

अधिसूचना

नई दिल्ली, 12 सितम्बर, 2016

आधार (अधिप्रमाणन) विनियम, 2016

(2016 का सं. 3)

सं. 13012/64/2016/विधि/यूआईडीएआई (2016 का सं.3).—आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 की धारा 54 की उप-धारा (2) के उप-खंड (एफ) एवं (डब्ल्यू) तथा उप-धारा (1) के अंतर्गत प्राप्त शक्तियों का प्रयोग करते हुए, भारतीय विशिष्ट पहचान प्राधिकरण एतद्वारा निम्नलिखित विनियम बनाता है, नामतः—

अध्याय — 1

प्रारंभिक

1. **संक्षिप्त नाम और प्रारंभ :-**
 - (1) इन विनियमों को आधार (अधिप्रमाणन) विनियम, 2016 कहा जाएगा।
 - (2) ये प्राधिकरण द्वारा सरकारी राजपत्र में जारी की गई अधिसूचना में नियुक्त तिथि को लागू होंगे।
2. **परिभाषाएं :-**
 - (1) जब तक कि संदर्भ में अन्यथा अपेक्षित न हो, इन विनियमों में,—
 - (क) **“अधिनियम”** से अभिप्राय आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 से है;
 - (ख) **“आधार नंबर धारक”** का अभिप्राय कोई व्यक्ति, जिसे अधिनियम के अंतर्गत आधार नंबर जारी किया गया है, से है;
 - (ग) **“अधिप्रमाणन”** का अभिप्राय, वह प्रक्रिया, जिसके द्वारा किसी व्यक्ति की जनसांख्यिकीय सूचना अथवा बायोमैट्रिक सूचना सहित आधार संख्या उसके सत्यापन के लिए ‘केन्द्रीय पहचान आंकड़े निक्षेपागार (सेंट्रल आइडेंटिटीज डाटा रिपोजिटरी)’ के पास जमा की जाती है और ऐसा निक्षेपागार उसकी शुद्धता अथवा कमी को उपलब्ध सूचनाओं के आधार पर सत्यापित करता है, से है;
 - (घ) **“अधिप्रमाणन सुविधा”** का अभिप्राय, वह सुविधा है, जो हां/ना प्रत्युत्तर अथवा ई-केवाईसी डाटा, जो भी प्रयोज्य हो, को उपलब्ध कराते हुए अधिप्रमाणन प्रक्रिया द्वारा आधार नंबर धारक की पहचान सूचना के सत्यापन के लिए उपलब्ध कराई जाती है;
 - (च) **“अधिप्रमाणन अभिलेख”** का अभिप्राय अधिप्रमाणन के समय तथा अनुरोधकर्ता संस्था की पहचान एवं उससे अनुलग्न प्राधिकरण द्वारा उपलब्ध कराये गए प्रत्युत्तर के अभिलेख से है;
 - (छ) **“अधिप्रमाणन सेवा एजेसी”** अथवा **“एएसए”** का अभिप्राय, वह संस्था होगी, जो प्राधिकरण द्वारा उपलब्ध कराई गयी अधिप्रमाणन सुविधा का उपयोग करते हुए अधिप्रमाणन के निष्पादन के लिए अनुरोधकर्ता संस्था को सक्षम बनाने के लिए सुरक्षित नेटवर्क संयोजन एवं सम्बद्ध सेवाएं सुनिश्चित करने के लिए आवश्यक अवसंरचना उपलब्ध करा रही है;
 - (ज) **“अधिप्रमाणन उपयोक्ता एजेसी”** अथवा **“एयूए”** का अभिप्राय वह अनुरोधकर्ता संस्था से है, जो प्राधिकरण द्वारा उपलब्ध कराई गयी हां/ना अधिप्रमाणन सुविधा का उपयोग करती है;
 - (झ) **“प्राधिकरण”** का अभिप्राय अधिनियम की धारा 11 की उप-धारा (1) के तहत स्थापित भारतीय विशिष्ट पहचान प्राधिकरण से है;
 - (ट) **“केन्द्रीय पहचान आंकड़े निक्षेपागार”** अथवा **“सीआईडीआर”** का अभिप्राय एक या एक से अधिक स्थानों पर केन्द्रीकृत डाटा बेस है, जिसमें आधार नंबर धारक को जारी आधार नंबर सहित ऐसे व्यक्तियों की जनसांख्यिकीय तथा बायोमैट्रिक सूचना तथा तत्संबंधी अन्य संबद्ध सूचना शामिल हैं, से है;

- (ठ) "ई-केवाईसी अधिप्रमाणन सुविधा" का अभिप्राय उस अधिप्रमाणन सुविधा से है, जिसमें अनुरोधकर्ता संस्था के माध्यम से आधार नंबर धारक की सहमति द्वारा बायोमैट्रिक सूचना तथा/अथवा ओटीपी एवं आधार नंबर सुरक्षित रूप से जमा की जाती है, जिसका मिलान सीआईडीआर में उपलब्ध डाटा से किया जाता है जिस पर प्राधिकरण अधिप्रमाणन लेन-देन से सम्बद्ध अन्य तकनीकी विवरणों सहित ई-केवाईसी डाटा वाला एक डिजिटल रूप से हस्ताक्षरित प्रत्युत्तर प्रदान करता है;
- (ड) "ई-केवाईसी डाटा" का अभिप्राय किसी आधार नंबर धारक की जनसांख्यिकीय सूचना एवं फोटोग्राफ से है;
- (ढ) "ई-केवाईसी उपयोक्ता एजेंसी" अथवा "केयूए" का अभिप्राय उस अनुरोधकर्ता संस्था से है, जो एयूए होने के अतिरिक्त प्राधिकरण द्वारा प्रावधानित ई-केवाईसी अधिप्रमाणन सुविधा का उपयोग करती है;
- (ण) "लाइसेंस कुंजी" से अभिप्राय, प्राधिकरण द्वारा निर्धारित प्रक्रिया के अनुसार अनुरोधकर्ता संस्था द्वारा जनित कुंजी से है;
- (त) "पीआईडी ब्लॉक" का अभिप्राय है, व्यक्तिगत पहचान डाटा (पर्सनल आईडेंटिटी डाटा) घटक, जिसके अन्तर्गत अधिप्रमाणन के दौरान आधार नंबर धारक से संग्रहीत आवश्यक जनसांख्यिकीय तथा/अथवा बायोमैट्रिक तथा/अथवा ओटीपी सम्मिलित हैं;
- (थ) "अनुरोध करने वाली संस्था" से अभिप्राय किसी एजेंसी या व्यक्ति से जो कि अधिप्रमाणन के लिए केन्द्रीय पहचान आंकड़े निक्षेपागार को किसी व्यक्ति विशेष के आधार नंबर तथा जनसांख्यिकीय सूचना अथवा बायोमैट्रिक सूचना प्रस्तुत करता है, से है;
- (द) "हां/ना अधिप्रमाणन सुविधा" का अभिप्राय एक प्रकार की अधिप्रमाणन सुविधा से है, जिसमें किसी अनुरोधकर्ता संस्था के माध्यम से आधार नंबर धारक की सहमति द्वारा पहचान संबंधी सूचना एवं आधार नंबर को सुरक्षित रूप से जमा किया जाता है और तत्पश्चात सीआईडीआर में उपलब्ध डाटा से उसका मिलान किया जाता है, तथा प्राधिकरण अधिप्रमाणन संव्यवहार से सम्बद्ध अन्य तकनीकी विवरण सहित "हां" या "ना" वाले प्रत्युत्तर पहचान संबंधी सूचना के बिना डिजिटल रूप से हस्ताक्षरित करके देता है।
- (2) इन विनियमों में उपयोग किए गए शब्द एवं अभिव्यक्तियां, जिन्हें इन विनियमों में परिभाषित नहीं किया गया है, का वही अर्थ होगा जो कि अधिनियम अथवा उसके तहत बनाए गए नियमों तथा अन्य विनियमों अथवा सूचना प्रौद्योगिकी अधिनियम, 2000 में परिभाषित किया गया है।

अध्याय - 2

आधार अधिप्रमाणन तंत्र

3. अधिप्रमाणन के प्रकार : -

प्राधिकरण द्वारा दो प्रकार की अधिप्रमाणन सुविधाएं उपलब्ध करायी जाएगी, नामतः :-

- (i) **हां/ना अधिप्रमाणन सुविधा**, जिसका निष्पादन विनियम 4(2) में निर्दिष्ट किसी भी माध्यम से किया जा सकता है; तथा
- (ii) **ई-केवाईसी सुविधा**, जिसका निष्पादन विनियम 4(2) में निर्दिष्ट केवल ओटीपी तथा/अथवा बायोमैट्रिक अधिप्रमाणन माध्यम द्वारा ही किया जा सकता है।

4. अधिप्रमाणन के माध्यम :-

- (1) प्राधिकरण के इन विनियमों के अनुसार तथा निर्दिष्टियों के अनुरूप इलेक्ट्रॉनिक रूप में किसी निवेदक संस्था द्वारा प्रेषित किसी अनुरोध को ही अधिप्रमाणन अनुरोध, के रूप में प्राधिकरण द्वारा स्वीकार किया जाएगा।
- (2) अधिप्रमाणन को निम्नलिखित माध्यमों द्वारा सम्पन्न किया जा सकता है :
- (क) **जनसांख्यिकीय अधिप्रमाणन** : आधार नंबर धारक द्वारा प्राप्त आधार नंबर धारक के आधार नंबर एवं जनसांख्यिकीय सूचना का मिलान, सीआईडीआर में आधार नंबर धारक की जनसांख्यिकीय सूचना के साथ किया जाता है।
- (ख) **वन-टाइम पिन आधारित अधिप्रमाणन** : सीमित समय की वैधता वाला एक वन टाइम पिन (ओटीपी) प्राधिकरण में पंजीकृत आधार नंबर धारक के मोबाइल नंबर तथा/अथवा ई-मेल पते पर भेजा जाता है, अथवा अन्य उचित साधनों द्वारा सृजित किया जाता है। आधार नंबर धारक अधिप्रमाणन के दौरान अपने आधार नंबर सहित इस ओटीपी को उपलब्ध करायेगा और इसका मिलान प्राधिकरण द्वारा सृजित ओटीपी से किया जाएगा।
- (ग) **बायोमैट्रिक आधारित अधिप्रमाणन** : आधार नंबर धारक द्वारा जमा किया गया आधार नंबर तथा बायोमैट्रिक सूचना का मिलान, सीआईडीआर में भंडारित कथित आधार नंबर की बायोमैट्रिक सूचना से किया जाता है। यह या तो फिंगरप्रिंट आधारित अथवा पुतली आधारित अधिप्रमाणन अथवा सीआईडीआर में भंडारित बायोमैट्रिक सूचना पर आधारित अन्य बायोमैट्रिक रूपात्मकता हो सकती है।
- (घ) **बहुकारकीय अधिप्रमाणन** : उपर्युक्त दो अथवा दो से अधिक माध्यमों के संयोजन का उपयोग अधिप्रमाणन के लिए किया जा सकता है।
- (3) कोई अनुरोधकर्ता संस्था अपनी वांछनीयताओं के अनुसार किसी विशेष सेवा कार्य व्यापार के लिए उप-विनियम (2) में निर्दिष्ट माध्यमों से वृहत्तर सुरक्षा के लिए बहुकारकीय अधिप्रमाणन सहित अधिप्रमाणन का उपयुक्त माध्यम चुन सकती है। किसी सन्देह के निराकरण के लिए यह स्पष्ट किया जाता है कि ई-केवाईसी अधिप्रमाणन केवल ओटीपी तथा/अथवा बायोमैट्रिक अधिप्रमाणन के उपयोग द्वारा ही सम्पन्न किया जाएगा।

5. आधार नंबर धारक के लिए सूचना :-

- (1) अधिप्रमाणन के समय अनुरोधकर्ता संस्था आधार नंबर धारक को निम्नलिखित विवरणों की सूचना देगी :
- (क) सूचना की प्रकृति, जिसे अधिप्रमाणन पर प्राधिकरण द्वारा सहभाजित किया जाएगा;

- (ख) उपयोग, जिसके लिए अधिप्रमाणन के दौरान प्राप्त सूचना रखी जा सकती है; और;
 (ग) पहचानसंबंधी जानकारी प्रस्तुत करने के विकल्प।

(2) अनुरोधकर्ता संस्था सुनिश्चित करेगी कि ऊपर उप-विनियम (1) में संदर्भित सूचना स्थानीय भाषा में भी आधार नंबर धारक को उपलब्ध करायी जायेगी।

6. आधार नंबर धारक की सहमति:-

- (1) विनियम 5 के अनुरूप सूचना के संचारण के पश्चात अनुरोधकर्ता संस्था अधिप्रमाणन हेतु आधार नंबर धारक की सहमति प्राप्त करेगी।
 (2) अनुरोधकर्ता संस्था ऊपर उप-विनियम (1) में सन्दर्भित सहमति भौतिक रूप में अथवा विषेशतः इलेक्ट्रॉनिक प्रारूप में प्राप्त करेगी और इस उद्देश्य के लिए प्राधिकरण द्वारा निर्दिष्ट तरीके अथवा प्रारूप में प्राप्त सहमति के लॉग अथवा अभिलेख रखेगी।

7. अनुरोधकर्ता संस्था द्वारा बायोमैट्रिक सूचना ग्रहण करना :-

- (1) अनुरोधकर्ता संस्था, प्राधिकरण द्वारा निर्धारित प्रक्रियाओं तथा विशिष्टियों के अनुसार प्रमाणित बायोमैट्रिक उपकरणों के प्रयोग द्वारा आधार नंबर धारक की बायोमैट्रिक सूचना को ग्रहण करेगी।
 (2) अनुरोधकर्ता संस्था, आवश्यक रूप से प्राधिकरण द्वारा निर्धारित विशिष्टियों के अनुरूप ग्रहण करते समय बायोमैट्रिक डाटा कूटबद्ध एवं सुरक्षित करेगी।
 (3) बायोमैट्रिक सूचना ग्रहण करने में अनुकूलतम परिणाम हेतु अनुरोधकर्ता संस्था इस उद्देश्य के लिए प्राधिकरण द्वारा समय-समय पर निर्दिष्ट प्रक्रियाओं को स्वीकार करेगी।

8. अधिप्रमाणन में प्रयुक्त उपकरण, क्लाइंट एप्लीकेशन्स आदि :-

- (1) अधिप्रमाणन के लिए प्रयुक्त समस्त यन्त्र एवं उपकरण इस उद्देश्य हेतु प्राधिकरण द्वारा समय-समय पर वांछनीयता एवं निर्गत विशिष्टियों के अनुसार प्रमाणित किये जाएंगे।
 (2) अधिप्रमाणन के उद्देश्य हेतु अनुरोधकर्ता संस्था द्वारा प्रयोग में लाये जाने वाले क्लाइंट एप्लीकेशन्स अर्थात् सॉफ्टवेयर इस उद्देश्य हेतु समय-समय पर प्राधिकरण द्वारा निर्दिष्ट मानक एपीआई तथा विशिष्टियों के अनुरूप होंगे।

