



COMPENDIUM OF REGULATIONS, CIRCULARS & GUIDELINES FOR

**(AUTHENTICATION USER AGENCY (AUA)/E-KYC USER AGENCY (KUA),
AUTHENTICATION SERVICE AGENCY (ASA) AND BIOMETRIC DEVICE
PROVIDER)**

UNIQUE IDENTIFICATION AUTHORITY OF INDIA

**Government of India (GoI)
3rd Floor, Tower II, Jeevan Bharati Building,
Connaught Circus,
New Delhi - 110001**

Updated as on 6th December 2017

Table of Contents

| Sl. No. | Contents | Date of Issue | Page No. |
|----------|--|---------------|-----------|
| 1 | SECTION -1 : Aadhaar Regulations | | 1 |
| 1.1 | Aadhaar (Authentication) Regulations, 2016 | 14-Sep-16 | 2 |
| 1.2 | Aadhaar (Data Security) Regulations, 2016 | 14-Sep-16 | 23 |
| 1.3 | Aadhaar (Sharing of Information) Regulations, 2016 | 14-Sep-16 | 27 |
| 2 | SECTION -2 : Circulars, Guidelines with IS | | 31 |
| 2.1 | Updated UIDAI Information Security Policy in respect of AUA/KUA for circulation | 25-Sep-17 | 32 |
| 2.2 | Updated UIDAI Information Security Policy in respect of ASA | 25-Sep-17 | 47 |
| 3 | SECTION -3 : Other Circulars, Guidelines etc | | 62 |
| 3.1 | Up-gradation of existing biometric public devices to Registered Devices | 25-Jan-17 | 63 |
| 3.2 | Instruction for providing Authentication or eKYC Services by AUA KUA to Sub-AUA | 28-Feb-17 | 66 |
| 3.3 | Procurement of Registered Devices for Aadhaar Authentication | 28-Feb-17 | 69 |
| 3.4 | Device Certification - Application Form and Undertaking | 16-May-17 | 71 |
| 3.5 | Registered Device Certification of Biometric Devices whose STQC certificate is already expired | 22-May-17 | 76 |
| 3.6 | Circular for Registered Devices (Implementation Timelines) | 24-May-17 | 78 |
| 3.7 | Circular for AUA/KUA and ASA Agreements V 4.0. | 31-May-17 | 82 |
| 3.8 | Delta Certification process of Biometric Devices for Registered Devices. | 9-Jun-17 | 84 |
| 3.9 | Implementation of HSM by AUA/KUA/ASA | 22-Jun-17 | 86 |
| 3.10 | Appointment of Sub-AUA –Application & Undertaking | 6-Jul-17 | 88 |
| 3.11 | Circular for Aadhaar Data Vault | 25-Jul-17 | 93 |
| 3.12 | Whitelisting of Aadhaar based applications developed by AUAs, KUAs and Sub-AUAs. | 27-Sep-17 | 95 |
| 3.13 | Extension for the Migration of Registered Device till 31 st Oct'2017 | 6-Oct-17 | 97 |
| 3.14 | DO's & DONT's FOR AADHAAR USER AGENCIES/DEPARTMENTS | 20-Oct-17 | 98 |
| 3.15 | Sharing of eKYC data with their Sub-AUAs | 27-Nov-17 | 101 |
| 3.16 | Discontinuation of the provision of partial match in Demographic Authentication | 27-Nov-17 | 102 |
| 3.17 | Timeline Extension for Registered Device implementation | 30-Nov-17 | 103 |
| 3.18 | Circular for Discontinuation of Partial Match | 1-Dec-17 | 104 |

SECTION 1

AADHAAR REGULATIONS

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;

AADHAAR (AUTHENTICATION) REGULATION, 2016

- (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

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 <ol style="list-style-type: none"> 1. State Co-operative Banks 2. District Co-operative Banks 3. Scheduled Urban Co-operatives Banks 4. Non Scheduled Urban Co-operative Banks |
| | 2.1.5 Payment & Settlement System Network <ol style="list-style-type: none"> 1. Financial market infrastructure 2. Retail 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 |
| 2.7 | Regulated by DGCA/AAI(AAI Act)- Duly licensed- <ol style="list-style-type: none"> 1. Airport operators having scheduled civil aviation operations, and 2. Scheduled Airline operators. |

| S. No. | Organisation Category |
|-------------------|---|
| 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 |
| | 3.1.6 Societies registered under Indian Societies Registration Act, 1860 or The Indian Trust Act, 1882 or The companies Act, 2013 (Sec 8) / Co-operative Society 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:-

| S. No | 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. 2. Entity should have IT Infrastructure owned or outsourced capable of carrying out minimum 1 Lakh Authentication transactions per month. 3. Organisation should have a prescribed Data Privacy policy to protect beneficiary privacy. 4. Organisation should have adopted data security requirements as per the IT Act 2000 | No financial requirement | No additional requirement for KUA |
| Category 2 | | No financial requirement | No additional requirement for KUA |
| Category 3 | 1. Backend infrastructure, such as servers, | 1. Paid up capital of Minimum ₹1 (one) Crore. | Entity should meet Authentication Transaction Criteria as |

| | | | |
|--|--|---|--|
| | <p>databases etc. of the entity, required specifically for the purpose of Aadhaar authentication, should be located with in 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 Act2000.</p> <p>5. Entity should be in business for minimum of 1 year from date of commencement of Business.</p> | <p>OR</p> <p>Annual turnover of Minimum ₹5 (Five) Crore during the last Financial year.</p> | <p>laid down by the Authority from time to time.</p> |
|--|--|---|--|

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 | Any AUA or KUA meeting authentication transaction criteria as laid down by the Authority from time to time |

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

| Category | Financial Requirement | Technical Requirement |
|---------------------|---|--|
| Category 1, 2 and 3 | No financial requirements | No technical requirements |
| Category 4 | An annual turnover of at least Rs. 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 |

NOTIFICATION

New Delhi, the 12th September, 2016

AADHAAR (DATA SECURITY) REGULATIONS, 2016

(No. 4 of 2016)

No. 13012/64/2016/Legal/UIDAI (No. 4 of 2016).—In exercise of the powers conferred by clause (p) 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 makes the following Regulations, namely: -

1. Short title and commencement. —

- (1) These regulations may be called the Aadhaar (Data Security) 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 (18 of 2016);
- (b) “Authority” means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Act;
- (c) “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;
- (d) “enrolling agency” means an agency appointed by the Authority or a Registrar, as the case may be, for collecting demographic and biometric information of individuals under this Act;
- (e) “information security policy” means the policy specified by the Authority under regulation 3 of these regulations;
- (f) “personnel” means all officers, employees, staff and other individuals employed or engaged by the Authority or by the service providers for discharging any functions under the Act;
- (g) “registrar” means any entity authorised or recognised by the Authority for the purpose of enrolling individuals under this Act;
- (h) “regulations” means the regulations made by the Authority under this Act;
- (i) “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;
- (j) “service provider” includes all entities engaged by the Authority for discharging any function related to its processes.

- (2) All other words and expressions used but not defined in these regulations, but defined in the Act or the Information Technology Act, 2000 and/or the rules and regulations made

AADHAAR (DATA SECURITY) REGULATION, 2016

thereunder shall have the same meaning as respectively assigned to them in such Acts or rules or regulations or any statutory modification or re-enactment thereto, as the case may be.

3. Measures for ensuring information security. —

- (1) The Authority may specify an information security policy setting out *inter alia* the technical and organisational measures to be adopted by the Authority and its personnel, and also security measures to be adopted by agencies, advisors, consultants and other service providers engaged by the Authority, registrar, enrolling agency, requesting entities, and Authentication Service Agencies.
- (2) Such information security policy may provide for:—
 - (a) identifying and maintaining an inventory of assets associated with the information and information processing facilities;
 - (b) implementing controls to prevent and detect any loss, damage, theft or compromise of the assets;
 - (c) allowing only controlled access to confidential information;
 - (d) implementing controls to detect and protect against virus/malwares;
 - (e) a change management process to ensure information security is maintained during changes;
 - (f) a patch management process to protect information systems from vulnerabilities and security risks;
 - (g) a robust monitoring process to identify unusual events and patterns that could impact security and performance of information systems and a proper reporting and mitigation process;
 - (h) encryption of data packets containing biometrics, and enabling decryption only in secured locations;
 - (i) partitioning of CIDR network into zones based on risk and trust;
 - (j) deploying necessary technical controls for protecting CIDR network;
 - (k) service continuity in case of a disaster;
 - (l) monitoring of equipment, systems and networks;
 - (m) measures for fraud prevention and effective remedies in case of fraud;
 - (n) requirement of entering into non-disclosure agreements with the personnel;
 - (o) provisions for audit of internal systems and networks;
 - (p) restrictions on personnel relating to processes, systems and networks.
 - (q) inclusion of security and confidentiality obligations in the agreements or arrangements with the agencies, consultants, advisors or other persons engaged by the Authority.
- (3) The Authority shall monitor compliance with the information security policy and other security requirements through internal audits or through independent agencies.
- (4) The Authority shall designate an officer as Chief Information Security Officer for disseminating and monitoring the information security policy and other security-related programmes and initiatives of the Authority.

4. Security obligations of the personnel —

- (1) The personnel shall comply with the information security policy, and other policies, guidelines, procedures, etc. issued by the Authority from time to time.
- (2) Without prejudice to any action that may be taken under the Act, personnel may be liable to action in accordance with procedures specified by the Authority for this purpose:

Provided that no such action shall be taken without giving the concerned personnel a reasonable opportunity of being heard.

5. Security obligations of service providers, etc. —

The agencies, consultants, advisors and other service providers engaged by the Authority for discharging any function relating to its processes shall:

- (a) ensure compliance with the information security policy specified by the Authority;
- (b) periodically report compliance with the information security policy and contractual requirements, as required by the Authority;
- (c) report promptly to the Authority any security incidents affecting the confidentiality, integrity and availability of information related to the Authority's functions;
- (d) ensure that records related to the Authority shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release;
- (e) ensure confidentiality obligations are maintained during the term and on termination of the agreement;
- (f) ensure that appropriate security and confidentiality obligations are provided for in their agreements with their employees and staff members;
- (g) ensure that the employees having physical access to CIDR data centers and logical access to CIDR data centers undergo necessary background checks;
- (h) define the security perimeters holding sensitive information, and ensure only authorised individuals are allowed access to such areas to prevent any data leakage or misuse; and
- (i) where they are involved in the handling of the biometric data, ensure that they use only those biometric devices which are certified by a certification body as identified by the Authority and ensure that appropriate systems are built to ensure security of the biometric data.

