



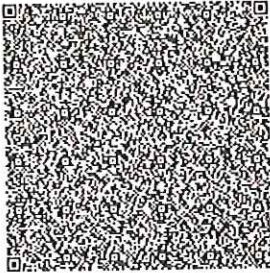
सत्यमेव जयते

INDIA NON JUDICIAL

Government of National Capital Territory of Delhi

e-Stamp

Certificate No.	: IN-DL16703818299002M
Certificate Issued Date	: 30-Sep-2014 11:31 AM
Account Reference	: IMPACC (IV)/ dl815803/ DELHI/ DL-DLH
Unique Doc. Reference	: SUBIN-DL81580330222100986787M
Purchased by	: CSC e Governance Services India Limited
Description of Document	: Article 5 General Agreement
Property Description	: Not Applicable
Consideration Price (Rs.)	: 0 (Zero)
First Party	: CSC e Governance Services India Limited
Second Party	: NIELIT
Stamp Duty Paid By	: CSC e Governance Services India Limited
Stamp Duty Amount(Rs.)	: 100 (One Hundred only)



Please write or type below this line

Ashtu



Statutory Alert:

1. The authenticity of this Stamp Certificate should be verified at "www.shcilestamp.com". Any discrepancy in the details on this Certificate and as available on the website renders it invalid.
2. The onus of checking the legitimacy is on the users of the certificate.
3. In case of any discrepancy please inform the Competent Authority.

**ASA (AUTHENTICATION SERVICE AGENCY) – AUA (AUTHENTICATION
USER AGENCY) AGREEMENT**

This ASA (Authentication Service Agency) – AUA (Authentication User Agency) Agreement (“Agreement”) is made at Delhi on this 1st day of October, 2014, by and between:

1. **CSC e-Governance Services India Limited**, a Company incorporated under the Companies Act 1956 having its registered Office at Electronics Niketan, 4th Floor, DIT, Programme Management Unit, 6, CGO Complex, Lodhi Road, New Delhi-110003 (hereinafter referred to as "**ASA/CSC SPV, wherever applicable**" which expression shall mean and includes its successors, and permitted assigns) represented through its authorised person as the party of the FIRST PART


And

2. **National Institute of Electronics and Information Technology (NIELIT)**, having its registered office at Electronics Niketan, 6, CGO Complex, New Delhi – 110003 (hereinafter referred to as “Authentication User Agency /**AUA**” , which expression shall unless repugnant to the context or meaning thereof, include its successors and permitted assigns), OF THE SECOND PART.

WHEREAS:

CSC SPV has been authorized as Authentication Service Agency by UIDAI, which has been set up with the mandate of issuing “Aadhaar Numbers” to the residents of India, based on their biometric and demographic information. CSC SPV has been authorized as Authentication Service Agency by UIDAI to provide i) UIDAI-compliant secured network connectivity for Aadhaar Authentication Services and to transmit AUAs’ authentication requests to Central Identity Data Repository {CIDR} and ii) e-KYC Services to Authentication User Agencies.




डॉ. अश्विनी कुमार शर्मा / DR. ASHWINI KUMAR SHARMA
प्रबंध निदेशक / Managing Director
राष्ट्रीय इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स निकेतन, 6, सीजीओ कॉम्प्लेक्स, नई दिल्ली-3
Electronics Niketan, 6, CGO Complex, New Delhi-3

The Authentication User Agency is desirous of using the Aadhaar Authentication Services and e- KYC Services provided by UIDAI, through CSC SPV , so as to provide Aadhaar Enabled Services to its beneficiaries, clients and customers and has approached UIDAI, by way of an application, for appointment as an Authentication User Agency.

- B. National Institute of Electronics & Information Technology (NIELIT) has since been approved as Authentication User Agency by UIDAI.
- C. The Authentication User Agency is aware of, and understands, the fact that the Aadhaar Authentication Services provided by CSC SPV, is subject to limitations posed by technology, and CSC SPV does not represent and warrant the same to be defect free.
- D. The Authentication User Agency is aware of, and understands that the Aadhaar Authentication Services are provided on an 'as is' basis, without any express or implied warranties in respect thereof, and CSC SPV does not assume any responsibility or liability for any damage, whether direct, indirect, incidental or consequential, arising as a result of the use of the Aadhaar Authentication Services.
- E. CSC -SPV has agreed (i) to provide UIDAI-compliant secured network connectivity to Authentication User Agency for Aadhaar Authentication Services and to transmit AUAs' authentication requests to Central Identity Data Repository {CIDR} and (ii) e- KYC Services to AUA.