9. अधिप्रमाणन अनुरोध भेजने की प्रक्रिया :-

- (1) अनुरोधकर्ता संस्था द्वारा प्रावधानित आधार नम्बर अथवा कोई अन्य अभिज्ञापक (आइडेंटिफायर) जो आधार नंबर के साथ संयोजित की गयी है तथा आधार नंबर धारक से आवश्यक जनसांख्यिकीय तथा/अथवा बायोमैट्रिक सूचना तथा/अथवा ओटीपी संग्रहीत करने के पश्चात प्राधिकरण द्वारा निर्दिष्ट विशिष्टियों के अनुसार क्लाइंट एप्लीकेशन तुरन्त किसी पारेषण से पूर्व इन इनपुट पैरामीटरों को पीआईडी ब्लॉक में पैकेज और कूटबद्ध करेगा, और सुरक्षित प्रोटोकॉल, जो इस उद्देश्य के लिए प्राधिकरण द्वारा निर्दिष्ट किया गया है, के प्रयोग द्वारा अनुरोधकर्ता संस्था के सर्वर के पास भेज देगा।
 (2) विधिमान्यकरण के उपरान्त अनुरोधकर्ता संस्था का सर्वर प्राधिकरण द्वारा निर्दिष्ट विशिष्टियों के अनुसार अधिप्रमाणन सेवा एजेंसी के सर्वर के माध्यम से अधिप्रमाणन अनुरोध को सीआईडीआर के पास भेज देगा। अधिप्रमाणन अनुरोधकर्ता संस्था तथा/अथवा अधिप्रमाणन सेवा एजेंसी द्वारा उनके पारस्परिक समझौते के अनुसार डिजिटल रूप से हस्ताक्षरित करेगा।
 (3) अधिप्रमाणन अनुरोध के माध्यम के आधार पर सीआईडीआर स्वयं भंडारित डाटा के विरुद्ध इनपुट पैरामीटरों का विधिमान्यकरण करेगा और डिजिटल रूप से हस्ताक्षरित 'हां' या 'ना' अधिप्रमाणन प्रत्युत्तर, अथवा कूटबद्ध ई-केवाईसी डाटा सहित डिजिटल रूप से हस्ताक्षरित ई-केवाईसी, जैसी स्थिति हो, को अधिप्रमाणन संव्यवहार से सम्बद्ध अन्य तकनीकी विवरणों के साथ वापस करेगा।
 (4) अधिप्रमाणन के सभी माध्यमों में, आधार नंबर अनिवार्य है और इसे उपर्युक्त उप-विनियम (1) में निर्दिष्ट इनपुट पैरामीटरों के साथ इस प्रकार जमा किया जाता है कि अधिप्रमाणन सदैव 1 : 1 के मिलान के साथ शेष रहे।
 (5) अनुरोधकर्ता संस्था सुनिश्चित करेगी कि प्राधिकरण द्वारा निर्दिष्ट विशिष्टियों एवं प्रक्रियाओं के अनुसार अधिप्रमाणन उपकरण द्वारा ग्रहण (कैचर) करते समय पीआईडी ब्लॉक का एन्क्रिप्शन होता रहे।

10. आधार नंबर धारक को अधिप्रमाणन की अधिसूचना :-

आधार नंबर धारक को किसी बायोमैट्रिक तथा/अथवा ओटीपी आधारित अधिप्रमाणन से अधिप्रमाणन के समय, प्राधिकरण द्वारा निर्धारित पंजीकृत ई-मेल तथा/अथवा आधार नंबर धारक के मोबाइल नंबर के माध्यम से अधिसूचित किया जा सकता है।

11. बायोमैट्रिक लॉकिंग:-

- (1) प्राधिकरण बायोमैट्रिक अधिप्रमाणन हेतु आवश्यकतानुसार आधार नंबर धारक को उसके बायोमैट्रिकस को स्थायी तौर पर लॉक करने तथा अस्थायी तौर पर अनलॉक करने की स्वतन्त्रता देगा।

- (2) ऐसे लॉक किए गए किसी बायोमैट्रिक अभिलेख के विरुद्ध समस्त बायोमैट्रिक अधिप्रमाणन एक उचित प्रत्युत्तर कोड सहित "नहीं" विकल्प के साथ असफल होंगे।
- (3) आधार नंबर धारक को अधिप्रमाणन हेतु अपने बायोमैट्रिक को अस्थायी तौर पर अनलॉक करने की अनुमति दी जाएगी और ऐसा अस्थायी अनलॉकिंग प्राधिकरण द्वारा निर्दिष्ट समयावधि के पश्चात अथवा अधिप्रमाणन संव्यवहार की पूर्णता तक, जो भी पहले हो, जारी नहीं रहेगा।
- (4) प्राधिकरण आधार नंबर धारक के लिए सुरक्षित तरीके से किसी भी समय ऐसे स्थायी लॉकिंग को समाप्त करने का प्रावधान करेगा।

अध्याय - 3

अनुरोधकर्ता संस्थाओं तथा अधिप्रमाणन सेवा एजेंसियों की नियुक्ति

12. अनुरोधकर्ता संस्थाओं तथा अधिप्रमाणन सेवा एजेंसियों की नियुक्ति :-

- (1) प्राधिकरण द्वारा प्रावधानित अधिप्रमाणन सुविधा के उपयोग के लिए अनुरोधकर्ता संस्था बनने वाली एजेंसियां इस उद्देश्य के लिए प्राधिकरण द्वारा निर्दिष्ट विधानों के अनुसार अनुरोधकर्ता संस्था के रूप में नियुक्ति के लिए आवेदन करेंगी। केवल अनुसूची 'क' के मानदंडों को पूरा करने वाली अनुरोधकर्ता संस्थाएं ही आवेदन करने की पात्र होंगी। प्राधिकरण आदेश द्वारा समय-समय पर अनुसूची 'क' में संशोधन कर कर सकता है ताकि पात्रता मानदंड को संशोधित किया जा सके।
- (2) अधिप्रमाणन सेवा एजेंसियों के रूप में नियुक्ति चाहने वाली संस्थाएं इस उद्देश्य के लिए प्राधिकरण द्वारा निर्दिष्ट विधानों के अनुरूप नियुक्ति के लिए आवेदन करेंगी। केवल अनुसूची 'ख' के मानदंडों को पूरा करने वाली संस्थाएं ही आवेदन करने की पात्र होंगी। प्राधिकरण आदेश द्वारा समय-समय पर अनुसूची 'ख' में संशोधन कर सकता है ताकि पात्रता मानदंड को संशोधित किया जा सके।
- (3) प्राधिकरण ऐसी आवेदक संस्था अथवा अधिप्रमाणन सेवा एजेंसियों, जैसी भी स्थिति हो, की गतिविधियों से सम्बद्ध मामलों के संबंध में आवेदक से अन्य सूचना अथवा स्पष्टीकरण का उल्लेख करने के लिए कह सकता है, जिसे आवेदन पर विचार करने और निपटान करने के लिए प्राधिकरण द्वारा विचारार्थ लिया जा सकता है।
- (4) आवेदक, प्राधिकरण द्वारा इस संबंध में निर्धारित समय के अन्दर निर्दिष्ट प्राधिकरण की सन्तुष्टि के अनुरूप ऐसी सूचना तथा स्पष्टीकरण का उल्लेख करेगा।
- (5) आवेदन पर विचार करते समय, आवेदक द्वारा प्रस्तुत की गयी सूचना और उसकी पात्रता को प्राधिकरण दस्तावेजों के प्रत्यक्ष सत्यापन, अवसंरचना एवं तकनीकी संबलका सत्यापन कर सकता है, जिन्हें आवेदक के पास होना आवश्यक है।
- (6) आवेदक द्वारा प्रस्तुत किये गए आवेदन, दस्तावेजों तथा उसकी पात्रता के सत्यापन के पश्चात प्राधिकरण :
 - (क) अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी के आवेदन, जो भी स्थिति हो, को अनुमोदित कर सकता है; तथा
 - (ख) संस्था अथवा एजेंसी के साथ प्राधिकरण की अधिप्रमाणन सुविधा के अनुरोधकर्ता संस्था द्वारा उपयोग के लिए नियमों एवं शर्तों अथवा एएसए द्वारा सेवाओं के प्रावधान में दायित्वों के गैर-निष्पादन की स्थिति में क्षतियों तथा हतोत्साहन के शर्तोंसमेत करते हुए उचित करार कर सकती है।
- (7) प्राधिकरण, समय-समय पर आवेदन शुल्क, वार्षिक सदस्यता शुल्क तथा वैयक्तिक अधिप्रमाणन संव्यवहार के लिए शुल्क सहित संस्थाओं द्वारा उनकी नियुक्ति के दौरान उनके द्वारा देय शुल्क एवं प्रभार निर्धारित कर सकती है।

13. प्रक्रिया, जहां नियुक्ति के लिए आवेदन अनुमोदित नहीं हुआ है :-

- (1) यदि, अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी, जैसी स्थिति हो, की नियुक्ति के लिए आवेदन प्राधिकरण द्वारा निर्दिष्ट वांछनीयताओं को सन्तुष्ट नहीं करती है तो प्राधिकरण आवेदन निरस्त कर सकता है।
- (2) आवेदन निरस्त के प्राधिकरण के निर्णय की सूचना आवेदक को इस निर्णय के तीस दिनों के अंदर लिखित रूप में दे दी जाएगी, जिसमें उसके आवेदन को निरस्त करने के कारणों का उल्लेख किया जाएगा।
- (3) कोई भी आवेदक जो प्राधिकरण के निर्णय से असन्तुष्ट है, तो वह इस निर्णय पर पुनर्विचार करने के लिए इस सूचना की प्राप्ति की तिथि के तीस दिनों के अंदर प्राधिकरण के पास आवेदन कर सकता है।
- (4) प्राधिकरण, आवेदक द्वारा भेजे गये आवेदन पर पुनर्विचार करेगा और इससे संबंधित निर्णय को यथाशीघ्र आवेदक को लिखित रूप में सूचित करेगा।

14. अनुरोधकर्ता संस्था की भूमिका तथा उत्तरदायित्व :-

- (1) अनुरोधकर्ता संस्था को निम्नलिखित कार्य एवं उत्तरदायित्वों का निर्वहन करना होगा :
 - (क) स्वयं के तंत्र, प्रक्रियाओं, अवसंरचना, तकनीक, सुरक्षा आदि सहित अधिप्रमाणन से संबंधित आवश्यक प्रचालनों का संस्थापन एवं अनुरक्षण करना;
 - (ख) अधिप्रमाणन अनुरोधों को भेजने के लिए प्राधिकरण द्वारा अनुमोदित एएसए के माध्यम से सीआईडीआर के साथ नेटवर्क कनेक्टिविटी सुनिश्चित करना;
 - (ग) सुनिश्चित करना कि अधिप्रमाणन अनुरोधों को भेजने के लिए प्रयुक्त अधिप्रमाणन उपकरणों तथा सीआईडीआर के मध्य नेटवर्क कनेक्टिविटी इस उद्देश्य के लिए प्राधिकरण द्वारा निर्धारित मानकों एवं विशिष्टियों के अनुरूप है;

- (घ) केवल उन्हीं यन्त्रों, उपकरण, अथवा सॉफ्टवेयर का उपयोग करना जो आवश्यक रूप से प्राधिकरण द्वारा पंजीकृत अथवा अनुमोदित अथवा प्रमाणित या प्राधिकरण द्वारा निर्दिष्ट हैं और इस उद्देश्य हेतु प्राधिकरण द्वारा निर्धारित मानकों और विशिष्टियों के अनुरूप हैं;
- (च) इस संबंध में प्राधिकरण द्वारा समय-समय पर निर्गत एवं सूचित नियमों एवं शर्तों, मानकों, निर्देशों तथा विशिष्टियों के लिए अपने यंत्रों तथा उपकरणों के प्रचालन की आवर्ती आधार पर निगरानी करना;
- (छ) सुनिश्चित करना कि अधिप्रमाणन कार्यों के निष्पादन, तथा आवश्यक तंत्रों, अवसंरचना एवं प्रक्रियाओं के अनुरक्षण के लिए उसके द्वारा नियुक्त कर्मचारियों के पास ऐसे कार्यों के निष्पादन की अपेक्षित योग्यता है;
- (ज) एएसए के विषय में प्राधिकरण को निरन्तर सूचित करना, जिसके साथ उसका समझौता हुआ है;
- (झ) सुनिश्चित करना कि उसके प्रचालन तथा तंत्र प्राधिकरण के मानकों तथा विशिष्टियों के अनुरूप हैं, जिसे सुनिश्चित करने के लिए किसी प्रतिष्ठित निकाय द्वारा प्रमाणित सूचना पद्धति लेखापरीक्षक द्वारा वार्षिक आधार पर लेखापरीक्षा करवाई गयी है और लेखापरीक्षा रिपोर्ट अनुरोध किए जाने पर प्राधिकरण के साथ सहभाजित करनी होगी;
- (ट) आधार नंबर धारकों को अधिप्रमाणन सेवाओं के सुचारु प्रावधान सुनिश्चित करने हेतु अपवाद संचलन क्रियाविधि तथा बैंक-अप पहचान अधिप्रमाणन क्रियाविधि क्रियान्वित करना;
- (ठ) अधिप्रमाणन से सम्बद्ध धोखाधड़ी अथवा विवाद सम्बन्धी किसी जांच की स्थिति में वह प्राधिकरण, अथवा इसके द्वारा नियुक्त या प्राधिकृत किसी एजेंसी अथवा किसी अन्य प्राधिकृत जांच एजेंसी का पूर्ण सहयोग करेगी और अपने परिसर, अभिलेख, कार्मिक तथा किसी अन्य संसाधन या सूचना तक उनकी पहुंच बनाने का प्रावधान करेगी;
- (ड) अनुरोधकर्ता संस्था द्वारा अपने आधार अधिप्रमाणन तंत्र को अपने स्थानीय अधिप्रमाणन तंत्र से समेकन की इच्छा करने की स्थिति में, ऐसे समेकन समय-समय पर प्राधिकरण द्वारा निर्गत मानकों तथा विशिष्टियों के अनुरूप सम्पादित करने होंगे;
- (ढ) वह प्राधिकरण को अपने नेटवर्क के भीतर आधार संबंधी सूचना अथवा तंत्र के आधार फ्रेमवर्क अथवा किसी अन्य समझौते से सम्बद्ध किसी सूचना अथवा तंत्र के किसी दुरुपयोग के विषय में सूचित करेगी; यदि अनुरोधकर्ता धोखाधड़ी संस्था धोखाधड़ी की शिकार है अथवा उसे आधार प्रमाणीकरण से संबंधित धोखाधड़ी जांच प्रणाली के माध्यम से किसी धोखाधड़ी की जानकारी प्राप्त होती है, वह उस धोखाधड़ी से संबंधित समस्त समस्त जानकारी प्राधिकरण को सहभाजित करेगी।
- (ण) वह अधिप्रमाणन प्रचालनों तथा परिणामों के लिए उत्तरदायी होगी, भले ही उसने अपने प्रचालनों को तीसरे पक्षों के साथ उप-अनुबन्धित किया हो। अनुरोधकर्ता संस्था यह सुनिश्चित करने के लिए भी उत्तरदायी होगी कि ऐसे तीसरे पक्ष की संस्थाओं के अधिप्रमाणन से सम्बन्धित प्रचालन प्राधिकरण के मानकों एवं विशिष्टियों के अनुरूप हैं और उनकी अनुमोदित स्वतन्त्र लेखापरीक्षा एजेंसियोंद्वारा नियमित लेखापरीक्षा करवाई गयी है;
- ऐसे ग्राहकों के साथ, अपने ग्राहकों को अधिप्रमाणन सेवाएं उपलब्ध कराने के लिए अधिप्रमाणन प्रभारों हेतु सहमत हो सकती है और प्राधिकरण कुछ समय के लिए इस संबंध में कुछ नहीं कहेगा; किन्तु भविष्य में इस संबंध में एक भिन्न क्रियाविधि निर्धारित करने का प्राधिकरण का अधिकार सुरक्षित माना जायेगा;
- (त) वह प्रत्येक समय प्राधिकरण द्वारा प्रावधानित अधिप्रमाणन सुविधाओं के उपयोग के उद्देश्यों के लिए प्राधिकरण द्वारा निर्गत किसी अनुबन्धित शर्तों एवं समस्त नियमों, विनियमों, नीतियों, नियमावलियों, प्रक्रियाओं, विशिष्टियों, मानकों तथा निर्देशों के अनुरूप होगी।