6. Audits and inspection of service providers, etc. —

- (1) All agencies, consultants, advisors and other service providers engaged by the Authority, and ecosystem partners such as registrars, requesting entities, Authentication User Agencies and Authentication Service Agencies shall get their operations audited by an information systems auditor certified by a recognised body under the Information Technology Act, 2000 and furnish certified audit reports to the Authority, upon request or at time periods specified by the Authority.
- (2) In addition to the audits referred to in sub-regulation (1), the Authority may conduct audits of the operations and systems of such entities or persons, either by itself or through an auditor appointed by the Authority.

7. Confidentiality. —

All procedures, orders, processes, standards and protocols related to security, which are designated as confidential by the Authority, shall be treated as confidential by all its personnel and shall be disclosed to the concerned parties only to the extent required for giving effect to the security measures. The nature of information that cannot be shared outside the Authority unless mandated under the Act includes, but not limited to, Information in CIDR, Technology details, Network Architecture, Information security policy and processes, software codes, internal reports, audit and assessment reports, applications details, asset details, contractual agreements, present and future planned infrastructure details, protection services, and capabilities of the system.

8. Savings. —

All procedures, orders, processes, standards 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.

9. Power to issue policies, process documents, etc. —

The Authority may issue policies, processes, standards and other documents, not inconsistent with these regulations, which are required to be specified under these regulations or for which provision is necessary for the purpose of giving effect to these regulations.

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

In order to clarify any matter pertaining to application or interpretation of these regulations, or to remove any difficulties in implementation of these regulations, the Authority shall have the power to issue clarifications and guidelines in the form of circulars which shall have effect of these regulations.

NOTIFICATION

New Delhi, the 12th September, 2016

AADHAAR (SHARING OF INFORMATION) REGULATIONS, 2016

(No. 5 of 2016)

No. 13012/64/2016/Legal/UIDAI (No. 5 of 2016).—In exercise of the powers conferred by sub-section (1), and sub-clause (o) of sub-section (2), of Section 54 read with sub-clause (k) of sub-section (2) of Section 23, and sub-sections

(2) and (4) of Section 29, 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 (Sharing of Information) 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 Letter” means a document for conveying the Aadhaar number to a resident;
 - (c) “Aadhaar number holder” means an individual who has been issued an Aadhaar number under the Act;
 - (d) “Authority” means the Unique Identification Authority of India established under sub-section (1) of section 11;
 - (e) “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.
- (2) All other words and expressions used in these regulations but not defined, and defined in the Act and the rules and other regulations made there under, shall have the meanings respectively assigned to them in the Act or the rules or other regulations, as the case may be.

CHAPTER II**RESTRICTIONS ON SHARING OF IDENTITY INFORMATION****3. Sharing of information by the Authority. —**

- (1) Core biometric information collected by the Authority under the Act shall not be shared with anyone for any reason whatsoever.
- (2) The demographic information and photograph of an individual collected by the Authority under the Act may be shared by the Authority with a requesting entity in response to an authentication request for e-KYC data pertaining to such individual, upon the requesting entity obtaining consent from the Aadhaar number holder for the authentication process, in accordance with the provisions of the Act and the Aadhaar (Authentication) Regulations, 2016.
- (3) The Authority shall share authentication records of the Aadhaar number holder with him in accordance with regulation 28 of the Aadhaar (Authentication) Regulations, 2016.
- (4) The Authority may share demographic information and photograph, and the authentication records of an Aadhaar number holder when required to do so in accordance with Section 33 of the Act.

4. Sharing of information by a requesting entity. —

- (1) Core biometric information collected or captured by a requesting entity from the Aadhaar number holder at the time of authentication shall not be stored except for buffered authentication as specified in the Aadhaar (Authentication) Regulations, 2016, and shall not be shared with anyone for any reason whatsoever.
- (2) The identity information available with a requesting entity:
 - (a) shall not be used by the requesting entity for any purpose other than that specified to the Aadhaar number holder at the time of submitting identity information for authentication; and
 - (b) shall not be disclosed further without the prior consent of the Aadhaar number holder.
- (3) A requesting entity may share the authentication logs of an Aadhaar number holder with the concerned Aadhaar number holder upon his request or for grievance redressal and resolution of disputes or with the Authority for audit purposes, as specified in regulation 18 of the Aadhaar (Authentication) Regulations, 2016.

5. Responsibility of any agency or entity other than requesting entity with respect to Aadhaar number. —

- (1) Any individual, agency or entity which collects Aadhaar number or any document containing the Aadhaar number, shall:
 - (a) collect, store and use the Aadhaar number for a lawful purpose;
 - (b) inform the Aadhaar number holder the following details:—
 - i. the purpose for which the information is collected;
 - ii. whether submission of Aadhaar number or proof of Aadhaar for such purpose is mandatory or voluntary, and if mandatory, the legal provision mandating it;

- iii. alternatives to submission of Aadhaar number or the document containing Aadhaar number, if any;
- (c) obtain consent of the Aadhaar number holder to the collection, storage and use of his Aadhaar number for the specified purposes.
- (2) Such individual, agency or entity shall not use the Aadhaar number for any purpose other than those specified to the Aadhaar number holder at the time of obtaining his consent.
- (3) Such individual, agency or entity shall not share the Aadhaar number with any person without the consent of the Aadhaar number holder.

6. Restrictions on sharing, circulating or publishing of Aadhaar number. —

- (1) The Aadhaar number of an individual shall not be published, displayed or posted publicly by any person or entity or agency.
- (2) Any individual, entity or agency, which is in possession of Aadhaar number(s) of Aadhaar number holders, shall ensure security and confidentiality of the Aadhaar numbers and of any record or database containing the Aadhaar numbers.
- (3) Without prejudice to sub-regulations (1) and (2), no entity, including a requesting entity, which is in possession of the Aadhaar number of an Aadhaar number holder, shall make public any database or record containing the Aadhaar numbers of individuals, unless the Aadhaar numbers have been redacted or blacked out through appropriate means, both in print and electronic form.
- (4) No entity, including a requesting entity, shall require an individual to transmit his Aadhaar number over the Internet unless such transmission is secure and the Aadhaar number is transmitted in encrypted form except where transmission is required for correction of errors or redressal of grievances.
- (5) No entity, including a requesting entity, shall retain Aadhaar numbers or any document or database containing Aadhaar numbers for longer than is necessary for the purpose specified to the Aadhaar number holder at the time of obtaining consent.

7. Liability for contravention of the regulations. —

Without prejudice to any action that may be taken under the Act, any contravention of regulations 3, 4, 5 and 6 of these regulations shall constitute a violation of sub-section (2) of Section 29 of the Act.

8. Redressal of grievances of Aadhaar number holders. —

In the event the identity information of an Aadhaar number holder has been shared or published in a manner contrary to the provisions of the Act or regulations, the Aadhaar number holder may raise queries and grievances in accordance with the regulation 32 of the Aadhaar (Enrolment and Update) Regulations, 2016.

CHAPTER III
MISCELLANEOUS

9. Information dissemination about sharing of Aadhaar numbers. —

The Authority may take necessary measures to educate Aadhaar number holders about the uses of Aadhaar numbers and implications associated with its sharing.

10. Savings. —

All procedures, orders, processes, standards 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.

11. Power to issue clarifications and guidelines. —

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.

SECTION 2

CIRCULARS, GUIDELINES WITH INFORMATION SECURITY (IS)



UIDAI INFORMATION SECURITY POLICY – UIDAI EXTERNAL ECOSYSTEM – AUTHENTICATION USER AGENCY /KYC USER AGENCY

UIDAI

Unique Identification Authority of India

Ministry of Electronics and Information Technology (MeitY),
Govt. of India (GoI), 3rd Floor, Tower II,
Jeevan Bharati Building, Connaught Circus,
New Delhi 110001

Document Control

| S. No. | Type of Information | Document Data |
|--------|----------------------|---|
| 1. | Document Title | UIDAI Information Security Policy –External Ecosystem AUA/KUA |
| 2. | Document Code | UISP-AUA |
| 3. | Date of Release | |
| 4. | Document Superseded | UIDAI Information Security Policy v3.2 |
| 5. | Document Revision No | 3.3 |
| 6. | Document Owner | Shri Ajai Chandra, ADG (Authentication), UIDAI |
| 7. | Document Author(s) | |

Document Approvers

| S. No. | Approver | Approved Through/ Nominee | Comments |
|--------|-------------------------|---------------------------|----------|
| 1. | Shri. A.B. Pandey (CEO) | | |
| | | | |

Document Change Approvals

| Version No. | Revision Date | Nature of Change | Date Approved |
|-------------|---------------|---|---|
| Version 1.1 | 01-Dec-2011 | First version (2011) | December-2011 |
| Version 2.0 | 08-May-2014 | <ul style="list-style-type: none"> Alignment with ISO 27001:2013 requirements Segregation of Control Statements from the Procedures and Guidelines Addition of Information Security Governance Framework Updating of security policies for UIDAI external ecosystem | 27-Oct-14 |
| Version 3.0 | 23-Jan-2015 | <ul style="list-style-type: none"> Revision of Governance framework (ISMS) for stage I ISO27001:2013 | 02-Feb-15 |
| Version 3.1 | 27-Feb-2015 | <ul style="list-style-type: none"> Update of Annexure documents as per stage-2 comments | 24-Apr-15 |
| Version 3.2 | 22-Dec-2015 | <ul style="list-style-type: none"> Creation of separate booklet from existing UIDAI information security policy document for external ecosystem partner for Authentication – AUA and KUA | No. F-11014/06/2014-Tech (Vol-II)/631 Dated 27 th April 2016 |
| Version 3.3 | 28-Feb-2017 | <ul style="list-style-type: none"> Annual review | |

Statement of Confidentiality

This document presents the Information Security Policy of UIDAI for external ecosystem partner AUA/KUA and contains information that is proprietary and confidential to UIDAI. Any use or disclosure in whole or part of this information for any reason without written permission of UIDAI is strictly prohibited.

