and certificate validation and an xml digital signature shall be treated valid only if signature validation, reference validation and certificate validation as specified below are complied with.

(2) To accomplish signature validation—

(a) canonical form of signedinfo as produced during reference validation shall be used;

(b) canonical form of signaturemethod using the canonicalization method shall be obtained;

(c) the public key contained in the signatory's x509 certificate that is included in the xml digital signature, the canonicalisied form of signedinfo signaturevalue, and canonicalisied form of signaturemethod shall be used to verify the signature.

(3) To accomplish reference validation—

(a) canonicalise the signedinfo element based on the canonicalisation method in the signedinfo shall be used;

(b) for each reference in the signedinfo—

(i) if transformations were applied by the signatory, then the verifier software may de-reference the uniform resource identifier (uri) and execute transforms provided by the signatory in the reference element;

(ii) compute digest of referenced item using the digestmethod specified in its reference element;

(iii) compare the computed digest value against digestvalue in the signedinfo reference; if there is any mismatch or validation fails;

(4) The Digital Signature Certificate included in the xml digital signature shall be verified in accordance with the provisions specified in rule 6.

(5) To verify counter signature, the signature on electronic record first and signature on previous signature shall be verified serially.

(6) To verify parallel signature, signature on electronic record shall be verified independently.

(7) To verify long term signature, the initial timestamp and all subsequent time stamp applied on the each prior timestamp shall be verified.

11. The xml digital signature standards.—The most important standards that shall be applicable for different activities associated with xml digital signature functions are as under—

The Product	Standard
XML Digital Signature Standard	RFC 3275 with the following constraint o Manifest is not permitted inside Object, o KeyInfo containing X509Certificate element is mandatory. o The Reference Processing shall use the Exclusive Canonicalization(without comments) in addition to other transforms. o For XML resource, XSLT shall be the last transform done to enable the rendering of the document on screen. o For rendering of document on the screen o Each referenced XML resource shall be implemented using XSLT. o Each non XML resource shall be implemented using Mime Type attribute mentioned in the object.
XML Namespace	RFC 3986
Signature encoding	UTF-8 RFC 3629
Signature Value Encoding	Base64 RFC 4648
Reference element Digest	SHA256 FIPS 180-4
Signature Algorithm	SHA256withRSA PKCS-1 Version 1.5
Signature block Canonicalization	o Exclusive (without comments), XML-EXC-C14N, RFC 3741 o Canonical XML 1. Canonical XML 1.0 (omits comments) http://www.w3.org/TR/2001/REC-xml-c14n-20010315 2. Canonical XML 1.1 (omits comments) http://www.w3.org/2006/12/xml-c14n11
Transform Algorithms	Exclusive (without comments), XML-EXC-C14N, RFC 3741 Canonical XML 1. Canonical XML 1.0 (omits comments) http://www.w3.org/TR/2001/REC-xml-c14n-20010315 2. Canonical XML 1.1 (omits comments) http://www.w3.org/2006/12/xml-c14n11 XSLT-XSL Transforms (XSLT) Version 1.0. W3C http://www.w3.org/TR/1999/REC-xslt-19991116 XPath – RFC 3653
Signature Type	enveloped or enveloping or detached
Digital Signature Certificate	(DER) X.509 V3 issued as per interoperability guidelines

Public Key Algorithms	RSA PKCS-1 Version 1.5
ECC curve	NIST P-256, P-384, or P-521
Long Term Signature formats	1. XMLERS RFC 6283 and XAdES 2. XMLERS RFC 6283 and PAdES with XAdES
Time Stamp Token	As specified RFC 3161 in XML notation

12. The basic Syntax of xml digital signature and terms used in the rule shall be as follows, namely:-

```
<Signature ID?>
<SignedInfo>
<CanonicalizationMethod/>
<SignatureMethod/>
(<Reference URI?>
(<Transforms>)?
<DigestMethod>
 <DigestValue>
</Reference>+
</SignedInfo>
<SignatureValue>
(<KeyInfo>
(KeyName)
(KeyValue)
(RetrievalMethod)
(<X509Data>
(X509SKI)
(X509SubjectName)
(X509Certificate)
(X509CRL)
(X509Digest)
</x509Data>)
</Keyinfo>)
(<Object ID?>)*
</Signature>
```

Where "?" denotes zero or one occurrence; "+" denotes one or more occurrences; and "*" denotes zero or more occurrences.”