NOW THEREFORE, in consideration of the mutual covenants and promises set forth herein and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby covenant and agree and this Agreement witnesses as follows:




श्री. अश्विनी कुमार शर्मा DR. ASHWINI KUMAR SHARMA
प्रबंध निदेशक / Managing Director
राष्ट्रीय इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स बिल्डिंग, 6, सीजीओ कॉम्प्लेक्स, नई दिल्ली-3
Electronics Bldg, 6, CGO Complex, New Delhi-3

DEFINITIONS & INTERPRETATION

“Aadhaar Authentication Services” shall mean the authentication services provided by UIDAI and used by Authentication User Agency where the personal identity information of / data of an Aadhaar- holder (who is a beneficiary, customer, employee or associate of the Authentication User Agency) is matched with their personal identity information / data that is stored in the UIDAI's Central Identity Data Repository in order to provide Aadhaar enabled services to such Aadhaar holder. The Authentication User Agency shall avail Aadhaar authentication service by establishing a connection with UIDAI's Central Identity Data Repository, through an Authentication Service Agency. The Aadhaar authentication services shall be provided in the manner and as per terms and conditions specified in Annexure I.

As per RBI e-KYC: Know Your Customer (KYC) Norms /Anti-Money Laundering (AML) Standards/ Combating of Financing of Terrorism (CFT)/Obligation of PSOs under Prevention of Money Laundering Act (PMLA), 2002 – e-KYC Service of UIDAI – Recognizing on-line Aadhaar authentication (electronic verification process) to be accepted as an 'Officially Valid Document' under PML Rules

“Aadhaar Enabled Services” shall mean services provided by an Authentication User Agency to Aadhaar Holder, using the Aadhaar Authentication Services of UIDAI.

“Aadhaar Holder” shall mean an individual who holds an Aadhaar Number.

“Aadhaar Number” shall mean the unique identification number issued to resident by UIDAI.

“Agreement” shall mean this agreement executed between the Parties, alongwith its schedules, annexure and exhibits, if any, and all




श्री. अश्विनी कुमार शर्मा, ASHWINI KUMAR SHARMA
प्रबंध निदेशक / Managing Director
राष्ट्रीय इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स बिल्डिंग, संजीव कामटेल संत भवन-3
Electronics Bldg, Sanjeev Kamteel Sant Bhawan-3

instruments supplemental to or amending, modifying or confirming this agreement in accordance with the provisions of this agreement, if any, in each case as they may be supplemented or amended from time to time.

"Authentication Device" shall mean a terminal or device from where the Authentication User Agency carries out its service/business functions and interacts with Aadhaar Holders, by seeking authentication of Aadhaar Holders identity to enable the Authentication User Agency's business function.

"Authentication Service Agency" shall mean

- a) an entity providing compliant secured network connectivity to the UIDAI and the Authentication User Agency for enabling Aadhaar Authentication Services as separate agreements entered into between the entity and UIDAI and Authentication User Agency respectively.
- b) an entity which is eligible to provide access to the e- KYC service through their network.

"Biometric Information" shall mean ten finger prints and iris image, captured by UIDAI, as a part of the enrolment process for issuance of Aadhaar Number.

"Business Day" shall mean any day other than a Saturday, Sunday or official public holiday in India.

"Confidential Information" shall mean any information which is considered confidential in terms of Clause 6 of this Agreement and shall include, but not limited to, information such as Aadhaar Number, name, address, age, date of birth, relationships and other demographic information, as also, biometric information such as finger print and iris scan of a resident.

"e-KYC Service" shall mean the transfer of demographic data (such as



Name, Address, Date of Birth, Gender, Mobile number, Email address, etc.) and photograph collected by UIDAI in the form of a digitally signed XML document to an Authentication User Agency, through an Authentication Service Agency, based on resident authorization received by UIDAI in the form of successful biometric or OTP-based Aadhaar Authentication.

"Law(s)" shall mean all applicable laws, by-laws, rules, regulations, orders, ordinances, protocols, codes, guidelines, policies, notices, directions, judgments, decrees or other requirements or official directive of any governmental authority or person acting under the authority of any governmental authority, whether in effect or which may come into effect in the future.

"OTP" shall mean one time password sent to the Aadhaar holder's cell phone for the purpose of authentication.

"Party" refers individually to Authentication Service Agency and the Authentication User Agency and "Parties" refer collectively to Authentication Service Agency and Authentication User Agency.

"Personal Identity Data (PID)" refers to Aadhaar-based Personal Identity Data / Information including biometric and demographic information as well as the OTP used for Authentication

"Standards" shall mean the standards issued by UIDAI with regard to matters covered by this Agreement, and sole right of interpretation whereof shall rest with UIDAI at all times.

"Sub-AUA" shall mean an entity appointed by the Authentication User Agency under this agreement to access Aadhaar authentication services through the Authentication User Agency.

"Term" shall mean the duration specified in Clause 7.

"Third Party" shall mean any party who is not a Party.