Feb 2017, UIDAI

Foreword

The UIDAI ecosystem is one of the most complex environments in the world today. The entire backbone of this ecosystem is the residents' identity Information, which is created, processed, transmitted, stored and securely disposed by UIDAI and its ecosystem partners. Hence, it is imperative to define and implement robust controls to safeguard the residents' identity information, and create trust between the residents and the UIDAI ecosystem against the misuse of such information.

UIDAI has defined a set of people, process and technical controls to govern the use of this information, in alignment with industry standards such as ISO 27001. Focus of this document is to protect residents' information and the information infrastructure, build capabilities to prevent and respond to information security threats, eliminate identified vulnerabilities and minimize damage from information security incidents through a combination of institutional structures, people, processes and technology.

This Information Security policy document specifies the scope and the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the Information Security environment/landscape of Unique Identification Authority of India (UIDAI).

Table of Contents

| | |
|---|----------|
| UIDAI Information Security Policy – AUA/KUA | 6 |
| 1. Policy Statement..... | 7 |
| 1.1 Control Objective | 7 |
| 1.2 Scope..... | 7 |
| 2. Information Security Policy for Authentication User Agencies (AUAs)/KYC User Agencies (KUAs)..... | 8 |
| 2.1 Purpose | 8 |
| 2.2 Terms and definitions | 8 |
| 2.3 Policy | 9 |
| 2.4 Human Resources | 10 |
| 2.5 Asset Management | 10 |
| 2.6 Access Control..... | 10 |
| 2.7 Password Policy..... | 11 |
| 2.8 Cryptography | 12 |
| 2.9 Physical and Environmental Security..... | 12 |
| 2.10 Operations Security..... | 13 |
| 2.11 Communications security..... | 14 |
| 2.12 Information Security Incident Management | 15 |
| 2.13 Compliance | 15 |
| 2.14 Change Management..... | 15 |



UIDAI Information Security Policy – AUA/KUA

1. Policy Statement

Security of UIDAI information assets handled by the external ecosystem partners for providing services, is of paramount importance. The confidentiality, integrity and availability of these shall be maintained at all times by these partners by deploying controls commensurate with the asset value.

1.1 Control Objective

UIDAI shall ensure the security of UIDAI information assets handled by AUAs/KUAs:

1. Providing AUAs/KUAs with an approach and directives for deploying security controls for all information assets used by them for providing services;
2. Establishing review mechanism to ensure that the AUAs/KUAs adhere to all provisions of the UIDAI Information Security Policy for AUAs/KUAs

1.2 Scope

The UIDAI Third Party Information Security Policy is applicable to all AUA/KUA that provide services to UIDAI.

1. **Authentication User Agencies (AUA):** Authentication User Agency is an organisation or an entity using AADHAAR authentication as part of its applications to provide services to residents;
2. **KYC User Agencies (KUA):** KYC User Agency is an organisation or an entity using AADHAAR authentication and eKYC services from UIDAI as part of its applications to provide services to residents.

An AUA sends authentication requests to enable its services / business functions. An AUA connects to the CIDR through an ASA (either by becoming ASA on its own or contracting services of an existing ASA). AUA/KUA uses demographic data, and/or biometric data in addition to the resident's UID. They use Aadhaar authentication to provide services such as opening of bank account, LPG connection, etc. to residents. Since the AUAs handle sensitive resident information such as the Biometric information, Aadhaar number, eKYC data etc. of the residents, it becomes imperative to ensure its security.

This Policy is applicable wherever UIDAI information is processed and/or stored by AUA/KUA.

2. Information Security Policy for Authentication User Agencies (AUAs)/KYC User Agencies (KUAs)

2.1 Purpose

This section outlines the Information Security Policy and Information Security Controls applicable to Authentication User Agencies (AUAs) / KYC User Agencies (KUAs).

2.2 Terms and definitions

| S.No. | Terms | Definition |
|-------|--|---|
| 1 | AAS | AADHAAR Authentication Server |
| 2 | ATM | Automatic Teller Machine |
| 3 | API | Application Program Interface |
| 4 | AUA/ASA | Authentication User Agency/Authentication Service Agency |
| 5 | CA | Certifying Authority |
| 6 | CCTV | Closed Circuit Television |
| 7 | CIDR | Central Identities Data Repository |
| 8 | CN | Common Name |
| 9 | CRM | Customer Relationship Management |
| 10 | eKYC | Electronic Know Your User |
| 11 | GRC | Governance, Risk and Compliance |
| 12 | Asset | An asset is anything that has value to the organization. Assets can be classified into the following 5 categories: 1. Paper assets: (Legal documentation, manuals, policies & procedures, organizational documents etc.) 2. Physical assets: (computer equipment, communications, utility equipment, buildings etc.) 3. Software assets: (database information, applications, software code, development tools, operational software etc.) 4. People assets: UIDAI human resources and stakeholders. 5. Service assets: (Logistics, building management systems, communications, utilities etc.) |
| 13 | Information/ Information Asset (IA) | Information that has value to the organization (UIDAI). Including but not limited to Citizen biometric and demographic information, personally identifiable information, employee information, organization information such as CIDR architecture, infrastructure, network details etc. |
| 14 | IDS | Intrusion Detection System |
| 15 | IPS | Intrusion Prevention System |
| 16 | ISO | Information security division |
| 17 | ISO (ISO27001) | International Organisation of Standardization |
| 18 | IT | Information Technology |
| 19 | KUA | Know your customer User Agencies |

| | | |
|----|------|--------------------------------------|
| 20 | NDA | Non-Disclosure Agreement |
| 21 | NTP | Network Time Protocol |
| 22 | OTP | One Time Password |
| 23 | PID | Personal Identity Data |
| 24 | PII | Personally Identifiable Information |
| 25 | PoT | Point of Transaction |
| 26 | SOP | Standard Operating Procedures |
| 27 | SPOC | Single Point of Contact |
| 28 | SSL | Secure Sockets Layer |
| 29 | STQC | Standard testing and quality control |
| 30 | VA | Vulnerability Assessment |
| 31 | VPN | Virtual Private Network |
| 32 | WAF | Web Application Firewall |

2.3 Policy

AUAs / KUAs shall ensure the confidentiality, integrity, and availability of UIDAI related data and services.

Information Security Domains and related Controls

2.4 Human Resources

1. AUAs / KUAs shall appoint a SPOC/team for Aadhaar related activities and communication with UIDAI;
2. AUA/KUA shall conduct a background check or sign an agreement/NDA with all personnel/agency handling Aadhaar related authentication data. UIDAI or agency appointed by UIDAI may validate this information.
3. An induction as well as periodic functional and information security trainings shall be conducted for all AUA/KUA personnel for Aadhaar related authentication services. The training shall include all relevant security guidelines per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016.
4. Aware of the UIDAI disciplinary and proper communication processes in the event of an information security breach.
5. All employees accessing UIDAI information assets shall be made aware of UIDAI information security policy and controls.

2.5 Asset Management

1. All assets used by the AUA/ KUA (business applications, operating systems, databases, network etc.) for the purpose of delivering services to residents using Aadhaar authentication services shall be identified labelled and classified . Details of the information asset shall be recorded.
2. The assets which are scheduled to be disposed must have a procedure as part of the disposal policy of the organization. Information systems containing UIDAI information shall be disposed-off securely only after obtaining approvals from UIDAI authorized personnel;
3. Before sending any equipment out for repair, the equipment shall be sanitised to ensure that it does not contain any UIDAI sensitive data;
4. AUA / KUA shall not transfer or make an unauthorized copy of any identity information from removable media to any personal device or other unauthorized electronic media / storage devices.
5. AUA shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets.
6. Authentication devices used to capture residents biometric should be STQC certified as specified by UIDAI.

2.6 Access Control

1. Only authorized individuals shall be provided access to information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing UIDAI information;
2. AUA / KUA employees with access to UIDAI information assets shall:
 - a) Have least privilege access for information access and processing;
 - b) The operator must be logged out after the session is finished.
 - c) Implement an equipment locking mechanism for workstation, servers and/ or network device
3. The application should have auto lock out feature i.e. after a certain time of inactivity (15 mins or as specified in the AUA/KUA policy document), the application should log out.

4. Access rights and privileges to information processing facilities for UIDAI information shall be revoked within 24 hours separation of respective personnel or as mentioned in the exit management policy of the organization. Post deactivation, user IDs shall be deleted if not in use as per Exit formalities.
5. Access rights and privileges to information facilities processing UIDAI information shall be reviewed on a quarterly basis and the report shall be stored for audit purposes;
6. Common user IDs / group user IDs shall not be used. Exceptions/ risk acceptance shall be approved and documented where there is no alternative;
7. Procedures shall be put in place for secure storage and management of administrative passwords for critical information systems if done manually then a fire proof safe or similar password vault must be used to maintain the access log register.
8. The users should not be provided with local admin access rights on their system. In the case of administrative access being provided, the users shall be prohibited from modifying the local security settings. Modifying the same shall result in disciplinary action.
9. Three successive login failures or as per the access control policy/password policy of the organization should result in a user's account being locked; they should not be able to login until their account is unlocked and the password reset in case of server logins. The user should contact the System Engineers/Administrators for getting the account unlocked. For applications there should be an automatic lock out period of 30 mins in case of three consecutive login failures or as per the access control policy/password policy of the organization.
10. The local security settings on all the systems shall be aligned and synced with the Active Directory or similar solutions for group policy enforcement..
11. If the application is operator assisted, the operator shall first authenticate himself before authenticating the residents.
12. The access rules of firewalls shall be maintained only by users responsible for firewall administration.

2.7 Password Policy

1. The allocation of initial passwords shall be done in a secure manner and these passwords shall be changed at first login;
2. All User passwords (including administrator passwords) shall remain confidential and shall not be shared, posted or otherwise divulged in any manner;
3. Avoid keeping a paper record of passwords, unless this can be stored securely;
4. If the passwords are being stored in the database or any other form, they should be stored in encrypted form.
5. Change passwords whenever there is any indication of possible system or password compromise;
6. Complex passwords shall be selected with a minimum length of 8 characters, which are:
 - (a) Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;
 - (b) Free of consecutive identical characters or all-numeric or all-alphabetical groups;
 - (c) Password should contain at least one numeric, one uppercase letter and one special character;
 - (d) Passwords shall be changed at regular intervals (passwords for privileged accounts shall be changed more frequently than normal passwords);
 - (e) System should not allow the use of last 5 passwords.
 - (f) System should not allow the username and password to be the same for a particular user.
 - (g) Users must not use the same password for various UIDAI access needs;
7. Passwords shall not be hardcoded in codes, login scripts, any executable program or files;
8. Password should not be stored or transmitted in applications in clear text or in any reversible form.