13. Digital Signature functions Standard.— The manner of digital signature creation and verification, in respect of signature profile and signature format, shall also conform to the following guidelines issued by Controller, namely:-

(i) Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act;

(ii) X.509 Certificate Policy for India PKI;

(iii) Signature profiles;

(iv) Online Certificate Status Protocol (OCSP) Service Guidelines for Certifying Authorities (CA);

(v) Time Stamping Services Guidelines for Certifying Authorities (CA).

[F. No. 19/26/2015-CCA]

TAPAN RAY, Addl. Secy.

अधिसूचना

नई दिल्ली, 25 अगस्त, 2015

सा.का.नि. 661(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 सूचना प्रौद्योगिकी (सुरक्षा प्रक्रिया) नियम, 2004 का और संशोधन करने के लिए निम्नलिखित नियम बनाती है, अर्थात् :--

1.(1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (सुरक्षा प्रक्रिया) संशोधन नियम, 2015 है ।

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

2. सूचना प्रौद्योगिकी (सुरक्षा प्रक्रिया) नियम, 2004 में,--

(क) नियम 2 में, खंड (ङ) के स्थान पर निम्नलिखित खंड रखा जाएगा, अर्थात् :--

"(ङ) इन नियमों में अनुप्रयुक्त शब्द और पद, जो परिभाषित नहीं हैं किंतु अधिनियम में और अंकीय हस्ताक्षर (अंतिम निकाय) नियम, 2015 में परिभाषित हैं, का क्रमश: वही अर्थ होगा जो उनका उक्त अधिनियम और नियमों में है ।" ;

(ख) नियम 4 में, खंड (च) के स्थान पर निम्नलिखित खंड रखा जाएगा, अर्थात् :--

"(च) अंकीय हस्ताक्षर (अंतिम निकाय) नियम, 2015 के नियम 7 या नियम 12 में निर्दिष्ट मानकों का, जहां तक उनका संबंध अंकीय हस्ताक्षर के सृजन, भंडारण और पारेषण से है, अनुपालन कर लिया गया है ; और

[फा. सं. 19/26/2015-सीसीए]

तपन राय, अपर सचिव

टिप्पण : मूल नियम भारत के राजपत्र, असाधारण, भाग II, खंड 3, उपखंड (i) में अधिसूचना सं. सा.का.नि. 735(अ), तारीख 29 अक्तूबर, 2014 द्वारा प्रकाशित किए गए थे ।

NOTIFICATION

New Delhi, the 25th August, 2015

G.S.R. 661(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 to amend the Information Technology (Security Procedure) Rules, 2004.

1. (1) These rules may be called the Information Technology (Security Procedure) Amendment Rules, 2015.
(2) They shall come into force on the date of their publication in the Official Gazette.

2. In the Information Technology (Security Procedure) Rules, 2004,—

(a) in rule 2, for clause (e), the following clause shall be substituted, namely:—

"(e) words and expressions used in these rules and not defined but defined in the Act and the Digital Signature (End entity) Rules, 2015 shall have the same meaning respectively assigned for them in the said Act and rules.";

(b) in rule 4, for clause (f), the following clause shall be substituted, namely:—

"(f) that the standards referred to in rule 7 or rule 12 of the Digital Signature (End entity) Rules, 2015 have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and".

[F. No. 19/26/2015-CCA]

TAPAN RAY, Addl. Secy.

Note : The principal rules were published in the Gazette of India, Extraordinary, Part II, and Section 3, Sub-section (i), vide notification number G.S.R. 735(E), dated the 29th October, 2004.

अधिसूचना

नई दिल्ली, 25 अगस्त, 2015

सा.का.नि. 662(अ)—केन्द्रीय सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 87 द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए सूचना प्रौद्योगिकी (प्रमाणीकरण प्राधिकारी) नियम, 2000 का और संशोधन करने के लिए निम्नलिखित नियम बनाती है, अर्थात् :--

1. (1) इन नियमों का संक्षिप्त नाम सूचना प्रौद्योगिकी (प्रमाणीकरण प्राधिकारी) संशोधन नियम, 2015 है ।