1. TERMS AND CONDITIONS OF APPOINTMENT OF AUTHENTICATION USER AGENCY

1.1 CSC SPV has granted the Authentication User Agency a non-exclusive and revocable right to use Aadhaar Authentication Services, for providing Aadhaar Enabled Services to Aadhaar Holder(s), in the manner set out in this Agreement. The Authentication User Agency understands and agrees that it shall be responsible to CSC SPV for all its Aadhaar authentication related aspects, covered by this Agreement, and in the event the Authentication User Agency outsources part(s) of its operations to other entities, the ultimate responsibility for the results of Aadhaar authentication related operations lies with the Authentication User Agency, and the Authentication User Agency shall ensure that the entity to which it has outsourced its operations is audited annually by information systems auditor certified by a recognized body. The Authentication User Agency also understands and agrees that it shall be responsible to UIDAI for all the Aadhaar authentication related aspects for all authentication requests which it transmits to the CIDR on behalf of Sub AUAs appointed by it. All the obligations of the Authentication User Agency under this agreement shall be equally applicable to the Sub AUAs. The Authentication User Agency understands that the Aadhaar Authentication Service and e-KYC services may be discontinued by CSC SPV by giving a notice period of atleast 06(Six) months or by obtaining consent from Authentication User Agency before discontinuing the services.

1.2. It is hereby mutually agreed between the Parties that the rights and obligations of the Authentication User Agency, under this Agreement, are non-transferable and non-assignable whether by sale, merger, or by operation of law, except with the express written consent of CSC SPV.



Page 6 of 25


श्री. अश्विनी कुमार शर्मा DR. ASHWINI KUMAR SHARMA
प्रबंध निदेशक / Managing Director
राष्ट्रीय इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स बिल्डिंग, 6, सी.बी. आर. मार्ग, दिल्ली-110068
Electronics Bldg, 6, C.B.I. Road, New Delhi-110068

- 1.3. The Authentication User Agency hereby unequivocally agrees that it shall use the Aadhaar Authentication Services and e- KYC Services, for providing Aadhaar Enabled Services to Aadhaar Holder(s), solely for the purposes set out in Annexure -II to this Agreement, and for no other purposes. In the event, the Authentication User Agency is desirous of using Aadhaar Authentication Services and/or e- KYC service, for new and additional services/business functions without compromising or violating requirements specified by UIDAI with regard to network specifications, security etc., from time to time, it shall obtain permission from CSC SPV in this regard.
- 1.4. It is hereby expressly agreed between the parties that in cases where the Authentication User Agency or its Sub AUA forwards an authentication request to the Central Identity Data Repository, through CSC SPV, and in the event of an Aadhaar authentication failure for whatever reasons, the Authentication User Agency may invoke other means of Identity authentication for providing service to the Aadhaar Holder, and the Authentication User Agency or its Sub AUA shall bear full responsibility for any decision taken in this regard and CSC SPV shall have no role in this regard.
- 1.5. It is hereby clearly understood by the Parties that CSC SPV shall have no responsibility or liability in relation to failures that may take place during the Aadhaar e-KYC process.
- 1.6. The Authentication User Agency hereby unequivocally agrees that all backend infrastructure, such as servers, databases etc., required specifically for the purpose of Aadhaar authentication and / or e- KYC service shall be based in the territory of India.
- 1.7. The Authentication User Agency hereby unequivocally agrees that Aadhaar Authentication Services shall be used by it only for providing Aadhaar Enabled Services to Aadhaar Holder(s) and the Aadhaar Authentication Services shall not, in any manner, whether direct or



डॉ. अश्विनी कुमार शर्मा, ASHWINI KUMAR SHARMA
प्रबंध निदेशक / Managing Director
राष्ट्रीय इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स भिखेतन, 6, सी.बी. ई. कॉम्प्लेक्स, नई दिल्ली-3
Electronics Bhiketan, 6, C.B.I. Complex New Delhi-3

indirect, be used for purposes that are anti-government or anti-State or discriminatory or related to money laundering or in contravention of any laws applicable in India.

2. OBLIGATIONS OF ASA

2.1. CSC SPV is empanelled by UIDAI to provide UIDAI-compliant secured network connectivity as a service to Authentication User Agencies and shall transmit AUAs' authentication requests to CIDR.

2.2. CSC SPV shall forward to CIDR only complete authentication requests and incomplete authentication requests shall be returned with appropriate error message.

2.3. CSC SPV shall :-

- a. Provide e-KYC data to the Authentication User Agency upon authorization of the e-KYC request by an Aadhaar Holder, in the form of successful biometric or OTP-based Aadhaar authentication
- b. Provide the e-KYC data in a manner conformant to the standards and processes described in the Demographic Data Standards and Verification Procedure (DDSV) Committee Report;
- c. Provide e-KYC data conforming to Section 3 (Authentication of electronic Records), Section 4 (Legal recognition of electronic records), Section 5 (Legal recognition of digital signatures) and Section 6 (Use of electronic records and digital signatures in Government and its agencies) of the Information Technology Act, 2000;
- d. Determine and prescribe Standards and specifications for transmission of Aadhaar Identity Data for the purposes of Aadhaar e-KYC services;
- e. Determine and prescribe standards to ensure the confidentiality, privacy and security of e-KYC data.