9. Passwords shall not be included in any automated log-on process, e.g. stored in a macro or function key;
10. Three successive login failures should result in a user's account being locked; they should not be able to login until their account is unlocked and the password reset. The user should contact the System Engineers/Administrators for getting the account unlocked;

2.8 Cryptography

1. The Personal Identity data (PID) block comprising of the resident's demographic / biometric data shall be encrypted as per the latest API documents specified by the UIDAI at the end point device used for authentication (for e.g. PoT terminal)
2. The PID shall be encrypted during transit and flow within the AUA / KUA ecosystem and while sharing this information with ASAs;
3. The encrypted PID block should not be stored unless in case of buffered authentication for not more than 24 hours after which it should be deleted from the local systems;
4. The authentication request shall be digitally signed by either by AUA/KUA or ASA as per the mutual agreement between them;
5. While establishing a secure channel to the AADHAAR Authentication Server (AAS), the AUA / KUA shall verify the following:
 - a) The digital certificate presented by the AAS has been issued / signed by a trusted Certifying Authority (CA);
 - b) The digital certificate presented by the AAS has neither been revoked nor expired;
 - c) The Common Name (CN) on the certificate presented by the AAS matches with its fully qualified domain name (presently, auth.uidai.gov.in);
6. Key management activities shall be performed by all AUAs / KUAs to protect the keys throughout their lifecycle. The activities shall address the following aspects of key management, including;
 - a) key generation;
 - b) key distribution;
 - c) Secure key storage;
 - d) key custodians and requirements for dual Control;
 - e) prevention of unauthorized substitution of keys;
 - f) Replacement of known or suspected compromised keys;
 - g) Key revocation and logging and auditing of key management related activities.

2.9 Physical and Environmental Security

1. The AUA/KUA servers should be placed in a secure lockable cage in the AUA Data Centre.
2. The facility should be manned by security guards during and after office hours
3. CCTV surveillance shall cover the AUA/KUA servers.
4. Access to the premises should be limited to authorised personnel only and appropriate logs for entry of personnel should be maintained.
5. The movement of all incoming and outgoing items shall be documented;
6. All required measures for the Data Centre safety shall be taken.
7. Lockable cabinets or safes shall be provided in the offices, rooms and information processing facilities for critical information storage especially for Aadhaar related information.
8. Fire doors and extinguishing systems shall be deployed, labeled, monitored, and tested regularly;
9. Preventive maintenance activities like audit of fire extinguishers, CCTV should be periodically done.

10. Physical access to restricted areas or offices and facilities hosting critical equipment shall be pre-approved and recorded along with the date, time and purpose of entry;
11. Signs or notices legibly setting forth the designation of restricted areas and provisions of entry shall be posted at all entrances and at other points along the restricted areas as necessary especially where the AUA servers are physically hosted.;
12. Controls shall be designed and implemented to protect power and network cables from unauthorized interception or damage;
13. A clear desk and clear screen policy for UIDAI information processing facilities shall be adopted to reduce risks of unauthorized access, loss and damage to information related to UIDAI. Following shall be ensured:
 - a) Screen saver or related technological controls shall be implemented to lock the screen of the information systems when unattended beyond a specified duration;
 - b) Unused paper documents and printed papers shall be shredded.

2.10 Operations Security

1. All AUAs / KUAs shall complete the AADHAAR AUA / KUA on-boarding process before the commencement of formal operations;
2. Standard Operating Procedure (SOP) shall be developed for all information systems and services related to UIDAI operations. The SOP shall include the necessary activities to be carried out for the operation and maintenance of the system or service and the actions to be taken in the event of a failure;
3. Persons involved in operational/development/testing functions shall not be given additional responsibilities in system administration processes, audit log maintenance, security review of system or process and which may compromise data security requirements;
4. Where segregation of duties is not possible or practical, the process shall include compensating controls – such as monitoring of activities, maintenance and review of audit trails and management supervision;
5. The Test and Production facilities / environments must be physically and/or logically separated.
6. The Operating System as well as the network services used for communication with the PoT terminals shall be updated with the latest security patches.
7. A formal Patch Management Procedure shall be established for applying patches to the information systems. Patches should be updated at both application and server level;
8. Periodic VA exercise should be conducted for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.
9. AUA / KUA employees shall not intentionally write, generate, compile copy or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any PID information;
10. All hosts that connect to the AADHAAR Authentication Service or handle resident's identity information shall be secured using endpoint security solutions. At the minimum, anti-virus / malware detection software shall be installed on such hosts;
11. Network intrusion and prevention systems should be in place – e.g. IPS, IDS, WAF, etc.
12. AUAs / KUAs shall ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring;

13. Regular monitoring of the audit logs shall take place for any possible unauthorized use of information systems and results shall be recorded. Access to audit trails and event logs shall be provided to authorized personnel only;
14. The authentication audit logs should contain, but not limited to, the following transactional details:
 - a) 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
 - e) Record of the consent of Aadhaar number holder for the resident
 - f) Details of the authentication transaction such as API Name, AUA / KUA Code, Sub-AUA, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-identity information.
15. Logs shall not, in any event, retain the PID, biometric and OTP information;
16. No data pertaining to the resident or the transaction shall be stored within the terminal device;
17. The logs of authentication transactions shall be maintained by the AUA/KUA for a period of 2 years, during which an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified;
18. Upon expiry of the period of 2 years, the logs shall be archived for a period of 5 years or the number of years as required by the laws or regulations governing the AUA/KUA, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by court or for any pending disputes;
19. All computer clocks shall be set to an agreed standard using a NTP server or must be managed centrally and procedure shall be made to check for and correct any significant variation;
20. The AUA / KUA server host shall reside in a segregated network segment that is isolated from the rest of the network of the AUA / KUA organisation; The AUA / KUA server host shall be dedicated for the Online AADHAAR Authentication purposes and shall not be used for any other activities;

2.11 Communications security

1. In case of a composite terminal device that comprises of a biometric reader without embedded software to affect the encryption of the personal identity data, communication between the biometric reader and the device performing the encryption shall be secured against all security threats / attacks
2. Terminal devices shall provide different log-ins for operators. These users shall be authenticated using some additional authentication scheme such as passwords, AADHAAR authentication, etc.;
3. Each terminal shall have a unique terminal ID. This number must be transmitted with each transaction along with UIDAI assigned institution code for the AUA / KUA as specified by the latest UIDAI API documents
4. A Unique Transaction Number (unique for that terminal) shall be generated automatically by the terminal which should be incremented for each transaction processed;
5. The network between AUA / KUA and ASA shall be secured. AUA / KUA shall connect with ASAs through leased lines or similar secure private lines. If a public network is used, a secure channel such as SSL or VPN shall be used.
6. The AUA / KUA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the AUA / KUA server from all sources other than AUAs / KUAs PoT terminals;
7. Wherever ATM/kiosk based authentication is used, the systems shall be secured at the device and communication level;

8. Special consideration shall be given to Wireless networks due to poorly defined network perimeter. Appropriate authentication, encryption and user level network access control technologies shall be implemented to secure access to the network;
9. Use of web based e-mail shall be restricted to official use and in accordance with the acceptable usage guidelines or as per organization policy;
10. UIDAI should be informed about the ASAs, the AUA has entered into an agreement;

2.12 Information Security Incident Management

1. AUA / KUA shall be responsible for reporting any security weaknesses, any incidents, possible misuse or violation of any of the stipulated guidelines to UIDAI immediately;

2.13 Compliance

1. AUAs / KUAs shall comply with all terms and conditions outlined in the UIDAI AUA / KUA agreement and AUA / KUA compliance checklist;
2. AUAs / KUAs shall ensure that its operations are audited by an information systems auditor certified by a recognised body on an annual basis and on a need basis to ensure compliance with UIDAI standards and specifications. The audit report shall be shared with UIDAI upon request;
3. If any non-compliance is found as a result of the audit, management shall:
 - a) Determine the causes of the non-compliance;
 - b) Evaluate the need for actions to avoid recurrence of the same;
 - c) Determine and enforce the implementation of corrective and preventive action;
 - d) Review the corrective action taken.
4. UIDAI shall reserve right to audit systems and processes of the AUA / KUA on an annual basis or as needed to ensure compliance with stipulated Information Security Policy – External Ecosystem AUA-KUA but not limited to this document. The audit plan shall include information security controls and technical testing controls including vulnerability assessment as well as penetration testing of Information Systems and any new technology or delivery channel introduced;
5. AUAs / KUAs shall use only licensed software for UIDAI related infrastructure environment. Record of all software licenses shall be kept and updated regularly;
6. AUAs / KUAs and their partners shall ensure compliance to all the relevant laws, rules and regulations, including, but not limited to, ISO27001:2013 Standard, Information Technology Act 2000 and 2008 amendments, Aadhaar Act, 2016 and Regulations;
7. It is recommended that AUA / KUA shall deploy as part of its systems, a Fraud Analytics module that is capable of analyzing authentication related transactions to identify fraud.
8. eKYC should be used as a facility using only biometric and OTP modalities by the AUAs
9. Separate license keys must be generated by all AUAs for their SUB-AUAs from the UIDAI portal
10. AUA must have their authentication servers routing to CIDR hosted in Data Centres within India

2.14 Change Management

1. AUAs / KUAs shall document all changes to UIDAI Information Processing facilities/ Infrastructure/ processes;
2. Entities shall implement only those changes related to Aadhaar which are approved by UIDAI for execution;
3. Change log/ register shall be maintained for all changes performed.