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

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

(क) नियम 6 में, सारणी में, "मानक" शीर्ष के अधीन "डीएसए और आरएसए" प्रविष्टियों के स्थान पर "डीएसए, आरएसए और कर्व एनआईएसटी पी-256, पी-384 या पी-521" प्रविष्टियां रखी जाएंगी ;

(ख) नियम 7 के स्थान पर निम्नलिखित नियम रखा जाएगा, अर्थात् :--

"**7. अंकीय हस्ताक्षर प्रमाणपत्र मानक**—प्रमाणीकरण प्राधिकारियों द्वारा जारी सभी अंकीय हस्ताक्षर प्रमाणपत्र और प्रमाणपत्र प्रतिसंहरण सूची सूचना प्रौद्योगिकी अधिनियम के अधीन नियंत्रक द्वारा अंकीय हस्ताक्षर प्रमाणपत्रों के लिए जारी अंतरकार्यकारी मार्गदर्शक सिद्धांतों के अनुरूप होगी ।" ;

(ग) नियम 23 में,--

(i) खंड (ङ) में "विवरण" शब्द के पश्चात् "नियंत्रक द्वारा जारी पहचान सत्यापन मार्गदर्शक सिद्धांतों के अनुसार" शब्द अंत:स्थापित किए जाएंगे ;

(ii) खंड (ङ) के पश्चात् निम्नलिखित खंड अंत:स्थापित किया जाएगा, अर्थात् :--

"(ङक) नियंत्रक द्वारा अनुज्ञप्ति के लिए आवेदन के दौरान प्रारंभिक प्रमाणीकरण पद्धति विवरण अनुमोदन के पश्चात् अंशदाता पहचान सत्यापन पद्धति या अंकीय हस्ताक्षर प्रमाणपत्र जारी करने के लिए अनुप्रयुक्त मार्गदर्शक सिद्धांतों में सभी परिवर्तन नियंत्रक द्वारा जारी पहचान सत्यापन मार्गदर्शक सिद्धांतों के अनुसार होंगे और परिवर्तनों को आवधिक रूप से प्रमाणीकरण पद्धति विवरण में शामिल किया जाएगा तथा उनका नियंत्रक द्वारा अनुमोदन किया जाएगा ;" ;

(घ) नियम 24 में, खंड (च) के अंत में, "नियंत्रक द्वारा भारत के लिए जारी पीकेएल (सीपी) एक्स.509 प्रमाणीकरण नीति के अनुसार" शब्द अंत:स्थापित किए जाएंगे ;

(ङ) नियम 25 में, खंड (ii) में, "भी है, कि" शब्दों के पश्चात् "नियंत्रक द्वारा जारी पहचान मार्गदर्शक सिद्धांतों के अनुसार" शब्द अंत:स्थापित किए जाएंगे ;

(च) नियम 31 में, उपनियम (1) में खंड (ix) के पश्चात् निम्नलिखित खंड अंत:स्थापित किया जाएगा ;

"(x) नियंत्रक द्वारा भारत के लिए जारी पीके1 सुसंगत एक्स.509 प्रमाणपत्र नीति का अनुपालन

(xi) नियंत्रक द्वारा अन्य सेवाओं जैसे समय स्टॉपिंग और ओसीएसपी सेवा मार्गदर्शक सिद्धांतों का अनुपालन ;

(xii) नियंत्रक द्वारा जारी पहचान सत्यापन मार्गदर्शक सिद्धांतों का अनुपालन ;

(xiii) नियंत्रक द्वारा जारी "अंकीय हस्ताक्षर प्रमाणपत्र अंतरकार्यकारी मार्गदर्शक सिद्धांतों" का अनुपालन ;

(छ) अनुसूची 4 में,

(क) प्ररूप क में उपशीर्ष "महत्वपूर्ण सूचना के अधीन :",--

(i) "भरा हुआ" शब्दों के स्थान पर "हस्ताक्षरित" शब्द रखे जाएंगे ;

(ii) "आवेदन अनिवार्यता स्वयं व्यक्ति द्वारा प्रस्तुत किया जाए" शब्दों का लोप किया जाएगा ;

(ख) प्ररूप ख में उपशीर्ष "पहचान और निवास के सबूत का अधिप्रमाणन" प्रविष्टियों के स्थान पर निम्नलिखित रखा जाएगा, अर्थात् :--