3. OBLIGATIONS OF THE AUTHENTICATION USER AGENCY (AUA)

- 3.1. The Authentication User Agency shall, for every service/business function for which it is desirous of using Aadhaar Authentication Services, choose suitable authentication type from Aadhaar Authentication package Framework provided by CSC SPV from time to time, which indicates the identity credentials/PID to be sought from the Aadhaar Holder, who is seeking to access the specific service/business function(s).
- 3.2. The Authentication User Agency shall obtain consent from the Aadhaar holder, for using the Aadhaar number and Biometric information for providing the Aadhaar Authentication Service. For taking consent of Aadhaar Holder, the Authentication User Agency would provide a check box for self declaration on the Web Form while capturing the Aadhaar Number of the candidate.
- 3.3. The Authentication User Agency hereby unequivocally agrees that it shall, establish network connectivity, through CSC SPV with the Central Identities Data Repository, established by UIDAI that contains all Aadhaar Identity Data, in compliance with all the specifications and standards prescribed by UIDAI, from time to time. The Authentication User Agency assumes complete responsibility with regard to its network connectivity with CSC SPV.
- 3.4. The Authentication User Agency shall establish and maintain necessary authentication related operations, including their own systems, processes, infrastructure, technology, security, etc., which may be necessary for providing Aadhaar Enabled Services, in compliance with standards and specifications, issued by UIDAI from time to time.
- 3.5. The Authentication User Agency shall ensure that the network connectivity between authentication devices and the Central Identities Data Repository, used for sending their authentication requests is in



डॉ. अश्विनी कुमार शर्मा
DR. ASHWINI KUMAR SHARMA
प्रमुख, निदेशक (Managing Director)
राष्ट्रीय इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स भिक्तेरा, 6, रेलवे कालोनी, कोलकाता-700 092
Electronics Bhiketa, 6, R.E. Colony, Kolkata-700 092

compliance with the standards and specifications issued by UIDAI from time to time. The Authentication User Agency shall build and maintain the connectivity between authentication devices and CSC SPVs systems either by itself, or by outsourcing it to a service provider. The Authentication User Agency shall work with CSC SPV in ensuring the compliance of the connectivity between CSC SPV and Central Identities Data Repository.

3.6. The Authentication User Agency shall only employ the Authentication Devices and associated application components (such as sensor and extractor pairs for fingerprint and iris scanners) which are duly registered with/ approved/ certified by UIDAI or an agency appointed by UIDAI for this purpose. The Authentication User Agency understands the authentication type to be employed by it in providing Aadhaar Enabled Services and shall employ the Authentication Devices which confirm to the authentication type adopted by the Authentication User Agency.

3.7. The Authentication User Agency shall install necessary Authentication Devices and other Information Technology devices along with device installation and maintenance kits, and the devices shall comply with specifications and standards prescribed by UIDAI from time to time. The Authentication User Agency shall ensure that the applications driving the authentication devices are duly registered with/ approved/ certified by UIDAI. The Authentication User Agency assumes complete responsibility for ensuring that the processes, procedures, systems and infrastructure at Authentication Device are in compliance with standards and specifications issued by UIDAI from time to time. It is hereby expressly agreed between the Parties that in the event Authentication User Agency's federated authentication system includes Aadhaar authentication as well as the Authentication User Agency's local authentication system, the Authentication User Agency shall integrate their authentication systems with Aadhaar



authentication system in compliance with standards and specifications issued by UIDAI from time to time.

- 3.8. The Authentication User Agency shall keep CSC SPV informed of the Sub AUAs with whom they have entered into agreements and shall duly register them in the manner prescribed by UIDAI from time to time. The AUA shall issue a Sub AUA code to identify each Sub AUA and shall include the Sub AUA code in all authentication requests originating from that Sub AUA which it forwards to CIDR for authentication. The AUA shall keep the CSC SPV informed of all Sub AUA codes that it issues. The Authentication User Agency shall ensure that the Sub AUAs comply with standards and protocols laid out by UIDAI from time to time. The Authentication User Agency understands that it shall be responsible for all authentication requests originating from the Sub AUA and routed through the Authentication User Agency
- 3.9. The Authentication User Agency shall ensure that the persons employed by it for providing Aadhaar Enabled Services and for maintaining necessary systems, infrastructure, processes, etc. in this regard, possess requisite qualifications for undertaking such works. The Authentication User Agency shall be responsible for ensuring that, in case Authentication Devices are operated by its own or its agents personnel, such personnel are suitably and adequately trained to conduct Aadhaar Enabled Services, in compliance with specifications and standards prescribed by UIDAI from time to time.
- 3.10. The Authentication User Agency shall, at all times, comply with standards, directions, specifications, etc. issued by UIDAI, in terms of network and other Information Technology infrastructure, processes, procedures, etc. for the purposes of availing Authentication services provided by UIDAI. The Authentication User Agency shall be further responsible, at all times, for compliance with specification issued by UIDAI, from time to time, with respect to all authentication related



aspects. In the event the Authentication User Agency outsources part(s) of its operations to other entities, the ultimate responsibility for the results of authentication related operations shall lie with the Authentication User Agency.