UIDAI INFORMATION SECURITY POLICY – UIDAI EXTERNAL ECOSYSTEM – AUTHENTICATION SERVICE AGENCIES

UIDAI

Unique Identification Authority of India

Ministry of Electronics and Information Technology (MeitY),
Govt. of India (GoI), 3rd Floor, Tower II,
Jeevan Bharati Building, Connaught Circus,
New Delhi 110001

Document Control

| S. No. | Type of Information | Document Data |
|--------|----------------------|---|
| 1. | Document Title | UIDAI Information Security Policy –External Ecosystem ASA |
| 2. | Document Code | UIISP-ASA |
| 3. | Date of Release | |
| 4. | Document Superseded | UIDAI Information Security Policy v3.2 |
| 5. | Document Revision No | 3.3 |
| 6. | Document Owner | Shri Ajai Chandra, ADG (Authentication), UIDAI |
| 7. | Document Author(s) | |

Document Approvers

| S. No. | Approver | Approved Through/ Nominee | Comments |
|--------|-------------------------|---------------------------|----------|
| 1. | Shri. A.B. Pandey (CEO) | | |
| | | | |

Document Change Approvals

| Version No. | Revision Date | Nature of Change | Date Approved |
|-------------|---------------|---|---|
| Version 1.1 | 01-Dec-2011 | First version (2011) | December-2011 |
| Version 2.0 | 08-May-2014 | <ul style="list-style-type: none"> Alignment with ISO 27001:2013 requirements Segregation of Control Statements from the Procedures and Guidelines Addition of Information Security Governance Framework Updating of security policies for UIDAI external ecosystem | 27-Oct-14 |
| Version 3.0 | 23-Jan-2015 | <ul style="list-style-type: none"> Revision of Governance framework (ISMS) for stage I ISO27001:2013 | 02-Feb-15 |
| Version 3.1 | 27-Feb-2015 | <ul style="list-style-type: none"> Update of Annexure documents as per stage-2 comments | 24-Apr-15 |
| Version 3.2 | 22-Dec-2015 | <ul style="list-style-type: none"> Creation of separate booklet from existing UIDAI information security policy document for external ecosystem partner for Authentication – ASA | No. F-11014/06/2014-Tech (Vol-II)/631 Dated 27 th April 2016 |
| Version 3.3 | 28-Feb-2017 | <ul style="list-style-type: none"> Annual Review | |

Statement of Confidentiality

This document presents the Information Security Policy of UIDAI for external ecosystem partners ASA and contains information that is proprietary and confidential to UIDAI. Any use or disclosure in whole or part of this information for any reason without written permission of UIDAI is strictly prohibited.

Feb 2017, UIDAI

Foreword

The UIDAI ecosystem is one of the most complex environments in the world today. The entire backbone of this ecosystem is the residents' identity Information, which is created, processed, transmitted, stored and securely disposed by UIDAI and its ecosystem partners. Hence, it is imperative to define and implement robust controls to safeguard the residents' identity information, and create trust between the residents and the UIDAI ecosystem against the misuse of such information.

UIDAI has defined a set of people, process and technical controls to govern the use of this information, in alignment with industry standards such as ISO 27001. Focus of this document is to protect residents' information and the information infrastructure, build capabilities to prevent and respond to information security threats, eliminate identified vulnerabilities and minimize damage from information security incidents through a combination of institutional structures, people, processes and technology.

This Information Security policy document specifies the scope and the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the Information Security environment/landscape of Unique Identification Authority of India (UIDAI).

Table of Contents

| | |
|--|-----------------|
| <i>UIDAI Information Security Policy – Authentication Service Agencies.....</i> | <i>6</i> |
| <i>1. Policy Statement.....</i> | <i>7</i> |
| 1.1 Control Objective | 7 |
| 1.2 Scope..... | 7 |
| <i>2. Information Security Policy for Authentication Service Agencies</i> | <i>8</i> |
| 2.1 Purpose | 8 |
| 2.2 Terms and definitions | 8 |
| 2.3 Policy | 9 |
| 2.4 Human Resources | 10 |
| 2.5 Asset Management | 10 |
| 2.6 Access Control..... | 10 |
| 2.7 Password Policy..... | 11 |
| 2.8 Cryptography | 11 |
| 2.9 Physical and Environmental Security..... | 12 |
| 2.10 Operations Security..... | 12 |
| 2.11 Communications Security | 13 |
| 2.12 Compliance | 14 |
| 2.13 Change Management..... | 15 |



UIDAI Information Security Policy – Authentication Service Agencies

1. Policy Statement

Security of UIDAI information assets handled by the external ecosystem partners for providing services, is of paramount importance. The confidentiality, integrity and availability of these shall be maintained at all times by these partners by deploying controls commensurate with the asset value.

1.1 Control Objective

UIDAI shall ensure the security of UIDAI information assets handled by third parties by:

1. Providing ASAs with an approach and directives for implementing information security of all information assets used by them for providing services to UIDAI and AUAs;
2. Establishing review mechanism to ensure that the ASAs adhere to all provisions of the UIDAI Information Security Policy – External Ecosystem ASA.

1.2 Scope

The UIDAI Information Security Policy – External Ecosystem partner ASA is applicable to all Authentication Service Agencies that provide CIDR connectivity to AUAs/KUAs.

1. **Authentication Service Agency (ASA):** Authentication Service Agency is an organization or an entity that transmits authentication requests to the CIDR on behalf of one or more AUAs.

ASAs have established secure leased line connectivity with the CIDR compliant with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to Authentication User Agencies (AUA) and transmit AUAs' authentication requests to CIDR. Only agencies contracted with UIDAI as ASAs shall send authentication requests to the CIDR; no other entity can directly communicate with CIDR. An ASA could serve several AUAs; and may also offer value added services such as multi-party authentication, authorization and MIS reports to AUAs.

This Policy is applicable wherever UIDAI information is processed and/or stored by Authentication Service Agencies.

2. Information Security Policy for Authentication Service Agencies

2.1 Purpose

This section outlines the Information Security policy and Information Security controls applicable for Authentication Service Agencies (ASAs).

2.2 Terms and definitions

| S.No. | Terms | Definition |
|-------|--|---|
| 1 | AAS | AADHAAR Authentication Server |
| 2 | ADG | Assistant Director General |
| 3 | AUA/ASA | Authentication User Agency/Authentication Service Agency |
| 4 | CA | Certifying Authority |
| 5 | CCTV | Closed Circuit Television |
| 6 | CIDR | Central Identities Data Repository |
| 7 | CN | Common Name |
| 8 | DDG | Deputy Director General |
| 9 | eKYC | Electronic Know Your User |
| 10 | GRC | Governance, Risk and Compliance |
| 11 | Asset | <p>An asset is anything that has value to the organization. Assets can be classified into the following 5 categories:</p> <ol style="list-style-type: none"> 1. Paper assets: (Legal documentation, manuals, policies & procedures, organizational documents etc.) 2. Physical assets: (computer equipment, communications, utility equipment, buildings etc.) 3. Software assets: (database information, applications, software code, development tools, operational software etc.) 4. People assets: UIDAI human resources and stakeholders. 5. Service assets: (Logistics, building management systems, communications, utilities etc.) |
| 12 | Information/ Information Asset (IA) | Information that has value to the organization (UIDAI). Including but not limited to Citizen biometric and demographic information, personally identifiable information, employee information, organization information such as CIDR architecture, infrastructure, network details etc. |
| 13 | IDS | Intrusion Detection System |
| 14 | ISO (ISO27001) | International Organisation of Standardization |
| 15 | IT | Information Technology |
| 16 | IPS | Intrusion Prevention system |
| 17 | KUA | Know your customer User Agencies |
| 18 | NDA | Non-Disclosure Agreement |
| 19 | NTP | Network Time Protocol |
| 20 | PID | Personal Identity Data |
| 21 | PII | Personally Identifiable Information |

| | | |
|----|------|--------------------------------------|
| 22 | SPOC | Single Point of Contact |
| 23 | SSL | Secure Sockets Layer |
| 24 | STQC | Standard testing and quality control |
| 25 | TSU | Technical Support Unit |
| 26 | VA | Vulnerability Assessment |
| 27 | VPN | Virtual Private Network |
| 28 | WAF | Web Application Firewall |

2.3 Policy

Authentication Service Agencies shall ensure the confidentiality, integrity, and availability of UIDAI related data and services.

Information Security Domains and related Controls

2.4 Human Resources

1. ASAs shall appoint a SPOC/team for all UIDAI related activities and communication with UIDAI;
2. ASA shall conduct a background check or sign an agreement/NDA with all personnel/agency handling aadhaar related authentication data. UIDAI or agency appointed by UIDAI may validate this information.
3. An induction as well as periodic functional and information security trainings shall be conducted for all ASA personnel for UIDAI related services. The training shall include all relevant security guidelines per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016.
4. All employees accessing UIDAI information assets shall be made aware of UIDAI information security policy and controls.

2.5 Asset Management

1. All assets used by the ASA (servers, network devices, etc.) for the purpose of delivering services to UIDAI shall be identified, labelled and classified. Details of the information asset shall be recorded.
2. The assets which are scheduled to be disposed must have a procedure as part of the disposal policy of the organization. Information systems containing UIDAI information shall be disposed-off securely only after obtaining approvals from UIDAI authorized personnel.
3. Before sending any equipment out for repair, the equipment shall be sanitised to ensure that it does not contain any UIDAI sensitive data.
4. ASA shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets.

2.6 Access Control

1. Only authorized individuals shall be provided access to information assets (such as servers, network devices etc.) processing UIDAI information.
2. ASA personnel with access to UIDAI information assets shall:
 - a) Have least privilege access for information access and processing;
 - b) The operator must be logged out after the session is finished.
3. The systems should have auto lock out feature i.e. after a certain time of inactivity (15 mins or as specified in the ASA policy document), the system should log out;
4. Access rights and privileges to information assets for UIDAI information shall be revoked within 24 hours separation of respective personnel or as mentioned in the exit management policy of the organization. Post deactivation, user IDs shall be deleted if not in use as per Exit formalities;
5. Access rights and privileges to information facilities processing UIDAI information shall be reviewed on a quarterly basis and the report shall be stored for audit purposes;
6. Common user IDs / group user IDs shall not be used. Exceptions/ risk acceptance shall be approved and documented where there is no alternative;
7. Procedures shall be put in place for secure storage and management of administrative passwords for critical information systems.
8. The users should not be provided with local admin access rights on their system. In the case of administrative access being provided, the users shall be prohibited from modifying the local security settings. Modifying the same shall result in disciplinary action.

9. Three successive login failures or as per the access control policy/password policy of the organization should result in a user's account being locked; they should not be able to login until their account is unlocked and the password reset in case of server logins. The user should contact the System Engineers/Administrators for getting the account unlocked. For applications there should be an automatic lock out period of 30 mins in case of three consecutive login failures or as per the access control policy/password policy of the organization.
10. The local security settings on all the systems shall be aligned and synced with the Active Directory or similar solutions for group policy enforcement.