15. हां/ना अधिप्रमाणन सुविधा का उपयोग :-

- (1) अनुरोधकर्ता संस्था, अपने निजी उपयोग अथवा अन्य एजेंसियों की ओर से किसी आधार नंबर धारक की पहचान के सत्यापन के लिए प्राधिकरण द्वारा प्रावधानित हां/ना अधिप्रमाणन सुविधा का उपयोग कर सकती है।
- (2) अनुरोधकर्ता संस्था, प्राधिकरण द्वारा प्रावधानित पोर्टल के माध्यम से किसी अन्य एजेंसी अथवा संस्था को प्रत्येक ऐसी संस्था के लिए एक अलग से लाइसेंस कुंजी के सृजन तथा सहभाजिता द्वारा कथित संस्था को हां/ना अधिप्रमाणन निष्पादन के लिए अनुज्ञा दे सकती है। सन्देह के निराकरण के लिए यह स्पष्ट किया जाता है कि लाइसेंस कुंजी की ऐसी सहभाजिता केवल हां/ना अधिप्रमाणन के निष्पादन हेतु ही अनुज्ञेय है और ई-केवाईसी अधिप्रमाणन की स्थिति में निषिद्ध है।
- (3) ऐसी एजेंसी अथवा संस्था :
- (क) किसी उद्देश्य के लिए किसी अन्य व्यक्ति अथवा संस्था के साथ लाइसेंस कुंजी सहभाजित नहीं करेगी; तथा
- (ख) आधार नंबर धारक की व्यक्तिगत सूचना, डाटा सुरक्षा एवं अनुरोधकर्ता संस्था के लिए प्रयोज्य अन्य प्रासंगिक उत्तरदायित्वों से सम्बद्ध समस्त दायित्वों का अनुपालन करेगी।

- (4) यह सुनिश्चित करना अनुरोधकर्ता संस्था का उत्तरदायित्व होगा कि कोई संस्था अथवा एजेंसी जिसके साथ उसने लाइसेंस कुंजी सहभाजित की है, प्राधिकरण के अधिनियम के प्रावधानों, विनियमों, प्रक्रियाओं, मानकों, दिशा-निर्देशों, विशिष्टियों तथा प्रोटोकॉल के अनुरूप है।
- (5) अनुरोधकर्ता संस्था, लाइसेंस कुंजी सहभाजित की गयी संस्था अथवा एजेंसी सहित प्राधिकरण के विनियमों, प्रक्रियाओं, मानकों, दिशा-निर्देशों तथा प्रोटोकॉल की गैर-अनुरूपता के लिए संयुक्त रूप से तथा पृथक-पृथक उत्तरदायी होगी।

16. ई-केवाईसी अधिप्रमाणन सुविधा का उपयोग :-

- (1) केयूए अपने स्वयं के उद्देश्यों के लिए आधार नंबर धारक का ई-केवाईसी डाटा प्राप्त करने के लिए प्राधिकरण द्वारा प्रावधानित ई-केवाईसी अधिप्रमाणन सुविधा का उपयोग कर सकता है।
- (2) केयूए अन्य एजेंसियों के माध्यम से ई-केवाईसी अधिप्रमाणन निष्पादित कर सकता है, और निर्दिष्ट उद्देश्य के लिए आधार नंबर धारक की सहमति प्राप्त करने के उपरांत इस उद्देश्य के लिए उस एजेंसी के साथ ई-केवाईसी डाटा सहभाजित कर सकता है।
- (3) केयूए आधार नंबर धारक की सहमति से कूटबद्ध प्रारूप में ई-केवाईसी अधिप्रमाणन से प्राप्त किसी आधार नंबर धारक का ई-केवाईसी डाटा भंडारित कर सकता है और तत्पश्चात किसी निर्दिष्ट उद्देश्य के लिए इस ई-केवाईसी डाटा को कथित उद्देश्य के लिए प्रत्येक बार सहभाजित की अलग से सहमति प्राप्त करने के उपरान्त किसी अन्य एजेंसी के साथ सहभाजित कर सकता है।
- (4) वह एजेंसी जिसके साथ केयूए ने आधार नंबर धारक का ई-केवाईसी डाटा सहभाजित किया है, वह एजेंसी केवल आधार नंबर धारक द्वारा कथित उद्देश्य की पूर्ति के लिए सहभाजिता के लिए दी गयी विशेष सहमति के समापन के पश्चात, किसी अन्य एजेंसी से ई-केवाईसी डाटा सहभाजित नहीं करेगी।
- (5) आधार नंबर धारक किसी भी समय अपना ई-केवाईसी डाटा भंडारण करने अथवा इसे किसी तीसरे पक्ष के साथ सहभाजित करने के लिए दी गयी सहमति को वापस ले सकता है, और प्रतिसंहरण की इस स्थिति में केयूए ई-केवाईसी डाटा को डिलीट (समाप्त) करेगा और भावी सहभाजिता अवरुद्ध कर देगा।
- (6) उप-विनियम (4) में उल्लिखित भावी सहभाजिता की निषिद्धि के अतिरिक्त, आधार नंबर धारक की व्यक्तिगत सूचना से सम्बन्धित अन्य समस्त दायित्व, अनुरोधकर्ता संस्थाओं के लिए प्रयोज्य डाटा सुरक्षा एवं अन्य प्रासंगिक उत्तरदायित्व भी उस एजेंसी अथवा संस्था के लिए भी प्रयोज्य होंगे, जिनके साथ विनियम 16 के अनुरूप ई-केवाईसी डाटा सहभाजित किया जा चुका है।
- (7) अनुरोध करने पर केयूए आधार नंबर धारक को ई-केवाईसी डाटा की डिजिटल रूप से हस्ताक्षरित इलेक्ट्रॉनिक प्रति उपलब्ध करायेगा, और आधार नंबर धारक कथित प्रति को किसी भी एजेंसी के साथ सहभाजित कर सकता है।
- बशर्ते कि वह एजेंसी जो आधार नंबर धारक से ई-केवाईसी डाटा के लिए अनुरोध कर रही है, वह ऐसा करने के उद्देश्य के विषय में सूचित करेगी और आधार नंबर धारक की सहमति लेगी।
- बशर्ते कि वह एजेंसी, जिसके साथ आधार नंबर धारक ने ई-केवाईसी डाटा सहभाजित किया है, आधार नंबर धारक द्वारा कथित उद्देश्य की पूर्ति के लिए सहभाजिता के लिए दी गयी विशेष सहमति के समापन के पश्चात किसी अन्य एजेंसी से ई-केवाईसी डाटा सहभाजित नहीं करेगी।
- (8) केयूए ऐसे सभी संव्यवहारों का प्राधिकरण द्वारा निर्दिष्ट समयावधि के लिए एक लेखापरीक्षणिय संलेख अनुरक्षित करेगा, जहां डाटा अन्य एजेंसियों के साथ सहभाजित किया गया है।

17. अनुरोधकर्ता संस्था द्वारा पहचान सूचना के उपयोग से सम्बद्ध दायित्व:-

- (1) अनुरोधकर्ता संस्था सुनिश्चित करेगी कि :
- (क) आधार नंबर धारक से संग्रहीत मुख्य बायोमैट्रिक सूचना को किसी भी उद्देश्य के लिए भंडारित, सहभाजित अथवा प्रकाशित नहीं किया गया है, और उसके पास मुख्य बायोमैट्रिक सूचना की कोई प्रति शेष नहीं है;
- (ख) संग्रहीत मुख्य बायोमैट्रिक सूचना को कूटबद्ध पीआईडी ब्लॉक के सृजन के बिना किसी नेटवर्क पर संप्रेषित नहीं किया गया है, जिसे प्राधिकरण द्वारा निर्धारित विशिष्टियों तथा प्रक्रियाओं के अनुरूप संप्रेषित किया जा सकता है;
- (ग) कूटबद्ध पीआईडी ब्लॉक भंडारित नहीं किया गया है, जब तक कि यह बफरकृत अधिप्रमाणन के लिए है, जहां इसे अल्प समयावधि के लिए अधिप्रमाणन उपकरण पर अस्थायी तौर पर रखा जा सकता है, और संप्रेषण के पश्चात इसे समाप्त कर दिया गया है;
- (घ) अधिप्रमाणन के दौरान, प्राप्त पहचान सूचना केवल अधिप्रमाणन के समय आधार नंबर धारक के लिए निर्दिष्ट उद्देश्य के लिए प्रयुक्त की गयी है, और जिस कार्ड नंबर धारक से यह सूचना सम्बद्ध है, उसकी पूर्व सहमति लिए बिना पुनः प्रकट नहीं की जाएगी;
- (च) अधिप्रमाणन के दौरान, आधार नंबर धारक की पहचान सूचना तथा अधिप्रमाणन प्रक्रिया के दौरान सृजित कोई अन्य सूचना जैसे अभिगम, उपयोग एवं प्रकटन के विरुद्ध संरक्षित रखी गयी है जिसकी अनुमति अधिनियम तथा इसके विनियम के अधीन नहीं है।

- (छ) अधिप्रमाणन अनुरोध के डिजिटल रूप में हस्ताक्षर के लिए प्रयुक्त प्राइवेट (निजी) कुंजी तथा लाइसेंस कुंजी सुरक्षित रखे गये हैं और अभिगम नियन्त्रित हैं; तथा
- (ज) अपने तंत्र में आधार-आधारित पहचान सूचना से सम्बद्ध डाटा भंडारण तथा डाटा संरक्षण से सम्बन्धित समस्त प्रासंगिक कानून एवं विनियम, जो उनके एजेंट (यदि लागू हो) के तथा अधिप्रमाणन उपकरण के विषय में हैं, अनुपालित हैं।

18. अनुरोधकर्ता संस्था द्वारा लॉग का रख-रखाव :-

- (1) अनुरोधकर्ता संस्था को अपने द्वारा अधिप्रमाणित किए गए कार्य के संबंध में नीचे सूचीबद्ध विवरण सहित कार्य लॉग का रख-रखाव करना होगा :-
- (क) आधार नंबर , जिसके अंतर्गत अधिप्रमाणन अपेक्षित है;
- (ख) प्रस्तुत अधिप्रमाणन अनुरोध के लिए विशिष्ट मापदंड;
- (ग) प्राप्त अधिप्रमाणन प्रतिक्रिया के लिए विशिष्ट मापदंड;
- (घ) अधिप्रमाणन के समय आधार नंबर धारक को किया गया सूचना प्रकटीकरण अभिलेख; तथा
- (च) अधिप्रमाणन के लिए आधार नंबर धारक की सहमति का अभिलेख
- परन्तु, किसी भी स्थिति में पीआईडी सूचना का रख-रखाव नहीं किया जाएगा।
- (2) अनुरोधकर्ता संस्था द्वारा अधिप्रमाणन कार्य के लॉग का रखरखाव 2 (दो) वर्ष की अवधि के लिए किया जाएगा तथा इस दौरान आधार नंबर धारक को इस संबंध में निर्धारित प्रक्रिया के अनुसार ऐसे लॉग को एक्सेस करने का अधिकार प्राप्त होगा।
- (3) उप विनियम (2) में विनिर्दिष्ट अवधि की समाप्ति के पश्चात, लॉग को 5 वर्ष की अवधि अथवा विधि अनुसार अथवा संस्था का संचालन करने वाले विनियमों के अनुसार अपेक्षित वर्षों के लिए, इनमें से जो भी बाद में हो, पुरालेख के तौर पर रखा जाएगा तथा उक्त अवधि की समाप्ति के पश्चात किसी न्यायालय अथवा किसी बकाया विवाद के लिए अपेक्षित अभिलेख के अलावा अन्य अभिलेख हटाया जा सकेगा।
- (4) अनुरोधकर्ता संस्था द्वारा संबंधित आधार नंबर धारक से प्राप्त अनुरोध अथवा शिकायत सुनवाई तथा विवादों के समाधान अथवा लेखापरीक्षा उद्देश्यों से प्राधिकरण के अलावा किसी भी अन्य व्यक्ति के साथ अधिप्रमाणन लॉग का सहभाजन नहीं किया जाएगा। इस उप विनियम में उल्लिखित उद्देश्य के अलावा किसी अन्य उद्देश्य से अधिप्रमाणन लॉग का प्रयोग नहीं किया जाना है।
- (5) अनुरोधकर्ता संस्था द्वारा लॉग के भंडारण के संबंध में सूचना प्रौद्योगिकी अधिनियम, 2000 तथा साक्ष्य अधिनियम, 1872 सहित, परन्तु सीमित नहीं, सभी संबंधित विधियों, नियमों तथा विनियमों का पालन किया जाएगा।
- (6) इस विनियम में विनिर्दिष्ट अधिप्रमाणन लॉग से संबंधित दायित्व इन विनियमों के अनुसार संस्था की नियुक्ति निरस्त करने के बावजूद भी मान्य रहेंगे।