3.11. The Authentication User Agency shall, at all times, comply with the provisions contained in the Information Technology Act, 2000 and the statutory rules framed there under, from time to time, in so far the same has application to its operations in accordance with this Agreement, and also with all other Laws rules and regulations, whether already in force or which may be enacted anytime in the future, pertaining to data security and management, data storage, sharing and data protection, as also with the National Identification Authority of India Bill, as and when the same is enacted into a law and comes into force, and shall ensure the same level of compliance by its Authentication Device.

3.12. The Authentication User Agency shall ensure that its operations and systems in terms of this Agreement are audited by information systems auditor certified by a recognized body on an annual basis to ensure compliance with UIDAI standards and specifications and the audit report should be shared with CSC SPV upon request.

3.13. In addition to the above, CSC SPV may choose to, in its sole discretion, audit the AUA's operations and systems in terms of this Agreement by itself or through an auditor appointed for this purpose, and the continuation of operations as the Authentication User Agency shall, at all times, be dependent upon the said audit confirming the compliance by the Authentication User Agency of the terms and conditions contained in this Agreement, and any failure in compliance of the same, if confirmed in the audit, may entail fine and/or penalties and termination of access to Aadhaar Authentication Services. The Authentication User Agency unequivocally agrees to provide full co-operation to CSC SPV or any agency approved and/or



appointed by CSC SPV in the audit process, and to provide to CSC SPV or any agency approved and/or appointed by CSC SPV, complete access to its premises, procedures, records, personnel, operations and systems, infrastructure, security, etc.

3.14. The Authentication User Agency shall monitor the operations of its Authentication Device, on a periodic basis, for compliance with the terms and conditions contained in this Agreement or with standards, directions, specifications, etc. issued and communicated by UIDAI/CSC SPV, in this regard, from time to time.

3.15. The Authentication User Agency shall maintain logs of all authentication transactions processed by it, capturing the complete details of the authentication transaction, such as the Aadhaar number against which authentication is sought, authentication package, date and timestamp, etc. as prescribed by UIDAI from time to time but shall not, in any event, capture the PID information and shall retain the same only for a duration, specified by UIDAI from time to time. The Authentication User Agency understands and agrees that the logs maintained by it shall be shared with any individual or entity only on a need-basis, and that the storage of the logs maintained by it shall comply with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

3.16. In case of any investigations around authentication related fraud(s) or dispute (s), the Authentication User Agency shall extend full cooperation to CSC SPV, and/or any agency appointed/authorized by it and/or any other authorized investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resource / information, etc. of or pertaining to its Authentication Device.

3.17. The Authentication User Agency, wherever applicable, shall be



responsible for identifying exception-handling mechanisms in the event of failure of Aadhaar Authentication Services.

- 3.18. The authentication charges, for providing Aadhaar Enabled Services by the Authentication User Agency to its customers, shall be evolve by the Authentication User Agency and CSC SPV shall have no say in this respect, for the time being, however, CSC SPV's right to prescribe a different mechanism in this respect, in the future, shall be deemed to have been reserved.
- 3.19. The Authentication User Agency unequivocally agrees that all devices and applications used by it in running its Aadhaar authentication operations shall be duly certified/ approved by UIDAI or an agency appointed/ approved by UIDAI (as and when UIDAI creates a certification mechanism for certifying Aadhaar enabled application). In case already certified/ approved applications employed by the Authentication User Agency undergo modifications, the Authentication User Agency shall deploy the modified applications only after renewed certification/ approval from UIDAI.
- 3.20. The Authentication User Agency agrees to incorporate and adopt standards, specifications and other terms and conditions as prescribed by UIDAI from time to time, in consultation with the ASA for the purpose of availing Authentication services of UIDAI.
- 3.21. Authentication User Agency hereby agrees to inform CSC SPV of any misuse of Aadhaar data or any compromise of Aadhaar related data or systems within their network.
- 3.22. AUA shall take due care to provide only complete and compliant request for authentication to ASA.
- 3.23. In cases where the authentication devices are operated by AUA's personnel (or personnel of their agents), the AUA is responsible for ensuring that the operating personnel who are adequately trained to



conduct Aadhaar-based authentication in compliance with UIDAI's requirements.