2.7 Password Policy

1. The allocation of initial passwords shall be done in a secure manner and these passwords shall be changed at first login;
2. All User passwords (including administrator passwords) shall remain confidential and shall not be shared, posted or otherwise divulged in any manner;
3. Avoid keeping a paper record of passwords, unless this can be stored securely;
4. If the passwords are being stored in the database or any other form, they should be stored in encrypted form.
5. Change passwords whenever there is any indication of possible system or password compromise;
6. Complex passwords shall be selected with a minimum length of 8 characters, which are:
 - a. Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;
 - b. Free of consecutive identical characters or all-numeric or all-alphabetical groups;
 - c. Password should contain at least one numeric, one uppercase letter and one special character;
 - d. Passwords shall be changed at regular intervals (passwords for privileged accounts shall be changed more frequently than normal passwords);
 - e. System should not allow the use of last 5 passwords.
 - f. System should not allow the username and password to be the same for a particular user.
 - g. Users must not use the same password for various UIDAI access needs;
7. Passwords shall not be hardcoded in codes, login scripts, any executable program or files;
8. Password should not be stored or transmitted in applications in clear text or in any reversible form.
9. Passwords shall not be included in any automated log-on process, e.g. stored in a macro or function key;
10. Three successive login failures should result in a user's account being locked; they should not be able to login until their account is unlocked and the password reset. The user should contact the System Engineers/Administrators for getting the account unlocked;

2.8 Cryptography

1. While establishing a secure channel to the AADHAAR Authentication Server (AAS), the ASA shall verify the following:
 - a) The digital certificate presented by the AAS has been issued / signed by a trusted Certifying Authority (CA);
 - b) The digital certificate presented by the AAS has neither been revoked nor expired;
 - c) The Common Name (CN) on the certificate presented by the AAS matches with its fully qualified domain name (presently, auth.uidai.gov.in);

2. Key management activities shall be performed by all ASAs to protect the keys throughout their lifecycle. The activities shall address the following aspects of key management, including;
 - a) key generation;
 - b) key distribution;
 - c) Secure key storage;
 - d) key custodians and requirements for dual Control;
 - e) prevention of unauthorized substitution of keys;
 - f) Replacement of known or suspected compromised keys;
 - g) Key revocation and logging and auditing of key management related activities.
3. Encrypted PID block and license keys that came as part of authentication packet should never be stored anywhere in its system.

2.9 Physical and Environmental Security

1. The ASA servers/network equipment should be placed in a secure lockable cage in the ASA data center.
2. The facility should be manned by security guards during and after office hours.
3. CCTV surveillance shall cover the ASA servers.
4. Access to the premises should be limited to authorised personnel only and appropriate logs for entry of personnel should be maintained.
5. The movement of all incoming and outgoing items shall be documented;
6. Lockable cabinets or safes shall be provided in the offices, rooms and information processing facilities for critical information storage especially for UIDAI related documents as applicable.
7. Fire doors and extinguishing systems shall be deployed, labeled, monitored, and tested regularly;
8. Preventive maintenance activities like audit of fire extinguishers, CCTV should be periodically done.
9. Physical access to restricted areas or offices and facilities hosting critical equipment shall be pre-approved and recorded along with the date, time and purpose of entry
10. Signs or notices legibly setting forth the designation of restricted areas and provisions of entry shall be posted at all entrances and at other points along the restricted areas as necessary especially where the ASA servers/network equipment are physically hosted.
11. Controls shall be designed and implemented to protect power and network cables from unauthorized interception or damage;
12. A clear desk and clear screen policy for UIDAI information processing facilities shall be adopted to reduce risks of unauthorized access, loss and damage to information related to UIDAI. Following shall be ensured:
 - a) Screen saver or related technological controls shall be implemented to lock the screen of the information systems when unattended beyond a specified duration;
 - b) Unused paper documents and printed papers shall be shredded.

2.10 Operations Security

1. All ASAs shall complete the AADHAAR ASA on-boarding process before the commencement of formal operations;
2. ASA shall only engage with the AUAs / KUAs approved by UIDAI and keep UIDAI informed of the list of AUAs it serves. In case of disengagement with an AUA / KUA, the ASA shall inform UIDAI within a period of 7 days from the date of disengagement;

3. Standard Operating Procedure (SOP) shall be developed for all information systems and services related to UIDAI operations. The SOP shall include the necessary activities to be carried out for the operation and maintenance of the system or service and the actions to be taken in the event of a failure;
4. Where segregation of duties is not possible or practical, the process shall include compensating controls – such as monitoring of activities, maintenance and review of audit trails and management supervision;
5. The Test and Production facilities / environments must be physically and/or logically separated.
6. ASA personnel shall conduct integrity checks to verify the completeness of the data packet and authenticity of the authentication user agency before processing the authentication request. A formal Patch Management Procedure shall be established for applying patches to the information systems. Patches should be updated at both application and server level;
7. Periodic VA exercise should be conducted for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.
8. ASA employees shall not intentionally write, generate, compile copy or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any PID information;
9. ASA servers connected to the CIDR shall be secured using endpoint security solutions. At the minimum, anti-virus / malware detection software shall be installed;
10. Network intrusion and prevention systems should be in place – e.g. IPS, IDS, WAF, etc.
11. ASAs shall ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring;
12. Regular monitoring of the audit logs shall take place for any possible unauthorized use of information systems and results shall be recorded. Access to audit trails and event logs shall be provided to authorized personnel only;
13. The authentication audit logs should contain, but not limited to, the following transactional details:
 - a. Identity of the requesting entity
 - b. Parameters of authentication request submitted
 - c. Parameters received as authentication response
14. Aadhaar number, PID information, device identity related data and eKYC response data shall not be retained in the ASA logs.
15. The logs of authentication transactions shall be maintained by the ASA for a period of 2 years, during which an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified.
16. Upon expiry of the period of 2 years, the logs shall be archived for a period of 5 years or the number of years as required by the laws or regulations governing the ASA, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by court or for any pending disputes.
17. All server/network devices clocks shall be set to an agreed standard using a NTP server or must be managed centrally and procedure shall be made to check for and correct any significant variation;
18. The ASA server host shall reside in a segregated network segment that is isolated from the rest of the network of the ASA organisation; The ASA server host shall be dedicated for the Online AADHAAR Authentication purposes and shall not be used for any other activities;
19. Service Continuity and service availability shall be ensured.

2.11 Communications Security

1. The network between AUA / KUA and ASA shall be secured. AUA / KUA shall connect with ASAs through leased lines or similar secure private lines. If a public network is used, a secure channel such as SSL or VPN shall be used.
2. The network between ASA and CIDR shall be secure. ASA shall connect with CIDR through leased lines or similar secure private lines.
3. The ASA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the server from all sources other than the respective AUAs / KUAs
4. The ASA server host shall reside in a segregated network segment that is isolated from the rest of the network of the ASA organisation;
5. Non-essential services shall be disabled on all information systems;
6. Use of e-mail shall be restricted to official use and in accordance with the acceptable usage guidelines or as per organization policy Information Security Incident Management.
7. ASA shall be responsible for reporting any security weaknesses, any incidents, possible misuse or violation of any of the stipulated guidelines to UIDAI immediately.

2.12 Compliance

1. ASAs shall comply with all terms and conditions outlined in the UIDAI ASA agreement and ASA compliance checklist.
2. ASAs shall ensure that its operations are audited by an information system auditor certified by a recognised body on an annual basis and on need basis to ensure compliance with standards and specifications. The audit report shall be shared with UIDAI upon request;
3. If any non-compliance is found as a result of the audit, management shall:
 - a) Determine the causes of the non-compliance;
 - b) Evaluate the need for actions to avoid recurrence of the same;
 - c) Determine and enforce implementation of corrective action;
 - d) Review the corrective action taken.
4. UIDAI shall reserve right to audit systems and processes of the ASA on an annual basis and as needed to ensure compliance with stipulated security guidelines. The audit plan shall include information security controls audit and technical testing including vulnerability assessment as well as penetration test of Information Systems and any new technology or delivery channel introduced;
5. ASA shall use only licensed software within the UIDAI network environment. Record of all software licenses shall be kept and updated regularly;
6. ASAs and their partners shall ensure compliance to all the relevant laws, rules and regulations, including, but not limited to, ISO27001: 2013 Standard, IT Act 2000 and 2008 amendments ;It is recommended that ASA shall deploy as part of its systems, a Fraud Analytics module that is capable of analyzing authentication related transactions to identify fraud.
7. ASA must have their authentication servers routing to CIDR hosted in data centres within India.
8. 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;
9. ASA shall at all times, comply with directions, specifications, etc. issued by the Authority, in terms of network and other Information Technology infrastructure, processes, procedures, etc.
10. ASA shall comply with all relevant laws and regulations relating, in particular, to data security and data management.

11. ASA 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.

2.13 Change Management

1. ASAs shall document all changes to UIDAI Information Processing facilities/ Infrastructure/ processes;
2. Change log/ register shall be maintained for all changes performed.

SECTION 3

OTHER CIRCULARS, GUIDELINES etc

IMPORTANT

No. K-11020/44/2012-UIDAI (Auth-I)
Government of India
Ministry of Electronics & IT
Unique Identification Authority of India
(Authentication Division)

Tower I, 9th Floor, Jeevan Bharati Building,
Connaught circus, New Delhi-110001.
Dated: 25.01.2017

To

All AUAs, ASAs

Sub: Upgradation of existing biometric public devices to Registered Devices

Dear Partners,

UIDAI is committed towards providing the highest quality of services in an efficient and secure manner. To enhance the security level, UIDAI has taken several security measures to ensure security of transactions and end to end traceability during the authentication process. To make it more robust and secure, UIDAI along with biometric device vendors and STQC is working on the concept of Registered Devices.

2. The key features of Registered Devices are:

- a. Device identification – Every device will have a unique identifier allowing traceability, analytics and fraud management.
- b. Eliminating advanced replay attacks – Biometric data is signed within the device using the provider key to ensure it is indeed captured live.
- c. A standardized and certified Device Driver is to be provided by the device providers. This device driver (exposed via an SDK/Service) encapsulates the biometric capture, any user experience while capture (such as preview), and signing and encryption of biometrics all within it. The Device Driver must form the encrypted PID block before returning to the host application.