19. अधिप्रमाणन सेवा एजेंसियों की भूमिका, उत्तरदायित्व एवं आचार संहिता :-

अधिप्रमाणन सेवा एजेंसी के क्रियाकलाप तथा दायित्व निम्नानुसार होंगे :-

- (क) अनुरोधकर्ता संस्था द्वारा अधिप्रमाणन अनुरोध ट्रांसमिट करने के लिए केन्द्रीय पहचान आंकड़े निक्षेपागार (सीआईडीआर) के साथ प्राधिकरण द्वारा इस उद्देश्य हेतु विनिर्दिष्ट विधि के अनुसार सुरक्षित कनेक्टिविटी उपलब्ध करवाना;
- (ख) सीआईडीआर को प्रेषित करने से पूर्व अधिप्रमाणन डाटा पैकेट से संबंधित बुनियादी अनुपालन एवं पूर्णतः जांच से संबंधित अनुपालन करना;
- (ग) सीआईडीआर से प्रतिक्रिया प्राप्त होने पर अनुरोधकर्ता संस्था को अनुरोध पर किए गए कार्य के परिणाम संप्रेषित करना;
- (घ) केवल प्राधिकरण द्वारा अनुमोदित अनुरोधकर्ता संस्थाओं के साथ कार्य करना तथा स्वयं द्वारा सेवित अनुरोधकर्ता संस्थाओं की सूची की जानकारी प्राधिकरण को देना;
- (च) अनुरोधकर्ता संस्था के साथ किए गए अनुबंधों की प्रत्येक संबंधित जानकारी प्राधिकरण को सूचित करना;
- (छ) यह सुनिश्चित करना कि स्वयं द्वारा नियुक्त व्यक्ति अधिप्रमाणन कार्य तथा आवश्यक सिस्टम, अवसंरचना, प्रक्रियाओं इत्यादि के रख-रखाव के कार्यों के लिए अपेक्षित योग्यता प्राप्त हैं;
- (ज) प्रचालनों की लेखापरीक्षा किसी मान्यता प्राप्त निकाय द्वारा प्रमाणित सूचना प्रणाली लेखापरीक्षकों द्वारा वार्षिक आधार पर किया जाए तथा इस संबंध में समय-समय पर प्राधिकरण द्वारा जारी नीतियों, प्रक्रियाओं, कार्यविधियों, मानकों, अथवा विशिष्टताओं के अनुपालन की पुष्टि की प्रमाणित लेखापरीक्षा रिपोर्ट प्राधिकरण को उपलब्ध करवाना सुनिश्चित करना;
- (झ) इस उद्देश्य से सिस्टम, प्रक्रियाएं, उपकरण, सॉफ्टवेयर एवं बायोमैट्रिक अवसंरचना, सुरक्षा तथा अन्य संबंधित घटकों सहित सभी अवसंरचनाएं एवं प्रचालन प्राधिकरण द्वारा विनिर्दिष्ट मानकों एवं विशिष्टताओं के अनुरूप होना सुनिश्चित करना;
- (ट) नेटवर्क तथा अन्य सूचना प्रौद्योगिकी अवसंरचना, प्रक्रियाओं, कार्यविधियों इत्यादि के संबंध में प्राधिकरण द्वारा जारी निदेशों, विशिष्टताओं इत्यादि का पूर्णतः अनुसरण करना;
- (ठ) सभी संबंधित विधानों तथा विनियमों, विशेष रूप से डाटा सुरक्षा तथा डाटा प्रबंधन, का अनुपालन;
- (ड) अधिप्रमाणन सेवा एजेंसियों द्वारा किसी अनुरोधकर्ता संस्था को अनुबंध के अंतर्गत प्रदान की गई अन्य मूल्यवर्धित सेवाएं आधार अधिप्रमाणन प्रक्रिया का भाग नहीं होंगी;

- (ढ) प्राधिकरण के प्रति अधिप्रमाणन से संबंधित सभी प्रचालनों, अधिप्रमाणन सेवा एजेंसी के उप-अनुबंध के अंतर्गत अपने प्रचालन अन्य संस्थाओं को दिए जाने के मामले में भी, के लिए उत्तरदायित्व अधिप्रमाणन सेवा एजेंसी का होगा;
- (ण) अधिप्रमाणन से सम्बद्ध धोखेबाजी अथवा विवाद से संबंधित मामले की जांच के लिए अधिप्रमाणन सेवा एजेंसी द्वारा प्राधिकरण (अथवा उसकी एजेंसी) तथा/अथवा अन्य प्राधिकृत जांच एजेंसी को अपने परिसर, अभिलेख, सिस्टम, कर्मियों, अवसंरचना, अन्य किसी संबंधित संसाधन अथवा सूचना तथा अन्य अधिप्रमाणन प्रचालनों से संबंधित अन्य घटक तक पहुँच सहित पूर्ण सहयोग प्रदान किया जाएगा;
- (त) किसी अनुरोधकर्ता संस्था को अधिप्रमाणन प्रभारों पर सेवाएं प्रदान करने की सहमति दी जा सकेगी तथा, ऐसी अनुरोधकर्ता संस्था से, प्राधिकरण का इस मामले में सामयिक तौर पर कोई हस्तक्षेप नहीं होगा, तथापि, ऐसे मामले में प्राधिकरण के पास भविष्य में किसी भिन्न तंत्र व्यवस्था के निर्धारण करने का अधिकार सुरक्षित होगा;
- (थ) प्राधिकरण द्वारा किसी भी समय पर जारी प्रत्येक संविदागत शर्तों तथा सभी नियमों, विनियमों, नीतियों, मैनुअलों, प्रक्रियाओं, विशिष्टताओं, मानकों तथा निदेशों का पूर्णतः पालन किया जाएगा।

20. अधिप्रमाणन सेवा एजेंसियों द्वारा लॉग का रखरखाव :-

- (1) अधिप्रमाणन सेवा एजेंसी द्वारा स्वयं निष्पादित अधिप्रमाणन कार्यों के लॉग का रख-रखाव किया जाएगा, जिसके कार्य में नीचे उल्लिखित विवरण होगा नामतः-
- (क) अनुरोधकर्ता संस्था की पहचान;
- (ख) प्रस्तुत अधिप्रमाणन अनुरोध के मापदंड; तथा
- (ग) प्राप्त अधिप्रमाणन प्रक्रिया के मापदंड:
- बशर्ते यह कि जहां लागू होगा, वहां आधार नंबर, पीआईडी सूचना, उपकरण पहचान से संबंधित डाटा तथा ई-केवाईसी प्रतिक्रिया डाटा, का प्रतिधारण नहीं किया जाएगा।
- (2) अधिप्रमाणन सेवा एजेंसी द्वारा अधिप्रमाणन कार्य के लॉग का रख-रखाव 2 (2) वर्ष की अवधि के लिए किया जाएगा तथा इस दौरान प्राधिकरण तथा/अथवा अनुरोधकर्ता संस्था द्वारा शिकायत निवारण, विवाद निपटान तथा लेखापरीक्षा कार्यों से इन विनियमों में विनिर्दिष्ट प्रक्रिया के अनुसार ऐसे अभिलेख के प्रयोग की मांग की जा सकेगी। इस उप विनियम में उल्लिखित उद्देश्य के अलावा किसी अन्य उद्देश्य से अधिप्रमाणन अभिलेख का प्रयोग नहीं किया जाएगा।
- (3) उप विनियम (2) में विनिर्दिष्ट अवधि की समाप्ति के पश्चात, लॉग को 5 वर्ष की अवधि अथवा विधि अनुसार अथवा संस्था का संचालन करने वाले विनियमों के अनुसार अपेक्षित वर्षों की नंबर के लिए, इनमें से जो भी बाद में हो, पुरालेख के तौर पर रखा जाएगा तथा उक्त अवधि की समाप्ति के पश्चात किसी न्यायालय अथवा किसी बकाया विवाद के लिए अपेक्षित लॉग के अलावा अन्य अभिलेख हटाया जा सकेगा।
- (4) अधिप्रमाणन सेवा एजेंसी द्वारा लॉग के भंडारण के संबंध में सूचना प्रौद्योगिकी अधिनियम, 2000 सहित सभी संबंधित विधियों का पालन किया जाएगा।
- (5) इस विनियम में विनिर्दिष्ट अधिप्रमाणन लॉग से संबंधित दायित्व इन विनियमों के अनुसार नियुक्ति निरस्त होने के बावजूद भी मान्य रहेंगे।

21. अनुरोधकर्ता संस्थाओं तथा अधिप्रमाणन सेवा एजेंसियों की लेखापरीक्षा :-

- (1) प्राधिकरण स्वयं अथवा उसके द्वारा नियुक्त अपनी लेखापरीक्षा एजेंसियों के माध्यम से अधिनियम, नियमावली, विनियमों, नीतियों, प्रक्रियाओं, प्राधिकरण द्वारा जारी दिशानिर्देशों के अनुपालन को सुनिश्चित करने के लिए अनुरोधकर्ता संस्थाओं, ऐसी एजेंसियों अथवा संस्थाओं सहित, जिनके साथ उन्होंने लाइसेंस कुंजी का सहभाजन किया है अथवा ऐसी संस्थाओं, जिनकी ओर से वे अधिप्रमाणन कार्य का निष्पादन कर रहे हैं तथा अधिप्रमाणन सेवा एजेंसियों का उनके प्रचालनों, अवसंरचना, सिस्टम एवं प्रक्रियाओं के संबंध में लेखापरीक्षा करसकता है।
- (2) प्राधिकरण स्वयं अथवा प्राधिकरण द्वारा नियुक्त लेखापरीक्षा के माध्यम से उप-विनियम (1) में संदर्भित संस्थाओं के प्रचालनों तथा सिस्टम का लेखापरीक्षा कर सकती है। ऐसे लेखापरीक्षा की बारम्बारता, समय एवं प्रक्रिया समय-समय पर प्राधिकरण द्वारा अधिसूचित की जाएगी।
- (3) लेखापरीक्षा की जाने वाली संस्था द्वारा प्राधिकरण अथवा प्राधिकरण द्वारा अनुमोदित तथा/अथवा प्राधिकरण द्वारा नियुक्त एजेंसी को लेखापरीक्षा प्रक्रिया के दौरान पूर्ण सहयोग प्रदान किया जाएगा तथा प्राधिकरण अथवा प्राधिकरण द्वारा अनुमोदित तथा/अथवा नियुक्त एजेंसी को अपनी प्रक्रिया, अभिलेखों तथा प्राधिकरण से प्राप्त सेवाओं से संबंधित सूचना के लिए पूर्ण पहुंच प्रदान की जाएगी। लेखापरीक्षा की लागत का वहन संबंधित संस्था द्वारा किया जाएगा।
- (4) प्राधिकरण द्वारा किसी प्रकार की त्रुटि की शिनाख्त किए जाने पर प्राधिकरण संबंधित संस्था से आवश्यक स्पष्टीकरण तथा/अथवा इसके क्रियाकलापों से संबंधित सूचना प्रस्तुत करने के लिए कहा जा सकेगा तथा ऐसी संस्था से ऐसी त्रुटि के निवारण अथवा इन विनियमों में विनिर्दिष्ट कार्रवाई करने की अपेक्षा की जा सकेगी।

22. डाटा सुरक्षा :-

- (1) अनुरोधकर्ता संस्था तथा अधिप्रमाणन सेवा एजेंसी द्वारा आधार अधिप्रमाणन अनुरोध कार्यों एवं केन्द्रीय पहचान आंकड़े निक्षेपागार (सीआईडीआर) को सम्प्रेषण के लिए भारत में स्थित डाटा केन्द्रों से अपने सर्वरों का उपयोग करना होगा।
- (2) अधिप्रमाणन सेवा एजेंसी प्राधिकरण के डाटा केन्द्र के साथ इस उद्देश्य से प्राधिकरण द्वारा निर्दिष्ट प्रक्रिया तथा सुरक्षा कार्यविधियों के अनुसार दोहरी रेडन्डेंट, सुरक्षित लीड लाइनें अथवा एमपीएलएस कनेक्टिविटी की स्थापना करेगी।

- (3) अनुरोधकर्ता संस्थाओं अधिप्रमाणन सेवा पहुंच के माध्यम से केवल प्राधिकरण से उपलब्ध करवाई गई अधिप्रमाणन सुविधा पर पहुंच के लिए उचित लाइसेंस कुंजी का प्रयोग, केवल प्राधिकरण द्वारा इस उद्देश्य से निर्दिष्ट सुरक्षित नेटवर्क से करेगी।
- (4) अनुरोधकर्ता संस्थाओं तथा अधिप्रमाणन सेवा एजेंसियाँ प्राधिकरण द्वारा समय-समय पर जारी सभी विनियमों, सूचना सुरक्षा नीतियों, प्रक्रियाओं, मानकों, विनिर्देशों तथा दिशा-निर्देशों का अनुपालन करेगी।

23. अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी द्वारा अधिप्रमाणन सुविधा की पहुंच को छोड़ना:-

- (1) प्राधिकरण द्वारा प्रदान की गई अधिप्रमाणन सुविधा के लिए प्रदान की गई पहुंच को छोड़नेकी इच्छुक, इन विनियमों के अंतर्गत नियुक्त की गई, अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी ऐसे सरेंडर के लिए अपना आवेदन प्राधिकरण को प्रस्तुत कर सकती हैं।
- (2) इन विनियमों के अंतर्गत सरेंडर के लिए प्राप्त अनुरोध का निपटान करते समय प्राधिकरण द्वारा अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी की सेवाओं को समाप्त करने के लिए निम्नलिखित सहित किसी भी आवश्यक मामले के प्रति प्राधिकरण को संतुष्ट करने की अपेक्षा की जा सकती है :-
 - (क) अधिप्रमाणन अभिलेख के रख-रखाव तथा परिरक्षण के लिए अनुरोधकर्ता संस्था द्वारा की गई व्यवस्था तथा इन विनियमों एवं प्रक्रियाओं के अनुसार इस उद्देश्य से प्राधिकरण द्वारा विनिर्दिष्ट अन्य दस्तावेज;
 - (ख) अनुरोधकर्ता संस्था द्वारा संबंधित आधार नंबर धारक से अनुरोध प्राप्त होने पर उपलब्ध कराने हेतु अधिप्रमाणन अभिलेख के रख-रखाव की व्यवस्था;
 - (ग) शिकायतों के निपटान, यदि कोई हों, का अभिलेख;
 - (घ) प्राधिकरण के साथ किया गया लेखा निपटान, यदि कोई हो;
 - (च) अधिप्रमाणन सेवा एजेंसी द्वारा सरेंडर किए जाने के मामले में अधिप्रमाणन सेवा एजेंसी को अपनी पहुंच छोड़ने करने से पूर्व अपनी सम्बद्ध अनुरोधकर्ता संस्थाओं को अन्य अधिप्रमाणन सेवा एजेंसियों के प्रचालन में जाने के लिए पर्याप्त समय देना सुनिश्चित करेगी।