3.24. When an AUA engages with a Sub AUA, it generates a Sub AUA Code to identify the specific Sub AUA. When transmitting authentication requests from a Sub AUA, the AUA always includes the Sub AUA Code so that Aadhaar authentication transaction logs can track the origin of all authentication requests.

3.25. The AUA shall take responsibility on behalf of their Sub AUAs for the standards to be maintained regarding security, infrastructure, processes, devices and other aspects as specified by UIDAI. The AUAs shall take responsibility on behalf of their Sub AUAs for completeness of the authentication requests.


3.26. AUA shall inform CSC SPV of any termination of contracts with Sub AUAs

3.27. AUA shall

a. Maintain logs of all e-KYC transactions processed by it, capturing the complete details of the e-KYC transaction, such as the Aadhaar number against which e-KYC is sought, transaction code, authentication type, requesting AUA, requesting authentication device, date and timestamp, etc. as prescribed by UIDAI from time to time. The Authentication User Agency understands and agrees that the logs maintained by it shall be shared with any individual or entity only on a need-basis, and that the storage of the logs maintained by it shall comply with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

b. Comply, at all times, with all the relevant laws, rules and regulations, including, but not limited to, the Information




श्री. अश्विनी कुमार शर्मा DR. ASHWINI KUMAR SHARMA
प्रबंध निदेशक / Managing Director
राष्ट्रीय इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स विभाग, कोलकाता
Electronics Division, Kolkata

Technology Act, 2000 and the Indian Evidence Act, 1872 in respect of storage of e-KYC data resulting from an e-KYC request contains PID data for the purposes of service delivery.

- c. Ensure that e-KYC data shall not be used by the AUA for purposes other than that for which the resident has explicitly given his/her consent
- d. not share the e-KYC data with any other agency for whatsoever purposes.

4. REPRESENTATIONS AND WARRANTIES

4.1. CSC SPV represents and warrants to the Authentication User Agency that:

- a. CSC SPV has all requisite powers and authority and has taken all actions necessary to execute, deliver, and perform its obligations under this Agreement;
- b. this Agreement has been validly executed by CSC SPV and constitutes a valid agreement binding on CSC SPV and enforceable in accordance with the laws of India;

4.2. The Authentication User Agency represents and warrants to CSC SPV that:

- a. the Authentication User Agency is an entity legally constituted and validly existing under the laws of India;
- b. the Authentication User Agency has all requisite powers and authority and has taken all actions necessary to execute, deliver, and perform its obligations under this Agreement;
- c. this Agreement has been validly executed by the Authentication



User Agency and constitutes a valid agreement binding on the Authentication User Agency and enforceable in accordance with the laws of India.

5. INDEMNITY AND LIMITATION OF LIABILITY

- 5.1. The Authentication User Agency understands that the use of Aadhaar Authentication Services by the Authentication User Agency does not result in incurring of any liability by CSC SPV whatsoever. The Authentication User Agency alone is responsible for the proper and judicious use of the Aadhaar Authentication Services. CSC SPV shall not, in any case, be held responsible for damage and/or harm, direct or indirect, material or immaterial, or of any nature whatsoever, arising from any unavailability of the Aadhaar Authentication Services or its use by the Authentication User Agency.
- 5.2. It is hereby mutually agreed between the Parties that CSC SPV shall not be liable for any unauthorized transactions occurring through the use of Aadhaar Authentication Services and the Authentication User Agency hereby fully indemnifies and holds CSC SPV harmless against any action, suit, proceeding initiated against it or any loss, cost or damage incurred by it as a result thereof.
- 5.3. Without prejudice to generality of the above, the Authentication User Agency shall indemnify and keep CSC SPV harmless and indemnified from and against all claims, liabilities, losses and incurred costs, fines, penalties, expenses, taxes, assessment, punitive damages, fees (including advocate's/ attorney's fee), liabilities (including any investigative, legal and other expenses incurred in connection with, and any amounts paid in settlement of, any pending or threatened legal action or proceeding), judgments, awards, assessments, obligations, damages, etc., which CSC SPV may suffer or incur arising out of, or in connection with the activities of AUA.



6. CONFIDENTIALITY, DATA PROTECTION, SECURITY AND USE OF INFORMATION

6.1. The Authentication User Agency and all its Sub AUAs shall treat all information, which is disclosed to it as a result of the operation of this Agreement, as Confidential Information, and shall maintain the secrecy of all such information and shall not divulge such or part thereof to any other third party. The Authentication User Agency shall use the Confidential Information strictly for the purposes of authentication of the Aadhaar Holder, and for providing Aadhaar Enabled Services, in accordance with this Agreement. The Authentication User Agency shall ensure compliance with all applicable laws and regulations including but not limited to regulations on data protection under the Information Technology Act, 2008 when collecting information from residents for their business purposes.