- d. There are two levels of Registered Devices named as Level 0 (software level upgrade is possible for existing public devices) and Level 1 (hardware and software level changes are required). The detailed specifications for Registered Devices are available at the link below:

https://uidai.gov.in/images/resource/aadhaar_registered_devices_2_0_09112016.pdf

3. It is expected that device vendor SDK's would be certified as either Level 0 or Level 1 by 31st March 2017. Please contact your biometric device vendor for their schedule to support registered devices. Register device authentication backend capability will be live by 31st March 2017.

4. A decision has been taken by UIDAI that use of public devices will be discontinued and only Registered Devices will be allowed to perform Aadhaar based authentication. Therefore, you need to ensure that all biometric devices deployed for Aadhaar enabled services are upgraded to Level 0 / Level 1 Registered Device by 1st June 2017 and all future procurement of biometric devices shall from now on be as per Level 0 / Level 1 Registered Device specifications. Authentication applications will also require modification to support the registered device SDK (Level 0 / Level 1). UIDAI Authentication API 2.0 will be upgraded to only support registered device authentication. This will promote a direct upgrade from the current applications with public devices using API 1.6 to applications with registered devices using API 2.0. Accordingly, the timelines for the support for Authentication API 1.6 will be extended from 31st March 2017 to 1st June 2017. Please note that there will be no extension of this timeline and use of public devices after 1st June 2017 shall result in failed authentication transactions for which the responsibility shall be yours.

5. You may also immediately ask your device vendor to ensure upgrade of existing biometric devices to Registered Devices and provide all the required support and details for the upgrade.

6. All ASAs also need to ensure that they are able to support Auth API 2.0 which supports Registered Devices and accordingly need to prepare their system on top priority.

7. Your application development team also needs to be sensitized as changes will be required in the application and backend server to make it compatible with Registered Device and Authentication API 2.0 and would need to be tested thoroughly. Therefore, it is suggested that your technical team should be ready and get in touch with your biometric device supplier/vendor for upgradation to the latest Registered Devices specifications.

8. UIDAI is committed to ensuring that all necessary applications are upgraded on time and there is smooth transition to Registered Devices. UIDAI has already initiated workshops with all stakeholders including device providers and will continuously support entire ecosystem during this transition. In case you have any query on Registered Devices, you may kindly get in touch with UIDAI team:

Shri Yashwant Kumar, ADG yashwant.kumar@uidai.net.in

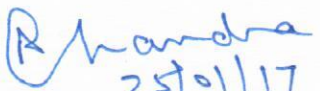
Shri Anup Kumar, ADG anup.kumar@uidai.net.in

Technical Contact Person:

Shri Rakesh Prasad rakesh.prasad@uidai.net.in

Shri Sanjith Sundaram sanjith.sundaram@uidai.net.in

9. This issues with the approval of CEO, UIDAI.


25/01/17
(Ajai Chandra)
ADG (Auth)

Copy for information to:

1. DG, STQC
2. Sh. Anup Kumar, ADG UIDAI
3. Sh. Pramod Varma, Chief Technology Architect, UIDAI
4. Sh. Vivek Raghavan, Chief Product Manager, UIDAI
5. All device vendors having STQC certified biometric devices

F. No. K-11022/460/2016-UIDAI (Auth-II)
Unique Identification Authority of India
Government of India

9th Floor, Tower I,
Jeevan Bharati Building
Connaught Circus
New Delhi – 110001
Dated: 28.02.2017

To

All AUAs / KUAs

Subject: Instructions for providing Authentication / e-KYC services by AUA/KUA to sub-AUAs and other entities

The Aadhaar (Authentication) Regulations 2016 allow Authentication User Agencies (AUAs) to appoint Sub-AUAs for availing authentication services under Regulation number 15. Similarly under Regulation number 16, e-KYC User Agencies (KUAs) can perform e-KYC authentication on behalf of other entities. In this regard, it is necessary that these services are provided by AUAs / KUAs in such a manner which does not violate any provisions of the Aadhaar Act, 2016 and its regulations.


The AUAs/ KUAs are directed to strictly observe the following instructions while providing authentication services to Sub-AUAs or other entities:

1. The AUA / KUA shall ensure that
 - i. the client application to be used or being already used for Aadhaar authentication is developed by AUA/KUA and is digitally signed by AUA/KUA.
 - ii. the client application does not store biometric data under any circumstance and biometrics /PID block is encrypted at frontend device / client level only.
 - iii. the client application does not replay any authentication request with stored biometric data under any circumstance.
 - iv. the client application is audited by information systems auditor(s) certified by STQC / CERT-IN and compliance audit report is submitted to UIDAI. All Sub-AUAs shall also access authentication services only through duly audited client applications.

All AUAs are required to implement the above mentioned points in their current or future authentication application as well as their sub-AUAs (if any) application at the earliest.

2. Before appointment of any sub-AUA, the AUA shall take permission from UIDAI for the appointment of such sub-AUA. The AUAs which have already appointed sub-AUA(s) also need to take permission for the same from UIDAI before 31st March 2017.
3. As per Regulation number 15(2) of Aadhaar (Authentication) Regulations, 2016, sharing of license key is prohibited in case of e-KYC authentication. The e-KYC User Agency (KUA) shall use e-KYC authentication facility in the manner as prescribed in Regulation number 16 of the said regulations.
4. AUA / KUA shall be fully responsible for the misuse and illegal sharing of the license key in production or pre-production environment of UIDAI. AUA / KUA shall not allow any other agency to perform authentication by sharing their license key. AUA / KUA shall not forward authentication request using PID block captured by unaudited application using their license key. For every sub-AUA, a separate license key shall be used.
5. In case, Authority notices misuse or illegal sharing of license key by the AUA / KUA / sub-AUA, Authority shall terminate the license of the AUA / KUA and other actions including criminal prosecution shall be taken against AUA / KUA as well as the sub-AUA and other entities as per Aadhaar Act and its Regulations.
6. AUA / KUA shall not perform any test transactions on UIDAI's production environment. Any test transaction may be performed on UIDAI's pre-production environment only.
7. In all authentication applications deployed by AUA / KUA and sub-AUA, name of AUA / KUA shall be clearly displayed to the Aadhaar number holder.

All the AUAs / KUAs are hereby required to ensure compliance of the above mentioned points and send the compliance audit report and a certificate as per attached proforma duly signed by the Chief Executive Officer or equivalent of the company by 31st March 2017. It may please be noted that failure to send audit report and the certificate by 31st March 2017 will result in immediate deactivation of license key without any further notice, and will be considered violation of the Aadhaar Act, 2016 and UIDAI shall take necessary action as per the Aadhaar Act, 2016 and may impose disincentives including termination of license of the AUA / KUA.


(Ajai Chandra)
Assistant Director General

Certificate to be given by AUA / KUA

| S.No. | Description | Remarks |
|-------|--|---|
| 1 | The authentication application being used by AUA for the purpose of authentication is developed and digitally signed by AUA | Yes / No |
| 2 | The authentication application does not store and/or replay stored biometric data. | Yes / No |
| 3 | Biometrics/PID block is captured and encrypted at the front end device / client level | Yes / No Front end device / Client level |
| 4 | Sub-AUAs are using authentication services through application duly audited by the AUA | Name of Sub AUA: Yes / No 1. 2. |
| 5 | Audit of the authentication application by STQC/CERT-IN certified information system auditor(s), and audit compliance report shared with UIDAI | Yes / No; Date of Audit: Date of compliance report sent to UIDAI: |
| 6 | Permission from UIDAI for all sub-AUAs mentioned in point number 4 above | Name of Sub AUA: Date of permission 1. 2. |
| 7 | Sharing of e-KYC data with other entities in compliance with Regulation number 16 of Aadhaar (Authentication) Regulations, 2016 | Name of the entity: 1. 2. |

It is certified that the information provided above and all its particulars have been verified by all the directors/partners/concerned officers and each one of them shall be jointly and severally liable for any discrepancy in the information supplied herein above as may be found by the Authority.

Dated:

Chief Executive Officer
Name of the Company

File No. K-11020/44/2012-UIDAI (Auth)
Government of India
Unique Identification Authority of India

9th Floor, Tower I,
Jeevan Bharati Building
Connaught Circus
New Delhi – 110001
Dated: 28.02.2017

To

All AUAs / KUAs

Subject: Procurement of Registered Devices for Aadhaar authentication

Dear Partner,


Please refer to this office letter no K-11020/44/2012-UIDAI (Auth-I) dated 25th Jan 2017 wherein it was informed that with effect from 1st June 2017 authentication request will be accepted only through registered devices. In this direction, UIDAI is working closely with various device manufacturers/vendors and STQC for smooth transition to the registered device regime. UIDAI is pleased to inform that the specifications for Registered Devices (Level 0) have been published on 22nd Feb 2017 and the specifications for Level 1 will be published soon.

2. STQC will launch the registered device certification scheme on 15th March 2017 following which device of vendors will be able to get their registered devices certified from STQC as and when they are ready. On our part, UIDAI is closely working with various device vendors for development and testing of registered devices.

3. You are therefore advised that any fresh procurement of biometric device should be of registered devices only. In case, you need to procure the device before the certification of registered devices, please ensure to take an undertaking from the device vendor for upgradation to registered devices, Level 0 or Level 1 at the cost of vendor as per your functional requirements.

4. A proforma for such undertaking is enclosed for your ready reference.

Encl: As above.


(Ajai Chandra)
Assistant Director General

TO BE OBTAINED ON DEVICE VENDOR/COMPANY LETTER HEAD

UNDERTAKING

I _____ (Name & Designation) hereby undertake that _____ number of biometric devices are being supplied to M/s _____ (Purchaser) _____ against Purchase Order No. -----dated ----- for use of Aadhaar authentication.

We have seen the Registered Device specifications published by UIDAI and we are confident to get STQC certificate as per these specifications.

I _____ (Name & Designation) further undertake that these devices will be upgraded to Registered Devices at least Level 0 without any additional cost to M/s _____ (purchaser) _____ before 1st June 2017.

Date:

Name _____

Designation _____

Company _____

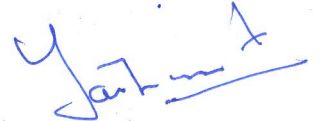
सं.के-11020/198/2017- यूआईडीएआई (ऑथ-II)
भारत सरकार
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)
ऑथेंटिकेशन डिवीज़न

जीवन भारती भवन, टॉवर I, नवां तल,
कनॉट सर्कस, नई दिल्ली -110001
दिनांक: 16.05.2017

परिपत्र

Reference is invited to this office circular issued vide No. K-11020/44/2012-UIDAI (Auth) dated 12.04.2017 circulating therewith the Application for Biometric Device Certification under Regulation 8(1) of Aadhaar (Authentication) Regulations, 2016 and the undertaking.