24. इन विनियमों के लागू होने से पूर्व नियुक्त की गई एजेंसियां :-

- (1) इन विनियमों के अंतर्गत, इन विनियमों के लागू होने से पूर्व नियुक्त की गई अधिप्रमाणन उपयोक्ता एजेंसी (एयूए) अथवा ई-केवाईसी उपयोक्ता एजेंसी (केयूए) को अनुरोधकर्ता संस्था तथा अधिप्रमाणन सेवा एजेंसी (एएसए) अथवा ई-केवाईसी सेवा एजेंसी (केएसए) को अधिप्रमाणन सेवा एजेंसी माना जाएगा तथा ऐसी एजेंसियों एवं योजना आयोग, भारत सरकार के दिनांक 28 जनवरी, 2009 की अधिसूचना नंबर ए-43011/02/2009-प्रशासन-1 के अधीन स्थापित भारतीय विशिष्ट पहचान प्राधिकरण अथवा ऐसे प्राधिकरण के किसी अधिकारी के मध्य अधिनियम के अंतर्गत किए गए सभी अनुबंध प्राधिकरण द्वारा जारी अधिनियम के प्रावधानों, इनके विनियमों तथा अन्य विनियमों, नीतियों, प्रक्रियाओं, कार्यविधियों, मानकों तथा विशिष्टताओं के साथ असंगत न होने की सीमा तक प्रभावी रहेंगे।
- (2) उप-विनियम (1) में उल्लिखित होने के बावजूद भी उप-विनियम (1) में संदर्भित किसी मान्यताप्राप्त अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी से अधिनियम के प्रावधानों, इन विनियमों, प्राधिकरण द्वारा निर्मित अन्य विनियमों, तथा प्राधिकरण द्वारा जारी नीतियों, प्रक्रियाओं, कार्यविधियों, मानकों तथा विशिष्टताओं का अनुपालन करने की अनिवार्यता होगी।
- (3) उप-विनियम (1) में संदर्भित किसी एजेंसी द्वारा इन विनियमों में निर्दिष्ट अधिप्रमाणन सेवाओं से विलग होने की अपेक्षा की स्थिति में वह अपने प्रत्यय पत्र एवं अपने क्रियाकलापों की तुरंत समाप्ति के लिए आवेदन प्रस्तुत कर सकती है :
बशर्ते कि ऐसे मामले में सेवाएं समाप्त करने पर एजेंसी अथवा प्राधिकरण को किसी मुआवजे का भुगतान नहीं किया जाएगा।
- (4) उप-विनियम(3) के अधीन सेवाएं समाप्त किए जाने की स्थिति में संबंधित संस्था से विनियम 23(2) उल्लिखित कार्य समापन अपेक्षाओं का पालन करने की अनिवार्यता होगी।

25. चूक की स्थिति में देयताएं एवं कार्रवाई :-

- (1) इस अधिनियम के अंतर्गत नियुक्त किसी संस्था अथवा अधिप्रमाणन सेवा एजेंसी यदि :-
 - (क) प्राधिकरण द्वारा समय-समय पर जारी किन्हीं प्रक्रियाओं, कार्यविधियों, मानकों, विशिष्टताओं अथवा निदेशों का अनुपालन नहीं करती है;
 - (ख) अधिनियम तथा इन विनियमों के दायित्वों का उल्लंघन करती है;
 - (ग) आधार अधिप्रमाणन सुविधाओं का प्रयोग, अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी की नियुक्ति के लिए दिए गए आवेदन में की गई निर्दिष्ट के अलावा किन्हीं अन्य उद्देश्यों से करती है;
 - (घ) इन विनियमों के उद्देश्यों से प्राधिकरण द्वारा अपेक्षित किसी सूचना को प्रस्तुत नहीं कर पाती है; अथवा
 - (च) प्राधिकरण द्वारा किसी निरीक्षण अथवा जांच अथवा पृष्ठताछ अथवा लेखापरीक्षा के दौरान सहयोग नहीं करती है,

तो प्राधिकरण द्वारा, इस अधिनियम के अध्याधीन की जाने वाली किसी अन्य कार्रवाई के प्रति किसी प्रतिकूलता के बिना, अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी के विरुद्ध अधिनियम के प्रावधानों, उससे संबंधित नियमों एवं विनियमों का उल्लंघन करने पर ऐसी संस्था अथवा एजेंसी के क्रियाकलापों को समाप्त करने सहित दंडात्मक कार्रवाई के उपाय अथवा ऐसे अन्य उपाय किए जा सकेंगे, जिनके संबंध में ऐसी संस्था तथा प्राधिकरण के मध्य किए गए अनुबंध में विशिष्ट व्यवस्था की गई हो ।

बशर्ते कि आधार अधिप्रमाणन से संबंधित सेवाओं तथा प्रचालनों की समाप्ति से पूर्व ऐसी संस्था अथवा एजेंसी को सुनवाई का अवसर प्रदान किया जाएगा ।

- (2) उप-विनियम (1) में संदर्भित ऐसी कार्रवाई किसी संस्था अथवा एजेंसी, जिसके साथ किसी अधिप्रमाणन सेवा एजेंसी द्वारा हॉ/नहीं अधिप्रमाणन की लाइसेंस कुंजी का सहभाजन किया गया हो तथा किसी ऐसी संस्था जिसके साथ ई-केवाईसी प्रयोक्ता एजेंसी द्वारा ई-केवाईसी डाटा का सहभाजन किया गया हो, के विरुद्ध भी की जा सकेगी ।
- (3) प्राधिकरण द्वारा सेवाएं समाप्त किए जाने पर अनुरोधकर्ता संस्था अथवा अधिप्रमाणन सेवा एजेंसी द्वारा आधार नाम तथा लोगो का प्रयोग, किसी भी स्वरूप तथा उद्देश्य, कारण चाहे कुछ भी हो, से नहीं किया जा सकेगा तथा उसे विनियम 23(2) में सूचीबद्ध घटकों सहित समापन के आवश्यक घटकों के प्रति प्राधिकरण को संतुष्ट करना होगा ।

अध्याय-4

अधिप्रमाणन कार्य क्रिया डाटा तथा अधिप्रमाणन अभिलेख

26. अधिप्रमाणन कार्यक्रियाडाटा का भंडारण एवं रख-रखाव :-

- (1) प्राधिकरण द्वारा निम्नलिखित सूचना से युक्त अधिप्रमाणन कार्य क्रिया डाटा का भंडारण एवं रख-रखाव किया जा सकेगा :-
 - (क) पीआईडी ब्लॉक सहित प्राप्त अधिप्रमाणन अनुरोध डाटा
 - (ख) प्रेषित अधिप्रमाणन प्रतिक्रिया डाटा
 - (ग) कार्य संचलन से सम्बद्ध मेटा डाटा
 - (घ) आवश्यकतानुसार अधिप्रमाणन सर्वर साईड विन्यास
 बशर्ते कि प्राधिकरण द्वारा किसी भी मामले में अधिप्रमाणन के उद्देश्य का भंडारण नहीं किया जाएगा ।

27. भंडारण की अवधि :-

- (1) प्राधिकरण द्वारा अधिप्रमाणन कार्य डाटा का भंडारण 6 माह की अवधि के लिए किया जाएगा तथा इसे 5 वर्ष की अवधि के लिए पुरालेख के तौर पर रखा जाएगा ।
- (2) उप - विनियम (1) में उल्लिखित 5 वर्ष की निर्दिष्ट अवधि की समाप्ति के पश्चात किसी न्यायालय अथवा किसी बकाया विवाद के लिए अपेक्षित अभिलेख के लिए रख-रखाव के अलावा अन्य अभिलेख हटाया जा सकेगा ।

28. आधार नंबर धारक द्वारा एक्सेस :-

(1)	विहित शर्तों तथा प्राधिकरण द्वारा निर्धारित शुल्क का भुगतान करने पर आधार नंबर धारक को अभिलेखों का पुरालेख किए जाने से पूर्व अनुरक्षण किए जाने की अवधि के दौरान, प्राधिकरण के सम्मुख आवेदन प्रस्तुत करके अपने अधिप्रमाणन अभिलेख को एक्सेस करने का अधिकार प्राप्त होगा ।
(2)	इन विनियमों में निर्दिष्ट के अनुसार, पुरालेख से पूर्व अनुरक्षण की अवधि के दौरान आधार, आधार नंबर धारकों को अपने डिजिटली हस्ताक्षरित सत्यापित अभिलेख की प्राप्ति के लिए प्राधिकरण द्वारा ऑनलाईन पोर्टल अथवा मोबाइल एप्लीकेशन अथवा निर्दिष्ट संपर्क केन्द्र की सुविधा उपलब्ध करवाई जा सकती है ।
(3)	प्राधिकरण द्वारा बायोमैट्रिक अथवा ओटीपी के माध्यम से निर्धारित शुल्क के भुगतान तथा प्रक्रियाओं के अनुसार आधार नंबर धारकों को डिजिटली हस्ताक्षरित ई-केवाईसी डाटा उपलब्ध करवाया जा सकता है ।
(4)	सत्यापित अभिलेख तथा ई-केवाईसी डाटा का सहभाजन किसी व्यक्ति अथवा संस्था के साथ नहीं किया जा सकेगा :-
	(क) आधार नंबर धारक जिनसे अभिलेख या ई-केवाईसी डाटा विनिर्दिष्ट अधिप्रमाणन प्रक्रिया के अनुसार संबंधित है, के अलावा किसी अन्य के साथ । आधार नंबर धारक द्वारा अपने डिजिटली हस्ताक्षरित सत्यापित अभिलेख तथा ई-केवाईसी डाटा का सहभाजन अन्य संस्थाओं के साथ किया जा सकेगा, जो ऐसे सहभाजन आधार नंबर धारक से प्रत्येक बार अनुमति प्राप्त किए बिना नहीं करेंगे ।
	(ख) अधिनियम में किए गए उल्लेख के अलावा ।

अध्याय - 5

विविध

29. व्यावृत्ति :-

भारत सरकार के योजना आयोग के दिनांक 28 जनवरी, 2009 की अधिसूचना संख्या ए-43011/02/2009-प्रशासन-1 के माध्यम से स्थापित भारतीय विशिष्ट पहचान प्राधिकरण अथवा ऐसे प्राधिकरण के किसी अधिकारी अथवा अधिनियम के तहत प्राधिकरण की स्थापना पूर्व द्वारा जारी सभी कार्यपद्धति, आदेश, प्रक्रियाएं, मानक तथा नीतियां अथवा हस्ताक्षर किए सभी समझौता ज्ञापन, करार अथवा सविदाएं उस सीमा तक लागू रहेंगी, जबतक कि वे अधिनियम के उपबंधों तथा इनके तहत तैयार किए गए अधिनियम अथवा विनियम के तहत असंगत सिद्ध न हो जाएं।

30. स्पष्टीकरण तथा दिशानिर्देशों को जारी करने की शक्ति तथा कठिनाईयों का निराकरण:-

इन विनियमों के अनुप्रयोग अथवा निर्वचन से संबंधित मामलों को स्पष्ट करने अथवा इन विनियमों के कार्यान्वयन में किन्हीं कठिनाईयों का निराकरण करने के लिए, प्राधिकरण के पास परिपत्र के रूप में स्पष्टीकरण तथा दिशानिर्देश जारी करने की शक्ति होगी, जिनका प्रभाव विनियम के समान होगा।

अनुसूची- क

अनुरोधकर्ता संस्थाओं की नियुक्ति के लिए पात्रता मापदंड

विनियम 10(1)देखें

1. अनुरोधकर्ता संस्था के रूप में प्राधिकरण द्वारा उपलब्ध करवाई जाने वाली अधिप्रमाणन सुविधा के प्रयोग की अपेक्षा रखने वाली संस्थाओं के लिए अधिप्रमाणन उपयोक्ता एजेंसी (एयूए) तथा/अथवा ई-केवाईसी उपयोक्ता एजेंसी (केयूए), जैसा भी मामला हो, की नियुक्ति के लिए निम्नलिखित श्रेणियां वर्गीकृत की गई हैं :-

क्रम संख्या	संस्था श्रेणी
श्रेणी - 1	
सरकारी संस्थाएं	
1.1	केन्द्र/राज्य सरकार के मंत्रालय/विभाग तथा उनके सम्बद्ध अथवा अधीनस्थ कार्यालय
1.2	केन्द्र/राज्य सरकार के स्वामित्व तथा अधीन उपक्रम (सरकारी क्षेत्र के उपक्रम)
1.3	केन्द्रीय/राज्य अधिनियम के अंतर्गत स्थापित प्राधिकरण/केन्द्र/राज्य सरकार द्वारा संस्थापित विशेष उद्देश्य संस्थान
श्रेणी - 2	
विनियमित सेवा प्रदाता	
2.1	भारतीय रिजर्व बैंक द्वारा विनियमित/लाइसेंस प्राप्त-बैंक तथा भुगतान एवं निपटान प्रणाली
2.1.1	सरकारी क्षेत्र के बैंक
2.1.2	निजी बैंक, भारत में प्रचालन के लिए भारतीय रिजर्व बैंक से लाइसेंस प्राप्त विदेशी बैंक, भुगतान बैंक, लघु वित्त बैंक
2.1.3	क्षेत्रीय ग्रामीण बैंक
2.1.4	सहकारी बैंक राज्य सहकारी बैंक जिला सहकारी बैंक अनुसूचित शहरी सहकारी बैंक गैर अनुसूचित शहरी सहकारी बैंक
2.1.5	भुगतान एवं निपटान प्रणाली नेटवर्क वित्तीय बाजार अवसंरचना 2 खुदरा भुगतान संस्था 3 कार्ड भुगतान नेटवर्क 4 एटीएम नेटवर्क 5 पूर्व-भुगतान प्रपत्र 6 व्हाईट लेबल एटीएम ऑपरेटर 7 इन्स्टैंट मनी ट्रांसफर
2.1.6	गैर बैंकिंग वित्त कम्पनियां
2.2	आईआरडीए/पीएफआरडीए द्वारा विनियमित-वित्तीय संस्थान
2.3	भारतीय दूरसंचार विनियामक प्राधिकरण द्वारा विनियमित - दूरसंचार
2.4	सीसीए द्वारा विनियमित - प्रमाणन प्राधिकरण, डिजीटल लॉकर प्रदाता, ई-हस्ताक्षर प्रदाता
2.5	सेबी द्वारा विनियमित - केवाईसी पंजीकरण एजेंसी (केआरए), डिपोजिटरी पार्टिसिपेंट (डीपी), एस्सेट मैनेजमेंट कम्पनी