The Authentication User Agency shall scrutinize the data collected by it, while processing authentication requests, on a periodic basis, and shall preserve such data collected in relation to an authentication request for as period as may be prescribed by UIDAI from time to time.

6.2. The Authentication User Agency is prohibited from storing any PID in their data base or in any storage device of any nature whatsoever including Authentication Device or in any machine, device or instrument of any kind whatsoever, removable storage devices or in physical form, at point in time.

6.3. The Authentication User Agency hereby unequivocally agrees to undertake all measures, including security safeguards, to ensure that the information in the possession or control of the Authentication User Agency, as a result of operation of this Agreement, is secured and protected against any loss or unauthorised access or use or



unauthorised disclosure thereof.

6.4. It is hereby mutually agreed between the parties that CSC SPV assumes no responsibility or liability for any action or inaction, use or misuse of the Confidential Information and other data in the control of the Authentication User Agency. The Authentication User Agency agrees and acknowledges that any loss, damage, liability caused or suffered by the Authentication User Agency due to disclosure of all information of confidential nature shall be borne by Authentication User Agency without transferring any liability or responsibility towards CSC SPV. (NOTE : Acceptability of this be checked at yours.)

6.5. It is hereby mutually agreed that this Clause 6 shall survive the termination of this Agreement.

7. TERM, TERMINATION AND CONSEQUENCES

7.1. Subject to clause 9.3, This Agreement shall be in force for a period of 3 years from the, date of its execution unless renewed in writing, by the Parties upon such terms and conditions as may be mutually agreed.

7.2. CSC SPV shall have the right to terminate this Agreement by giving thirty (90) days notice, in writing, prior to expiry of the Term, without any protest or demur from the Authentication User Agency, in the event of the Authentication User Agency:

- a. fails to comply with the Standards or the decision and directions issued by UIDAI, from time to time, with regard to the interpretation and enforcement of the Standards;
- b. is in breach of its obligations under this Agreement;
- c. uses the Aadhaar Authentication Services for any other purpose than those specified in Annexure-II of this Agreement unless otherwise agreed by ASA;



- d. is in liquidation, or if a receiver has been appointed in respect of the Authentication User Agency or the Authentication User Agency becomes subject to any form of insolvency administration or files for voluntary liquidation.

7.3. The Authentication User Agency shall have no right to compensation for termination of this Agreement by CSC SPV, in pursuance of clauses 7.2 above.

7.4. The agreement may be terminated by AUA without assigning any reason whatsoever and without any compensation by giving 90 days notice to the other Party in writing.

8. FORCE MAJEURE

8.1. The Parties hereto agree that a Force Majeure Event shall mean any unforeseeable act or event that prevents the affected Party from performing its obligations under this Agreement or complying with any conditions required by the other Party under this Agreement and such act or event is beyond the reasonable control and not because of any fault of the affected Party and such Party has been unable to avoid such an act or event by the exercise of prudent foresight and due diligence

8.2. Without prejudice to the foregoing, the Parties hereto agree that the occurrence of any of the events shall also be deemed to be a Force Majeure Event:

- a. War and other hostilities (whether war to be declared or not), invasion, act of foreign enemies, mobilization, requisition or embargo that directly impacts the provision of services under this agreement
- b. Rebellion, revolution, insurrection, military or usurped power and civil war that directly impacts the provision of services under this agreement



- c. Riot, civil commotion, terrorism or disorder that directly impacts the provision of services under this agreement
- d. Pestilence, epidemics, inclement weather causing floods or lightning or cyclone, typhoon or earthquake and which directly impacts the provision of services under this agreement

8.3. **CONSEQUENCES OF FORCE MAJEURE** : Neither Party shall be considered to be in default or breach of its obligations under this Agreement to the extent that the performance of such obligations is prevented due to a Force Majeure Event

9. GENERAL TERMS

- 9.1. Both the parties shall not engage, and shall cause their Personnel as well as and their Personnel not to engage, either directly or indirectly, in any business or professional activities which would conflict with the activities assigned to them under this Agreement.
- 9.2. Both the parties shall keep safe, secure and confidential and protect from unauthorized access, loss or damage all documents, data and information of any nature collected in the course of this agreement.
- 9.3. AUA, shall function as AUA only as long as it is designated so by the UIDAI and the day it ceases to be AUA, all the contracts between the ASA and AUA will stand terminated without any notice.

10. GOVERNING LAW AND DISPUTE RESOLUTION

- 10.1. This Agreement shall, in all respects, be governed by, and construed in accordance with the laws of India and the courts of New Delhi shall have the exclusive jurisdiction.
- 10.2. All or any disputes which arises out of or in relation to this agreement shall at the first instance be resolved through good faith negotiations, which negotiations shall begin promptly after a Party has delivered to the other Party a written request for such



डॉ. बरिनी कुमार शर्मा
प्रबंध निदेशक Managing Director
राष्ट्रीय इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स भिखैन, रोड
Electronics Bikaner, G. C.

consultation.