(i) "पहचान सत्यापन पद्धति और निवास के सबूत की अपेक्षाएं सीए की प्रमाणन पद्धति विवरण (सीपीएस) और नियंत्रक द्वारा जारी पहचान सत्यापन मार्गदर्शक सिद्धांतों के अनुसार होंगी ।" ;

(ii) "महत्वपूर्ण सूचना" उपशीर्ष के अधीन :",--

(1) "भरा हुआ" शब्दों के स्थान पर "हस्ताक्षरित" शब्द रखे जाएंगे ;

(2) "आवेदन अनिवार्यता स्वयं व्यक्ति द्वारा प्रस्तुत किया जाए" शब्दों का लोप किया जाएगा ।

[फा. सं. 19/26/2015-सीसीए]

तपन राय, अपर सचिव

टिप्पणी : मूल नियम भारत के राजपत्र, असाधारण, भाग II, खंड 3, उपखंड (i) में अधिसूचना सं. सा.का.नि. 789(अ), तारीख 17 अक्तूबर, 2000 द्वारा प्रकाशित किए गए थे और उनका अंतिम संशोधन सं. सा.का.नि. 783(अ), तारीख 25 अक्तूबर, 2011 द्वारा किया गया था ।

NOTIFICATION

New Delhi, the 25th August, 2015

G.S.R. 662(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.

1. (1) These rules may be called the Information Technology (Certifying Authorities) Amendment Rules, 2015.

(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 6, in the table , under the heading "The Standard", for the entries "DSA and RSA", the entries " DSA , RSA and Curves NIST P-256, P-384, or P-521" shall be substituted;

(b) for rule 7, the following rule shall be substituted, namely:—

"7.**Digital Signature Certificate Standard**.—All Digital Signature Certificates and Certificate Revocation List issued by the Certifying Authorities shall conform to Interoperability Guidelines for Digital Signature Certificates issued by Controller under the Information Technology Act.";

(c) in rule 23,—

(i) in clause (e), after the word " Statement", the words "in accordance with the Identity Verification Guidelines issued by the Controller" shall be inserted;

(ii) after clause(e), the following clause shall be inserted, namely:-

"(ea) subsequent to initial approval of Certification Practice Statement by the Controller during the application for a licence, all the changes in the subscriber identity verification method or guidelines employed for issuance of Digital Signature Certificate shall be in accordance with the Identity Verification Guidelines issued by the Controller and the changes shall be incorporated in the Certification Practice Statement periodically and shall be approved by the Controller;";

(d) in rule 24, in clause (f) , the words, brackets and letters "in accordance with the X.509 Certificate Policy for India PKI(CP) issued by the Controller" shall be inserted at the end ;

(e) in rule 25, in clause (ii) , the words "in accordance with the Identity Verification Guidelines issued by the Controller" shall be inserted at the end;

(f) in rule 31, in sub-rule (1) **,** after clause (ix), the following clauses shall be inserted namely:-

"(x) compliance to relevant X.509 Certificate Policy for India PKI issued by the Controller;

(xi) compliance to guidelines issued by the Controller for other services like Time Stamping and OCSP service;

(xii) compliance to Identity Verification Guidelines issued by the Controller;

(xiii) compliance to "Digital Signature Certificates Interoperability Guidelines" issued by the Controller.";

(g) in SCHEDULE IV,**—**

(a) in Form A, under the sub-heading "Important Notice:",—

(i) for the word "filled " the word "signed" shall be substituted;

(ii) the words "Application form must be submitted in person." shall be omitted;

(b) in Form B,

(i) for the entries under the sub-heading "Authentication of Identity and Proof of Residence", the following shall be substituted, namely:—

"The identity verification methods and proof of residence requirements shall be as per Certification Practice Statement (CPS) of the CA and Identity Verification Guidelines issued by the Controller.";

(ii) under the sub-heading "Important Notice:",—

(1) for the word "filled " the word "signed" shall be substituted;

(2) the words "Application form must be submitted in person." shall be omitted.

[F. No. 19/26/2015-CCA]

TAPAN RAY, Addl. Secy.

Note. : The principal rules were published in the Gazette of India, Extraordinary, Part II, and Section 3, Sub-section (i), vide notification number G.S.R. 789(E), dated the 17th October, 2000 and last amended by notification No. G.S.R. 783(E), dated the 25th October 2011.

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