क्रम संख्या	संस्था श्रेणी
	(एएमसी), ट्रेडिंग एक्सचेंज , रजिस्ट्रार एंड ट्रांसफर एजेंट
2.6	राष्ट्रीय आवास बैंक द्वारा संचालित
श्रेणी - 3	अन्य संस्थाएं
3.1	3.1.1 कंपनी अधिनियम, 1956 / कंपनी अधिनियम, 2013 के अंतर्गत भारत में पंजीकृत कम्पनी (समूह कम्पनियों के अंतर्गत किसी कम्पनी को अलग से आवेदन करना होगा)
	3.1.2 भारतीय साझेदारी अधिनियम, 1932 अथवा सीमित दायित्व साझेदारी अधिनियम, 2008 के अंतर्गत भारत में पंजीकृत साझेदारी
	3.1.3 स्वामित्व वाली फर्म
	3.1.4 गैर लाभकारी संगठन (कंपनी अधिनियम 1956 के खंड 25 के अधीन)
	3.1.5 अकादमिक संस्थान / अनुसंधान एवं विकास संगठन
	3.1.6 इंडियन सोसायटिज रजिस्ट्रेशन अधिनियम, 1860 अथवा भारतीय न्यास अधिनियम, 1882 अथवा कंपनी अधिनियम, 2013 (खंड 8) / सहकारी समिति अधिनियम, 1912 के अंतर्गत पंजीकृत सोसायटियां
	3.1.7 उपर्युक्त श्रेणियों के अलावा अन्य संस्थान

2. अनुरोधकर्ता संस्था के तौर पर संस्थाओं की नियुक्ति के लिए तकनीकी एवं वित्तीय मापदंड निम्नानुसार हैं:-

श्रेणी	अधिप्रमाणन उपयोक्ता एजेंसी (एयूए)		ई-केवाईसी उपयोक्ता एजेंसी के लिए अतिरिक्त अपेक्षाएं (केयूए)
	तकनीकी अपेक्षाएं	वित्तीय अपेक्षाएं	
श्रेणी - 1	1. आधार अधिप्रमाणन के उद्देश्य से संस्था के पास सर्वर, डाटाबेस इत्यादि जैसी विशेषतः अपेक्षित बैकएंड अवसंरचना भारतीय क्षेत्र में स्थापित होनी चाहिए ।	कोई वित्तीय अपेक्षाएं नहीं	केयूए के लिए कोई अतिरिक्त अपेक्षाएं नहीं
श्रेणी - 2	2. संस्था के पास अपने स्वामित्व अथवा बाह्य स्रोतों से प्राप्त प्रतिमाह 1 लाख अधिप्रमाणन कार्यों के लिए सक्षम आईटी अवसंरचना होनी चाहिए । 3. लाभग्राही की गोपनीयता के संरक्षण के लिए संस्था के पास निर्धारित डाटा गोपनीयता नीति होनी चाहिए । 4. संस्था के पास आईटी अधिनियम, 2000 के अनुसार अंगीकृत डाटा सुरक्षा अपेक्षाएं होनी चाहिए ।	कोई वित्तीय अपेक्षाएं नहीं	केयूए के लिए कोई अतिरिक्त अपेक्षाएं नहीं
श्रेणी - 3	1. आधार अधिप्रमाणन के उद्देश्य से संस्था के पास सर्वर, डाटाबेस इत्यादि जैसी विशेषतः अपेक्षित बैकएंड अवसंरचना भारतीय क्षेत्र में स्थापित होनी चाहिए । 2. संस्था के पास अपने स्वामित्व अथवा बाह्य स्रोतों से प्राप्त प्रतिमाह 1 लाख अधिप्रमाणन कार्यों के लिए सक्षम आईटी अवसंरचना होनी चाहिए । 3. लाभग्राही की गोपनीयता के संरक्षण के लिए संस्था के पास निर्धारित डाटा गोपनीयता नीति होनी चाहिए । 4. संस्था के पास आईटी अधिनियम, 2000 के अनुसार अंगीकृत डाटा सुरक्षा अपेक्षाएं होनी चाहिए । 5. संस्था इस व्यवसाय को प्रारम्भ करने की तिथि से कम से कम 1 वर्ष से इस व्यवसाय में होनी चाहिए ।	न्यूनतम 1 (एक) करोड़ की चुकता पूंजी अथवा पिछले वित्तीय वर्ष के दौरान न्यूनतम 5 (पांच) करोड़ रुपए की वार्षिक टर्नओवर	संस्था प्राधिकरण द्वारा समय-समय पर निर्धारित अधिप्रमाणन कार्य मापदंडों के अनुरूप होनी चाहिए ।

अनुसूची- ख

अधिप्रमाणन सेवा एजेंसियों के लिए पात्रता मापदंड

विनियम 10(2) देखें

1. अधिप्रमाणन सेवाओं के लिए अनुरोधकर्ता संस्थाओं के लिए केन्द्रीय पहचान आंकड़े निक्षेपागार (सीआईडीआर) एक्सेस की अपेक्षा रखने वाली संस्थाओं को अभिप्रमाणन सेवा एजेंसी के तौर पर नियुक्ति के लिए निम्नलिखित श्रेणियों में वर्गीकृत किया गया है :-

क्र. संख्या	संस्था श्रेणी
श्रेणी - 1	केन्द्र/राज्य सरकार के मंत्रालय/विभाग तथा केन्द्र/राज्य सरकार के सम्बद्ध अथवा अधीनस्थ कार्यालय
श्रेणी - 2	केन्द्र/राज्य अधिनियम के अध्याधीन स्थापित प्राधिकरण
श्रेणी - 3	प्राधिकरण द्वारा निश्चित राष्ट्रीय महत्व की कोई संस्था
श्रेणी - 4	कंपनी अधिनियम, 1956 के अधीन भारत में पंजीकृत कोई कंपनी
श्रेणी - 5	अधिप्रमाणन उपयोक्ता एजेंसी (एयूए)/ई-केवाईसी उपयोक्ता एजेंसी(केयूए)

2. अधिप्रमाणन सेवा एजेंसी के तौर पर संस्थाओं की नियुक्ति के लिए तकनीकी एवं वित्तीय मापदंड निम्नानुसार हैं :-

श्रेणी	वित्तीय अपेक्षाएं	तकनीकी अपेक्षाएं
श्रेणी 1, 2 तथा 3	कोई वित्तीय अपेक्षाएं नहीं	कोई तकनीकी अपेक्षाएं नहीं
श्रेणी - 4	पिछले तीन वित्तीय वर्षों में वार्षिक टर्नओवर कम से कम 100 करोड़ रूपए	दूरसंचार सेवा प्रदाता (टीएसपी) सहित सभी संघटित लाइसेंसी (एक्सेस सेवा प्राधिकार से युक्त)/संघटित लाइसेंसी (एसएस)/संघटित एक्सेस सेवा लाइसेंसी/ सेल्युलर मोबाइल टेलीफोन सेवा लाइसेंस धारक, जो पैन-इंडिया फाइबर ऑप्टिक नेटवर्क का प्रचालन कर रहे हैं तथा जिनके पास सभी राज्यों के लिए न्यूनतम 100 एमपीएलएस प्वाइंट(पीओएस) उपलब्ध है। अथवा नेटवर्क सेवा प्रदाता (एनएसपी) अथवा डाटा ट्रांसमिशन के लिए पैन-इंडिया नेटवर्क कनेक्टिविटी के लिए सिस्टम इन्टीग्रेटर होना चाहिए तथा भारत में 100 एमपीएलएस पीओपी (पीओपी) होनी चाहिए।
श्रेणी - 5	कोई वित्तीय अपेक्षाएं नहीं	प्राधिकरण द्वारा समय-समय पर निर्धारित अधिप्रमाणन कार्य मापदंडों को पूरा करने वाली अधिप्रमाणन उपयोक्ता एजेंसी(एयूए) अथवा ई-केवाईसी उपयोक्ता एजेंसी।

डॉ. अजय भूषण पाण्डेय, मुख्य कार्यपालक अधिकारी

[विज्ञापन-III/4/असा./238]

NOTIFICATION

New Delhi, the 12th September, 2016

AADHAAR (AUTHENTICATION) REGULATIONS, 2016

(No. 3 of 2016)

No. 13012/64/2016/Legal/UIDAI (No. 3 of 2016).—In exercise of the powers conferred by sub-section (1), and sub-clauses (f) and (w) of sub-section (2) of Section 54 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, the Unique Identification Authority of India hereby makes the following regulations, namely:—

CHAPTER I

PRELIMINARY

1. Short title and commencement.—

- (1) These regulations may be called the Aadhaar (Authentication) Regulations, 2016.
- (2) These regulations shall come into force on the date of their publication in the Official Gazette.

2. Definitions.--

- (1) In these regulations, unless the context otherwise requires,—
 - (a) “Act” means the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016;

- (b) “**Aadhaar number holder**” means an individual who has been issued an Aadhaar number under the Act;
- (c) “**Authentication**” means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;
- (d) “**Authentication facility**” means the facility provided by the Authority for verifying the identity information of an Aadhaar number holder through the process of authentication, by providing a Yes/ No response or e-KYC data, as applicable;
- (e) “**Authentication record**” means the record of the time of authentication and identity of the requesting entity and the response provided by the Authority thereto;
- (f) “**Authentication Service Agency**” or “**ASA**” shall mean an entity providing necessary infrastructure for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility provided by the Authority;
- (g) “**Authentication User Agency**” or “**AUA**” means a requesting entity that uses the Yes/ No authentication facility provided by the Authority;
- (h) “**Authority**” means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Act;
- (i) “**Central Identities Data Repository**” or “**CIDR**” means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;
- (j) “**e-KYC authentication facility**” means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction;
- (k) “**e-KYC data**” means demographic information and photograph of an Aadhaar number holder;
- (l) “**e-KYC User Agency**” or “**KUA**” shall mean a requesting entity which, in addition to being an AUA, uses e-KYC authentication facility provided by the Authority;
- (m) “**License Key**” is the key generated by a requesting entity as per the process laid down by the Authority
- (n) “**PID Block**” means the Personal Identity Data element which includes necessary demographic and/or biometric and/or OTP collected from the Aadhaar number holder during authentication.
- (o) “**Requesting entity**” means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the Central Identities Data Repository for authentication; and
- (p) “**Yes/No authentication facility**” means a type of authentication facility in which the identity information and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is then matched against the data available in the CIDR, and the Authority responds with a digitally signed response containing “Yes” or “No”, along with other technical details related to the authentication transaction, but no identity information.
- (2) Words and expressions used and not defined in these regulations shall have the meaning assigned thereto under the Act or under the rules or regulations made there under or under the Information Technology Act, 2000.

CHAPTER II**AADHAAR AUTHENTICATION FRAMEWORK****3. Types of Authentication.—**

There shall be two types of authentication facilities provided by the Authority, namely—

- (i) **Yes/No authentication facility, which may be carried out using any of the modes specified in regulation 4(2); and**
- (ii) **e-KYC authentication facility, which may be carried out only using OTP and/ or biometric authentication modes as specified in regulation 4(2).**

4. Modes of Authentication. —

- (1) An authentication request shall be entertained by the Authority only upon a request sent by a requesting entity electronically in accordance with these regulations and conforming to the specifications laid down by the Authority.
- (2) Authentication may be carried out through the following modes:
 - (a) **Demographic authentication:** The Aadhaar number and demographic information of the Aadhaar number holder obtained from the Aadhaar number holder is matched with the demographic information of the Aadhaar number holder in the CIDR.
 - (b) **One-time pin based authentication:** A One Time Pin (OTP), with limited time validity, is sent to the mobile number and/ or e-mail address of the Aadhaar number holder registered with the Authority, or generated by other appropriate means. The Aadhaar number holder shall provide this OTP along with his Aadhaar number during authentication and the same shall be matched with the OTP generated by the Authority.
 - (c) **Biometric-based authentication:** The Aadhaar number and biometric information submitted by an Aadhaar number holder are matched with the biometric information of the said Aadhaar number holder stored in the CIDR. This may be fingerprints-based or iris-based authentication or other biometric modalities based on biometric information stored in the CIDR.
 - (d) **Multi-factor authentication:** A combination of two or more of the above modes may be used for authentication.
- (3) A requesting entity may choose suitable mode(s) of authentication from the modes specified in sub-regulation (2) for a particular service or business function as per its requirement, including multiple factor authentication for enhancing security. For the avoidance of doubt, it is clarified that e-KYC authentication shall only be carried out using OTP and/ or biometric authentication.

5. Information to the Aadhaar number holder.—

- (1) **At the time of authentication,** a requesting entity shall inform the Aadhaar number holder of the following details:—
 - (a) the nature of information that will be shared by the Authority upon authentication;
 - (b) the uses to which the information received during authentication may be put; and
 - (c) alternatives to submission of identity information.
- (2) A requesting entity shall ensure that the information referred to in sub-regulation (1) above is provided to the Aadhaar number holder in local language as well.

6. Consent of the Aadhaar number holder.—

- (1) After communicating the information in accordance with regulation 5, a requesting entity shall obtain the consent of the Aadhaar number holder for the authentication.
- (2) A requesting entity shall obtain the consent referred to in sub-regulation (1) above in physical or preferably in electronic form and maintain logs or records of the consent obtained in the manner and form as may be specified by the Authority for this purpose.

7. Capturing of biometric information by requesting entity.—

- (1) A requesting entity shall capture the biometric information of the Aadhaar number holder using certified biometric devices as per the processes and specifications laid down by the Authority.
- (2) A requesting entity shall necessarily encrypt and secure the biometric data at the time of capture as per the specifications laid down by the Authority.
- (3) For optimum results in capturing of biometric information, a requesting entity shall adopt the processes as may be specified by the Authority from time to time for this purpose.

8. Devices, client applications, etc. used in authentication.—

- (1) All devices and equipment used for authentication shall be certified as required and as per the specifications issued, by the Authority from time to time for this purpose.
- (2) The client applications i.e. software used by requesting entity for the purpose of authentication, shall conform to the standard APIs and specifications laid down by the Authority from time to time for this purpose.