10.3. If the parties are unable to resolve such dispute within 90 days of the commencement of negotiations as mentioned above, then the same shall be referred to arbitration in accordance with the provisions of the Arbitration and Conciliation Act, 1996.

10.4. The venue for arbitration shall be New Delhi, India and the language used in the arbitral proceedings shall be English.

11. General

11.1. Commercial Terms and conditions for transactions, bandwidth, last mile connectivity etc will be decided mutually before signing ASA-AUA agreements as per the existing CSC SPV tariff structures and discounting policy. Any charge levied by UIDAI for Aadhaar services will be carried forward to AUA.

11.2. Notices

Any notice, direction or other documentation required or remitted to be given hereunder shall be in writing and may only be given by personal delivery, international courier, electronic mail or facsimile (with confirmation received) at the addresses hereinafter set forth: All notices or other communication under or in connection with this agreement be given in writing by registered AD or Speed Post or by telex or by facsimile at the following address (unless otherwise communicated):

If to CSC SPV, at:

Attention : Chief Executive Officer

CSC e-Governance Services India Limited,

Electronics Niketan, 3th Floor,

Department of Electronics and Information Technology

6, CGO Complex, Lodhi Road, New Delhi-110003


Telephone No: 91-9810784845

Fax No : 011 - _____





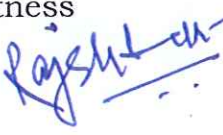

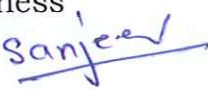

If to _____, at:

Attention:




डॉ. अश्विनी कुमार शर्मा DR. ASHWINI KUMAR SHARMA
प्रबंध निदेशक (Managing Director)
राष्ट्रीय इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स निकेतन, 3^थ फ्लोर
Electronics Niketan, 3rd Floor

Either Party may change individuals designated to receive Notices or addresses or in such an event, notice shall be given to the other Party by means of written Notice of any such change

Signed and delivered on behalf of CSC e-Governance Services India Limited	Signed and delivered on behalf of National Institute of Electronics & Information Technology (NIELIT)
Signature  	Signature  
Name : Dr. Dinesh Kumar Tyagi	Name : Dr. Ashwini Kumar Sharma
Designation : Chief Executive Officer	Designation : Managing Director
Date : 01/10/2014	Date : 01/10/2014
Place : New Delhi	Place : New Delhi
Witness 1.  2.  1/10/14	Witness 1.  2.  1/10/14

ANNEXURE-I

(Aadhaar Authentication Services – operation conditions)

1. The system designed by UIDAI for providing authentication services shall be available across multiple data centres. Other than planned outage the system is expected to run at 98% uptime which translates to about 3 hours of unexpected down time in a week.
2. The CIDR response time is expected to be between 1 to 3 seconds.
3. In order to ensure that the authentication service is friendly to the resident Aadhaar holder it is important that the authentication user agency and sub authentication user agency provide an efficient application to maintain end use latency under 5 seconds. AUAs / Sub - AUAs should consider round trip network latency from their devices to UIDAI data centre and back while planning service roll out on the field. Depending on the choice of network and bandwidth, on the field performance may vary. It is important that for a good resident experience, AUAs / Sub- AUAs should try to keep the full round trip service time to be less than 8-10 seconds on an average.



Handwritten signature


डॉ. अश्विनी कुमार शर्मा/DR. ASHWINI KUMAR SHARMA
प्रबंध निदेशक /Managing Director
राष्ट्रीय इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स निकेतन, 6, सीजीओ कॉम्प्लेक्स, नई दिल्ली-3
Electronics Nিকেতন, 6, CGO Complex, New Delhi-3

Annexure- II

Purposes for which Aadhaar Authentication Services shall be used by the Authentication User Agency

1. Authentication of the candidates at the time of Registration on the Student web portal of NIELIT. Based on the authentication status, the demographic details would be fetched from UIDAI Server at CIDR and would be used during the registration process of a candidate.
2. Candidates would be authenticated at the Examination Hall by providing his/her biometric details like fingerprints along with other information
3. Providing Scholarship to the authenticated candidates under DBT Scheme




डॉ. अश्विनी कुमार शर्मा DR. ASHWINI KUMAR SHARMA
प्रबंध निदेशक (Managing Director)
राष्ट्रीय इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी संस्थान
National Institute of Electronics and Information Technology
इलेक्ट्रॉनिक्स बिल्डिंग-6, सीजीओ कॉम्प्लेक्स, नई दिल्ली-3
Electronics Bldg-6, CGO Complex, New Delhi-3