9. Process of sending authentication requests.—

- (1) After collecting the Aadhaar number or any other identifier provided by the requesting entity which is mapped to Aadhaar number and necessary demographic and / or biometric information and/ or OTP from the Aadhaar number holder, the client application shall immediately package and encrypt these input parameters into PID block before any transmission, as per the specifications laid down by the Authority, and shall send it to server of the requesting entity using secure protocols as may be laid down by the Authority for this purpose.
- (2) After validation, the server of a requesting entity shall pass the authentication request to the CIDR, through the server of the Authentication Service Agency as per the specifications laid down by the Authority. The authentication request shall be digitally signed by the requesting entity and/or by the Authentication Service Agency, as per the mutual agreement between them.
- (3) Based on the mode of authentication request, the CIDR shall validate the input parameters against the data stored therein and return a digitally signed Yes or No authentication response, or a digitally signed e-KYC authentication response with encrypted e-KYC data, as the case may be, along with other technical details related to the authentication transaction.
- (4) In all modes of authentication, the Aadhaar number is mandatory and is submitted along with the input parameters specified in sub-regulation (1) above such that authentication is always reduced to a 1:1 match.
- (5) A requesting entity shall ensure that encryption of PID Block takes place at the time of capture on the authentication device as per the processes and specifications laid down by the Authority.

10. Notification of authentication to Aadhaar number holder.—

The Aadhaar number holder may be notified of any biometric and/or OTP based authentication, through the registered email and/or mobile number of the Aadhaar number holder as determined by the Authority, at the time of authentication.

11. Biometric locking.—

- (1) The Authority may enable an Aadhaar number holder to permanently lock his biometrics and temporarily unlock it when needed for biometric authentication.
- (2) All biometric authentication against any such locked biometric records shall fail with a “No” answer with an appropriate response code.
- (3) An Aadhaar number holder shall be allowed to temporarily unlock his biometrics for authentication, and such temporary unlocking shall not continue beyond the time period specified by the Authority or till completion of the authentication transaction, whichever is earlier.
- (4) The Authority may make provisions for Aadhaar number holders to remove such permanent locks at any point in a secure manner.

CHAPTER III**APPOINTMENT OF REQUESTING ENTITIES AND AUTHENTICATION SERVICE AGENCIES****12. Appointment of Requesting Entities and Authentication Service Agencies.—**

- (1) Agencies seeking to become requesting entities to use the authentication facility provided by the Authority shall apply for appointment as requesting entities in accordance with the procedure as may be specified by the Authority for this purpose. Only those entities that fulfill the criteria laid down in Schedule A are eligible to apply. The Authority may by order, amend Schedule A from time to time so as to modify the eligibility criteria.
- (2) Entities seeking appointment as Authentication Service Agencies shall apply for appointment to the Authority in accordance with the procedure as may be specified by the Authority for this purpose. Only those entities that fulfill the criteria laid down in Schedule B are eligible to apply. The Authority may by order, amend Schedule B from time to time so as to modify the eligibility criteria.
- (3) The Authority may require the applicant to furnish further information or clarifications, regarding matters relevant to the activity of such a requesting entity or Authentication Service Agencies, as the case may be, which may otherwise be considered necessary by the Authority, to consider and dispose of the application.
- (4) The applicant shall furnish such information and clarification to the satisfaction of the Authority, within the time as may be specified in this regard by the Authority.
- (5) While considering the application, the information furnished by the applicant and its eligibility, the Authority may verify the information through physical verification of documents, infrastructure, and technological support which the applicant is required to have.
- (6) After verification of the application, documents, information furnished by the applicant and its eligibility, the Authority may:
 - a. approve the application for requesting entity or Authentication Service Agency, as the case may be; and
 - b. enter into appropriate agreements with the entity or agency incorporating the terms and conditions for use by requesting entities of the Authority's authentication facility, or provision of services by ASAs, including damages and disincentives for non-performance of obligations.
- (7) The Authority may from time to time, determine the fees and charges payable by entities during their appointment, including application fees, annual subscription fees and fees for individual authentication transactions.

13. Procedure where application for appointment is not approved. —

- (1) In the event an application for appointment of requesting entity or Authentication Service Agency, as the case may be, does not satisfy the requirements specified by the Authority, the Authority may reject the application.
- (2) The decision of the Authority to reject the application shall be communicated to the applicant in writing within thirty days of such decision, stating therein the grounds on which the application has been rejected.
- (3) Any applicant, aggrieved by the decision of the Authority, may apply to the Authority, within a period of thirty days from the date of receipt of such intimation for reconsideration of its decision.
- (4) The Authority shall reconsider an application made by the applicant and communicate its decision thereon, as soon as possible in writing.

14. Roles and responsibilities of requesting entities. —

- (1) A requesting entity shall have the following functions and obligations:—
 - (a) establish and maintain necessary authentication related operations, including own systems, processes, infrastructure, technology, security, etc., which may be necessary for performing authentication;

- (b) establish network connectivity with the CIDR, through an ASA duly approved by the Authority, for sending authentication requests;
- (c) ensure that the network connectivity between authentication devices and the CIDR, used for sending authentication requests is in compliance with the standards and specifications laid down by the Authority for this purpose;
- (d) employ only those devices, equipment, or software, which are duly registered with or approved or certified by the Authority or agency specified by the Authority for this purpose as necessary, and are in accordance with the standards and specifications laid down by the Authority for this purpose;
- (e) monitor the operations of its devices and equipment, on a periodic basis, for compliance with the terms and conditions, standards, directions, and specifications, issued and communicated by the Authority, in this regard, from time to time,
- (f) ensure that persons employed by it for performing authentication functions, and for maintaining necessary systems, infrastructure and processes, possess requisite qualifications for undertaking such works.
- (g) keep the Authority informed of the ASAs with whom it has entered into agreements;
- (h) ensure that its operations and systems are audited by information systems auditor certified by a recognised body on an annual basis to ensure compliance with the Authority's standards and specifications and the audit report should be shared with the Authority upon request;
- (i) implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication services to Aadhaar number holders;
- (j) in case of any investigation involving authentication related fraud(s) or dispute(s), it shall extend full cooperation to the Authority, or any agency appointed or authorised by it or any other authorised investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resources or information;
- (k) in the event the requesting entity seeks to integrate its Aadhaar authentication system with its local authentication system, such integration shall be carried out in compliance with standards and specifications issued by the Authority from time to time;
- (l) shall inform the Authority of any misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or systems within their network. If the requesting entity is a victim of fraud or identifies a fraud pattern through its fraud analytics system related to Aadhaar authentication, it shall share all necessary details of the fraud with the Authority;
- (m) shall be responsible for the authentication operations and results, even if it sub-contracts parts of its operations to third parties. The requesting entity is also responsible for ensuring that the authentication related operations of such third party entities comply with Authority standards and specifications and that they are regularly audited by approved independent audit agencies;

may agree upon the authentication charges for providing authentication services to its customer, with such customer, and the Authority shall have no say in this respect, for the time being; however, the Authority's right to prescribe a different mechanism in this respect in the future shall be deemed to have been reserved;
- (n) shall, at all times, comply with any contractual terms and all rules, regulations, policies, manuals, procedures, specifications, standards, and directions issued by the Authority, for the purposes of using the authentication facilities provided by the Authority.

15. Use of Yes/ No authentication facility.—

- (1) A requesting entity may use Yes/ No authentication facility provided by the Authority for verifying the identity of an Aadhaar number holder for its own use or on behalf of other agencies.
- (2) A requesting entity may permit any other agency or entity to perform Yes/ No authentication by generating and

sharing a separate license key for every such entity through the portal provided by the Authority to the said requesting entity. For the avoidance of doubt, it is clarified that such sharing of license key is only permissible for performing Yes/ No authentication, and is prohibited in case of e-KYC authentication.

- (3) Such agency or entity:
 - a. shall not further share the license key with any other person or entity for any purpose; and
 - b. shall comply with all obligations relating to personal information of the Aadhaar number holder, data security and other relevant responsibilities that are applicable to requesting entities.
- (4) It shall be the responsibility of the requesting entity to ensure that any entity or agency with which it has shared a license key, complies with the provisions of the Act, regulations, processes, standards, guidelines, specifications and protocols of the Authority that are applicable to the requesting entity.
- (5) The requesting entity shall be jointly and severally liable, along with the entity or agency with which it has shared a license key, for non-compliance with the regulations, processes, standards, guidelines and protocols of the Authority.

16. Use of e-KYC authentication facility.—

- (1) A KUA may use the e-KYC authentication facility provided by the Authority for obtaining the e-KYC data of the Aadhaar number holder for its own purposes.
- (2) A KUA may perform e-KYC authentication on behalf of other agencies, and share the e-KYC data with such agency for a specified purpose, upon obtaining consent from the Aadhaar number holder for such purpose.
- (3) A KUA may store, with consent of the Aadhaar number holder, e-KYC data of an Aadhaar number holder, received upon e-KYC authentication, in encrypted form and subsequently share the e-KYC data with any other agency, for a specified purpose, upon obtaining separate consent for every such sharing from the Aadhaar number holder for that purpose.
- (4) The agency with whom the KUA has shared the e-KYC data of the Aadhaar number holder shall not share it further with any other entity or agency except for completing the transaction for which the Aadhaar number holder has specifically consented to such sharing.
- (5) The Aadhaar number holder may, at any time, revoke consent given to a KUA for storing his e-KYC data or for sharing it with third parties, and upon such revocation, the KUA shall delete the e-KYC data and cease any further sharing.
- (6) In addition to the restriction on further sharing contained in sub-regulation (4), all other obligations relating to the personal information of the Aadhaar number holder, data security and other relevant responsibilities applicable to requesting entities, shall also apply to the agency or entity with whom e-KYC data has been shared in accordance with this regulation 16.
- (7) Upon request, a KUA shall provide a digitally signed electronic copy of the e-KYC data to the Aadhaar number holder, and the Aadhaar number holder may subsequently share the said copy with any agency:

Provided that the agency that is requesting e-KYC data from the Aadhaar number holder shall inform the purpose of doing so and take the consent of the Aadhaar number;

Provided further that the agency with whom the Aadhaar number holder has shared the e-KYC data shall not share it further with any other entity/agency except for completing the transaction for which the Aadhaar number holder specifically consented to such sharing.

- (8) The KUA shall maintain auditable logs of all such transactions where e-KYC data has been shared with other agencies, for a period specified by the Authority.

17. Obligations relating to use of identity information by requesting entity.—

- (1) A requesting entity shall ensure that:
 - (a) the core biometric information collected from the Aadhaar number holder is not stored, shared or

published for any purpose whatsoever, and no copy of the core biometric information is retained with it;

- (b) the core biometric information collected is not transmitted over a network without creation of encrypted PID block which can then be transmitted in accordance with specifications and processes laid down by the Authority.
- (c) the encrypted PID block is not stored, unless it is for buffered authentication where it may be held temporarily on the authentication device for a short period of time, and that the same is deleted after transmission;
- (d) identity information received during authentication is only used for the purpose specified to the Aadhaar number holder at the time of authentication, and shall not be disclosed further, except with the prior consent of the Aadhaar number holder to whom such information relates;
- (e) the identity information of the Aadhaar number holders collected during authentication and any other information generated during the authentication process is kept confidential, secure and protected against access, use and disclosure not permitted under the Act and its regulations;
- (f) the private key used for digitally signing the authentication request and the license keys are kept secure and access controlled; and
- (g) all relevant laws and regulations in relation to data storage and data protection relating to the Aadhaar-based identity information in their systems, that of their agents (if applicable) and with authentication devices, are complied with.

18. Maintenance of logs by requesting entity. —

- (1) A requesting entity shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely:—
 - (a) the Aadhaar number against which authentication is sought;
 - (b) specified parameters of authentication request submitted;
 - (c) specified parameters received as authentication response;
 - (d) the record of disclosure of information to the Aadhaar number holder at the time of authentication; and
 - (e) record of consent of the Aadhaar number holder for authentication,
 but shall not, in any event, retain the PID information.
- (2) The logs of authentication transactions shall be maintained by the requesting entity for a period of 2 (two) years, during which period an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified.
- (3) Upon expiry of the period specified in sub-regulation (2), the logs shall be archived for a period of five years or the number of years as required by the laws or regulations governing the entity, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by a court or required to be retained for any pending disputes.
- (4) The requesting entity shall not share the authentication logs with any person other than the concerned Aadhaar number holder upon his request or for grievance redressal and resolution of disputes or with the Authority for audit purposes. The authentication logs shall not be used for any purpose other than stated in this sub-regulation.
- (5) The requesting entity shall comply with all relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872, for the storage of logs.
- (6) The obligations relating to authentication logs as specified in this regulation shall continue to remain in force despite termination of appointment in accordance with these regulations.

19. Roles, responsibilities and code of conduct of Authentication Service Agencies.—

An Authentication Service Agency shall **have the following functions and obligations:—**

- (a) provide secured connectivity to the CIDR to transmit authentication request from a requesting entity in the manner as may specified by the Authority for this purpose;

- (b) perform basic compliance and completeness checks on the authentication data packet before forwarding it to CIDR;
- (c) on receiving the response from CIDR, transmit the result of the transaction to the requesting entity that has placed the request;
- (d) only engage with the requesting entities approved by the Authority and keep the Authority informed of the list of requesting entities that it serves;
- (e) communicate to the Authority, all relevant information pertaining to any agreement that it may enter into with a requesting entity;
- (f) ensure that the persons employed by it for performing authentication and for maintaining necessary systems, infrastructure, processes, etc., possess requisite qualifications for undertaking such works;
- (g) ensure that its operations are audited by an information systems auditor certified by a recognized body on an annual basis, and provide a certified audit report, to the Authority, confirming its compliance with the policies, processes, procedures, standards, or specifications, issued by the Authority in this regard, from time to time;
- (h) ensure that all infrastructure and operations including systems, processes, devices, software and biometric infrastructure, security, and other related aspects, are in compliance with the standards and specifications as may specified by the Authority for this purpose;
- (i) at all times, comply with directions, specifications, etc. issued by the Authority, in terms of network and other Information Technology infrastructure, processes, procedures, etc.
- (j) comply with all relevant laws and regulations relating, in particular, to data security and data management;
- (k) any value added service that an ASA provides to a requesting entity under a contract shall not form part of the Aadhaar authentication process;
- (l) shall be responsible to the Authority for all its authentication related operations, even in the event the ASA sub-contracts parts of its operations to other entities, the responsibility shall remain with the ASA;
- (m) in case of investigations relating to authentication related fraud or dispute, the ASA shall extend full co-operation to the Authority (or their agency) and/or any other authorized investigation agency, including providing access to its premises, records, systems, personnel, infrastructure, any other relevant resource or information and any other relevant aspect of its authentication operations;
- (n) may agree upon the authentication charges for providing services to a requesting entity, with such requesting entity, and the Authority shall have no say in this respect, for the time being; however, the Authority's right to prescribe a different mechanism in this respect in the future shall be deemed to have been reserved;
- (o) shall, at all times, comply with any contractual terms and all rules, regulations, policies, manuals, procedures, specifications, standards, and directions issued by the Authority.

20. Maintenance of logs by Authentication Service Agencies.—

- (1) An Authentication Service Agency shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely:—
 - (a) identity of the requesting entity;
 - (b) parameters of authentication request submitted; and
 - (c) parameters received as authentication response:
 Provided that no Aadhaar number, PID information, device identity related data and e-KYC response data, where applicable shall be retained.
- (2) Authentication logs shall be maintained by the ASA for a period of 2 (two) years, during which period the Authority and/or the requesting entity may require access to such records for grievance redressal, dispute redressal and audit in accordance with the procedure specified in these regulations. The authentication logs shall not be used for any purpose other than stated in this sub-regulation.

- (3) Upon expiry of the period specified in sub-regulation (2), the authentication logs shall be archived for a period of five years, and upon expiry of the said period of five years or the number of years as required by the laws or regulations governing the entity whichever is later, the authentication logs shall be deleted except those logs required to be retained by a court or which are required to be retained for any pending disputes.
- (4) The ASA shall comply with all applicable laws in respect of storage and maintenance of these logs, including the Information Technology Act, 2000.
- (5) The obligations relating to authentication logs as specified in this regulation shall continue to remain in force despite termination of appointment in accordance with these regulations.

21. Audit of requesting entities and Authentication Service Agencies.—

- (1) The Authority may undertake audit of the operations, infrastructure, systems and procedures, of requesting entities, including the agencies or entities with whom they have shared a license key or the entities on whose behalf they have performed authentication, and Authentication Service Agencies, either by itself or through audit agencies appointed by it, to ensure that such entities are acting in compliance with the Act, rules, regulations, policies, procedures, guidelines issued by the Authority.
- (2) The Authority may conduct audits of the operations and systems of the entities referred to in sub-regulation (1), either by itself or through an auditor appointed by the Authority. The frequency, time and manner of such audits shall be as may be notified by the Authority from time to time.
- (3) An entity subject to audit shall provide full co-operation to the Authority or any agency approved and/or appointed by the Authority in the audit process, and provide to the Authority or any agency approved and/or appointed by the Authority, complete access to its procedures, records and information pertaining to services availed from the Authority. The cost of audits shall be borne by the concerned entity.
- (4) On identification of any deficiency by the Authority, the Authority may require the concerned entity to furnish necessary clarifications and/or information as to its activities and may also require such entity either to rectify the deficiencies or take action as specified in these regulations.

22. Data Security. —

- (1) Requesting entities and Authentication Service Agencies shall have their servers used for Aadhaar authentication request formation and routing to CIDR to be located within data centres located in India.
- (2) Authentication Service Agency shall establish dual redundant, secured leased lines or MPLS connectivity with the data centres of the Authority, in accordance with the procedure and security processes as may be specified by the Authority for this purpose.
- (3) Requesting entities shall use appropriate license keys to access the authentication facility provided by the Authority only through an ASA over secure network, as may be specified by the Authority for this purpose.
- (4) Requesting Entities and Authentication Service Agencies shall adhere to all regulations, information security policies, processes, standards, specifications and guidelines issued by the Authority from time to time.

23. Surrender of the access to authentication facility by requesting entity or Authentication Service Agency. —

- (1) A Requesting Entity or ASA, appointed under these regulations, desirous of surrendering the access to the authentication facility granted by Authority, may make a request for such surrender to the Authority.
- (2) While disposing such surrender request under these regulations, the Authority may require the requesting entity or ASA to satisfy the Authority about any matter necessary for smooth discontinuance or termination of services, including—
 - (a) the arrangements made by the requesting entity for maintenance and preservation of authentication logs and other documents in accordance with these regulations and procedures as may be specified by the Authority for this purpose;
 - (b) the arrangements made by the requesting entity for making authentication record available to the respective Aadhaar number holder on such request;
 - (c) records of redressal of grievances, if any;

- (d) settlement of accounts with the Authority, if any;
- (e) in case of surrender by ASAs, the ASA, prior to the surrender of its access, shall ensure that its associated requesting entities are given adequate time to migrate to other ASAs in operation.

24. Agencies appointed before commencement of these regulations. —

- (1) Any Authentication User Agency (AUA) or e-KYC User Agency (KUA), appointed prior to the commencement of these regulations shall be deemed to be a requesting entity, and any Authentication Service Agency (ASA) or e-KYC Service Agency (KSA) shall be deemed to be an Authentication Service Agency, under these regulations, and all the agreements entered into between such agencies and the Unique Identification Authority of India, established *vide* notification of the Government of India in the Planning Commission number A-43011/02/2009-Admin. I, dated the 28th January, 2009 or any officer of such authority shall continue to be in force to the extent not inconsistent with the provisions of the Act, these regulations, and other regulations, policies, processes, procedures, standards and specifications issued by the Authority.
- (2) Notwithstanding anything contained in sub-regulation (1), any deemed requesting entity or Authentication Service Agency referred to in sub-regulation (1) shall be required to comply with the provisions of the Act, these regulations, other regulations framed by the Authority, and the policies, processes, procedures, standards and specifications issued by the Authority.
- (3) In the event any such agency referred to in sub-regulation(1) seeks to discontinue using the authentication facility as specified in these regulations, it may immediately make an application for termination of its credentials and stop its functions forthwith:

Provided that in such cases, no compensation shall be payable to the agency or to the Authority upon such termination.

- (4) On discontinuance under sub-regulation (3), the concerned entity shall be required to comply with the closure requirements listed in regulation 23(2).

25. Liability and action in case of default. —

- (1) Where any requesting entity or an ASA appointed under the Act,
 - (a) fails to comply with any of the processes, procedures, standards, specifications or directions issued by the Authority, from time to time;
 - (b) is in breach of its obligations under the Act and these regulations;
 - (c) uses the Aadhaar authentication facilities for any purpose other than those specified in the application for appointment as requesting entity or ASA,
 - (d) fails to furnish any information required by the Authority for the purpose of these regulations; or
 - (e) fails to cooperate in any inspection or investigation or enquiry or audit conducted by the Authority,

the Authority may, without prejudice to any other action which may be taken under the Act, take such steps to impose disincentives on the requesting entity or an ASA for contravention of the provisions of the Act, rules and regulations there under, including suspension of activities of such entity or agency, or other steps as may be more specifically provided for in the agreement entered into by such entities with the Authority:

Provided that the entity or agency shall be given the opportunity of being heard before the termination of appointment and discontinuance of its operations relating to Aadhaar authentication.

- (2) Any such action referred to in sub-regulation (1) may also be taken against any entity or agency with which an AUA has shared its license key for Yes/ No authentication and any entity with which a KUA has shared e-KYC data.
- (3) Upon termination of appointment by the Authority, the requesting entity or the ASA shall, forthwith, cease to use the Aadhaar name and logo for any purposes, and in any form, whatsoever, and may be required to satisfy the Authority of necessary aspects of closure, including those enumerated in regulation 23(2).

CHAPTER IV**AUTHENTICATION TRANSACTION DATA AND AUTHENTICATION RECORDS****26. Storage and Maintenance of Authentication Transaction Data. —**

- (1) The Authority shall store and maintain authentication transaction data, which shall contain the following information:—
- (a) authentication request data received including PID block;
 - (b) authentication response data sent
 - (c) meta data related to the transaction.
 - (d) any authentication server side configurations as necessary

Provided that the Authority shall not, in any case, store the purpose of authentication.

27. Duration of storage. —

- (1) Authentication transaction data shall be retained by the Authority for a period of 6 months, and thereafter archived for a period of five years.
- (2) Upon expiry of the period of five years specified in sub-regulation (1), the authentication transaction data shall be deleted except when such authentication transaction data are required to be maintained by a court or in connection with any pending dispute.

28. Access by Aadhaar number holder. —

- (1) An Aadhaar number holder shall have the right to access his authentication records subject to conditions laid down and payment of such fees as prescribed by the Authority by making requests to the Authority within the period of retention of such records before they are archived.
- (2) The Authority may provide mechanisms such as online portal or mobile application or designated contact centers for Aadhaar number holders to obtain their digitally signed authentication records within the period of retention of such records before they are archived as specified in these regulations.
- (3) The Authority may provide digitally signed e-KYC data to the Aadhaar number holder through biometric or OTP authentication, subject to payment of such fees and processes as specified by the Authority,
- (4) The authentication records and e-KYC data shall not be shared with any person or entity:
 - (a) other than with the Aadhaar number holder to whom the records or e-KYC data relate in accordance with the verification procedure specified. Aadhaar number holder may share their digitally signed authentication records and e-KYC data with other entities which shall not further share with any other agencies without obtaining consent of the Aadhaar holder every time before such sharing.
 - (b) except in accordance with the Act.

CHAPTER V**MISCELLANEOUS****29. Savings.—**

All procedures, orders, processes, standards, specifications and policies issued and MOUs, agreements or contracts entered by the Unique Identification Authority of India, established *vide* notification of the Government of India in the Planning Commission number A-43011/02/2009-Admin. I, dated the 28th January, 2009 or any officer of such authority, prior to the establishment of the Authority under the Act shall continue to be in force to the extent that they are not inconsistent with the provisions of the Act and regulations framed thereunder.

30. Power to issue clarifications, guidelines and removal of difficulties. —

In order to remove any difficulties or clarify any matter pertaining to application or interpretation of these regulations, the Authority may issue clarifications and guidelines in the form of circulars.

Schedule A**Eligibility criteria for appointment as requesting entities
See Regulation 10 (1)**

1. Entities seeking to use authentication facility provided by the Authority as requesting entities are classified under following categories for appointment as Authentication User Agency (AUA) and/or e-KYC User Agency (KUA), as the case may be:

S.No.	Organisation Category
Category 1	Government Organisation
1.1	A Central/ State Government Ministry/Department and their attached or sub-ordinate offices.
1.2	An undertaking owned and managed by Central / State Government (PSU)
1.3	An Authority constituted under the Central / State Act/Special Purpose Organisation constituted by Central/State govt.
Category 2	Regulated Service Providers
2.1	Regulated / Licensed by RBI – Banks and Payment & Settlement System
2.1.1	Public Sector Banks (PSB)
2.1.2	Private Banks, Foreign Banks Licensed by RBI to operate in India, Payment Banks, Small Finance Banks
2.1.3	Regional Rural Banks
2.1.4	Co-operative Banks 5. State Co-operative Banks 6. District Co-operative Banks 7. Scheduled Urban Cop-operatives Banks 8. Non Scheduled Urban Co-operative Banks
2.1.5	Payment & Settlement System Network 1. Financial market infrastructure 2. Retails payments Organisation 3. Cards payment network 4. ATM networks 5. Pre-paid payment instruments 6. White label ATM operators 7. Instant Money Transfer
2.1.6	Non-Banking Financial Company
2.2	Regulated by IRDA/PFRDA - Financial Institutions
2.3	Regulated by TRAI – Telecom
2.4	Regulated by CCA – Certifying Authority, Digital Locker providers, e-Sign providers
2.5	Regulated by SEBI – KYC Registration Agency (KRA), Depository Participant (DP), Asset Management Company (AMC), Trading Exchanges, Registrar and Transfer Agents
2.6	Regulated by National Housing Bank
Category 3	Other Entities
3.1	3.1.1 Company registered in India under the Companies Act 1956 / The companies Act 2013 (Company under group of companies has to apply individually)
	3.1.2 Partnership registered under the India Partnership Act 1932 or under the Limited Liability Partnership Act, 2008
	3.1.3 Proprietorship firm
	3.1.4 Not-for-profit Organisations (under section 25 under The Companies Act 1956)
	3.1.5 Academic Institutions / Research and Development Organisations

S.No.	Organisation Category
	3.1.6 Societies registered under Indian Societies Registration Act, 1860 or The Indian Trust Act, 1882 or The Companies Act, 2013 (Sec 8) / The Co-operative Societies Act 1912
	3.1.7 Any entity other than above mentioned categories

2. Technical and Financial criteria for entities for appointment as requesting entity are as under:-

Category	Authentication User Agency (AUA)		Additional requirements for eKYC User Agency (KUA)
	Technical Requirements	Financial Requirements	
Category 1	1. Backend infrastructure, such as servers, databases etc. of the entity, required specifically for the purpose of Aadhaar authentication, should be located within the territory of India.	No financial requirement	No additional requirement for KUA
Category 2	<p>2. Entity should have IT Infrastructure owned or outsourced capable of carrying out minimum 1 Lakh Authentication transactions per month.</p> <p>3. Organisation should have a prescribed Data Privacy policy to protect beneficiary privacy.</p> <p>4. Organisation should have adopted data security requirements as per the IT Act 2000.</p>	No financial requirement	No additional requirement for KUA
Category 3	<p>1. Backend infrastructure, such as servers, databases etc. of the entity, required specifically for the purpose of Aadhaar authentication, should be located within the territory of India.</p> <p>2. Entity should have IT Infrastructure owned or outsourced capable of carrying out minimum 1 Lakh Authentication transaction per month.</p> <p>3. Organisation should have a prescribed Data Privacy policy to protect beneficiary privacy.</p> <p>4. Organisation should have adopted Data security requirements as per the IT Act 2000.</p> <p>5. Entity should be in business for minimum of 1 year from date of commencement of Business.</p>	<p>1. Paid up capital of minimum • 1 (one) Crore.</p> <p style="text-align: center;">OR</p> <p>Annual turnover of minimum • 5 (Five) Crore during the last Financial year.</p>	Entity should meet Authentication Transaction Criteria as laid down by the Authority from time to time.

Schedule B

Eligibility criteria of Authentication Service Agencies

See Regulation 10(2)

1. Entities seeking to provide secure access to CIDR to requesting entities for enabling authentication services are classified under following categories for appointment as Authentication Service Agency:

S. No	Organisation Category
Category 1	A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government
Category 2	An Authority constituted under the Central / State Act
Category 3	Any other entity of national importance as determined by the Authority
Category 4	A company registered in India under the Indian Companies Act 1956
Category 5	AUA / KUA

2. Technical and Financial criteria for entities for appointment as Authentication Service Agency are as under:-

Category	Financial Requirement	Technical Requirement
Category 1, 2 and 3	No financial requirements	No technical requirements
Category 4	An annual turnover of at least • 100 crores in last three financial years	A Telecom Service Provider (TSP) including All Unified Licensees (having Access Service Authorization) / Unified Licensees (AS) / Unified Access Services Licensees / Cellular Mobile Telephone Service Licensees operating pan-India fiber optics network and should have a minimum of 100 MPLS Points of Presence (PoP) across all states OR Should be a Network Service Provider (NSP) or System Integrator having pan-India network connectivity for data transmission and should have 100 MPLS PoPs in India,
Category 5	No Financial requirements	Any AUA or KUA meeting authentication transaction criteria as laid down by the Authority from time to time

Dr. AJAY BHUSHAN PANDEY, Chief Executive Officer

[ADVT.-III/4/Exty./238]