The Competent Authority has approved the revised version of the Undertaking to be submitted alongwith Application and STQC certificate issued for the said device model for obtaining UIDAI certification. The revised version of the Undertaking is enclosed herewith.


(यशवंत कुमार)

सहायक महानिदेशक

दूरभाष : 011-23462606

संलग्नक: जैसा उपर कहा गया है।

To

1. DG STQC
2. All AUAs/KUAs and ASAs
3. STQC Certified Device Providers
4. All Regional Office UIDAI and Tech Centre, Bengaluru

**Application for Biometric Device Certification under Regulation 8(1) of
Aadhaar (Authentication) Regulations, 2016**

| | |
|---|--|
| Organization Details | |
| Name of the Device Provider | |
| Registered Office address | |
| Correspondence address | |
| Management Point of Contact | |
| Technical Point of Contact | |
| Webpage link, e-mail address, Helpdesk number | |
| Details of Service Centers in India | |
| Name and address of OEM | |
| Device Details | |
| Device Make and Model | |
| Type of device (Fingerprint/Iris) | |
| Details of device | |
| End of Service date <i>(End of Service date would mean the date by which the device provider will provide technical support to the purchasers)</i> | |
| STQC Certification details | |
| Type of Registered Device (Level 0 / Level 1) | |
| Certified for Operating Systems | |
| STQC Certification number | |
| Date of issue of STQC certification | |
| Certification is valid up to (date) | |

Undertaking

This Undertaking is executed by (Device provider name), a <nature of constitution of the biometric authentication device provider>, having its registered office/principal place of business at <insert the registered office or principal place of business>duly represented by its authorized representative <insert the name of the authorized signatory>

By this writing, the undersigned on behalf ofaffirms, declares and undertakes the following:

1. That (Device provider name) is desirous to receive UIDAI certification for its biometric device as specified in the application enclosed herewith.
2. That (Device provider name) hereby declares that it is fully aware and understands the provisions of The Aadhaar (Targeted Delivery of Financial And Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act, 2016) and its Regulations made thereunder and undertakes that it shall at all times abide by the same.
3. That (Device provider name) is also fully aware that it shall be liable for penal provisions, as applicable for any contravention of the Aadhaar Act 2016 and any regulations made thereunder.
4. That (Device provider name), after the receipt of UIDAI certification, shall implement all changes in all biometric devices or its software which may be required by UIDAI from time to time for the purposes of security, improving the performance parameters etc. as per device specifications issued by UIDAI from time to time till the End of Service date.
5. That (Device provider name) undertakes to provide support to the entity to which it has supplied the biometric devices and shall keep the device certification and authorization/approval from UIDAI valid for all the biometric device models in use for Aadhaar Authentication till declared End of Service (EOS) date for the device. Provided that in case, the (Device provider name) are not able to obtain the certification and approval from UIDAI for the updated specifications, the (Device provider name) undertakes to replace such

biometric devices with the new UIDAI certified biometric devices at no additional cost to the purchaser, for the sale concluded on or after 15th March 2017.

6. That (Device provider name) is fully aware that it shall be liable to an appropriate amount which shall be mutually decided between us and AUA /KUA, in case:

- it is discovered that the device provider private key has been compromised due to incorrect or buggy implementation or due to negligence on the part of management server setup and administration.
- it is discovered that the device key has been compromised due to a defect or backdoor or lack of proper security implementation within the Registered Device(RD) service.
- it is discovered that the biometric replay/injection is possible within RD service due to a defect or a backdoor or lack of proper implementation of RD service.

UIDAI shall have no role and / or liability in any condition.

7. That the (Device provider name) understands and agrees that the UIDAI shall have the right to audit the biometric device provider manufacturing facility and continuously monitor and audit the performance and security of all devices in production. Based on this monitoring / audit, UIDAI may decide to temporarily suspend any individual device model from the ecosystem. In the event of temporary suspension, the (Device provider name) undertakes to resolve the identified issue within time period as specified by UIDAI, failing which the UIDAI certification of device model may be permanently revoked for which the (Device provider name) undertakes to replace all such devices in use in field with UIDAI certified devices at its own cost. The inspection/audit report will remain confidential between UIDAI and the device provider.

8. That the (Device provider name) affirms and declares that the information filled up in the application form and that this undertaking was placed before the board of directors / partners of the (Device provider name) in its meeting dated _____ and has been read over and verified to be true and correct.

9. That no particulars have been concealed and upon verification of the application, the board / partners have approved the same for submission at the hands of _____. Any change in the name, contact details, addresses etc. as filled up in this application form shall also be immediately conveyed to UIDAI.
10. That the board resolution / minutes of the meeting dated _____ approving the application form and authorizing _____ to submit the same is/are being annexed herewith as Document No. 1.
11. That the application form being duly filled up and all its particulars being verified by all the directors / partners each one of them shall be jointly and severally liable for any discrepancy in the information supplied herein above and as may be found by the authority.

This undertaking is being executed on thisday of2017 at

(Authorized signatory)

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

सं.के-11020/198/2017- यूआईडीएआई (ऑथ-II)
भारत सरकार
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)
ऑथेंटिकेशन डिवीज़न

जीवन भारती भवन, टॉवर I, नवां तल,
कनॉट सर्कस, नई दिल्ली -110001
दिनांक: 22.05.2017

परिपत्र

Subject: Clarification for biometric devices whose STQC certificate is already expired

Unique Identification Authority of India (UIDAI) has introduced Registered Devices for the purpose of biometric authentication. The use of public devices will be discontinued after 31st May 2017 and only the Registered Devices will be allowed to perform Aadhaar authentication. All devices presently deployed in the field by various Authentication User Agencies (AUAs) are required to be upgraded to Registered Devices.


2. For getting Registered Device certification, a biometric device vendor should have valid STQC certificate for public device as per UIDAI's biometric device specifications and in addition, biometric device vendors need to develop RD service (registered device service) for their existing device models, and need to get biometric device RD service certified by STQC and UIDAI.

3. It has come to the notice that there are some public device models deployed in the field whose public device STQC certification has already expired. Since, valid STQC certificate of public device is a mandatory requirement for certification of Registered Device, such devices are facing difficulty in getting RD service certification as per existing policy. Therefore, in order to ensure that such devices whose public device STQC certification has expired also get upgraded to RD, following clarifications/directions are issued:

- i. RD certification will be allowed for devices whose public device STQC certification has expired. For this, device vendors can apply to STQC for RD services certification after depositing necessary fees and documents required for –
 - a. RD service certification
 - b. Re-certification as per STQC published procedure for maintenance of certification.

Y. J. K.

- ii. In case supplier of a certified device is not interested for upgrading the device to L0 (RD Service Certification), any other device provider may also apply for Registered Device services certification for such type of devices, subject to production of No Objection Certificate (NoC) from the STQC test report owner (original supplier/manufacturer).
- iii. This RD service certification will be valid only for up-gradation of the existing public devices to Registered Device and not for sale of new devices. Therefore, vendor will not be able to sell new devices based upon this RD service certificate only, unless they obtain quality and accuracy certificate from STQC. However, they may initiate action in parallel for these activities.
- iv. After satisfactory completion of STQC - UIDAI testing for RD service, vendor will submit prescribed undertaking for UIDAI certificate for deploying RD service.
- v. Vendor will be responsible for ensuring that the quality and accuracy specifications of all the devices, being upgraded to Registered Devices, continue to comply with the specifications of public devices.


(यशवंत कुमार)

सहायक महानिदेशक

दूरभाष : 011-23462606

To

1. DG STQC
2. All AUAs/KUAs and ASAs
3. STQC Certified Device Providers
4. Tech Centre, Bengaluru

File no. K-11020/44/2012-UIDAI (Auth-I)
Government of India
Unique Identification Authority of India

9th Floor, Tower I,
Jeevan Bharati Building
Connaught Circus
New Delhi – 110001

Dated: 24th May 2017

CIRCULAR

Reference is invited to this office letter no. K-11020/44/2012-UIDAI (Auth-I) dated 25.01.2017 sent to all Authentication User Agencies (AUAs), Authentication Service Agencies (ASAs) and all STQC certified device providers. It was intimated that all AUAs and ASAs will implement authentication API 2.0 for Aadhaar authentication and the device providers will get their devices certified as Registered Device by 31st May 2017. The specifications for Registered Devices were issued by UIDAI on 22.02.2017 which was followed by STQC guidelines for Registered Devices certification process on 27.02.2017. UIDAI vide its circular no K-11020/44/2012-UIDAI (Auth-I) dated 12.04.2017 also circulated the application form and the undertaking to be given by device providers for obtaining Registered Device certification.

2. In response to the above mentioned circulars and guidelines, twenty two device providers have applied to STQC for RD service certification. At the same time, Auth API 2.0 specifications have also been communicated to all AUAs and ASAs. During the period of last four months UIDAI and STQC have held a series of workshops and handholding meetings with AUAs, ASAs and device providers at UIDAI HQ as well as at UIDAI Tech Center, Bengaluru.

3. UIDAI has started issuing RD certification to those device providers who have obtained RD service certification from STQC and have submitted their application to UIDAI. It is noticed that while a number of device providers are in the process of getting Registered Device service certification from STQC, some device providers are not yet ready with their Registered Device service. Similarly, whereas a large number of AUAs and ASAs have successfully tested Auth API 2.0 with certified Registered Device, others are at various stages of development. Further, a number of representations have been received from certain AUAs regarding their logistical

limitations for upgrading all of their existing public devices to Registered Devices by 31st May 2017.

4. It is to be understood that Registered Device is a critical requirement for enhanced security and privacy in the Aadhaar authentication eco-system. Therefore, it is imperative that all stakeholders viz. AUAs, ASAs and device providers fulfill the necessary requirements in a time bound manner. However, given the status of preparedness of AUAs, ASAs and device providers as per para 3 above, these entities are directed to fulfill the following requirements:

AUA Requirements:

AUAs shall upgrade to Authentication API 2.0, KUAs shall upgrade to eKYC API 2.1 and authentication application to the registered device compliance by 31st May 2017 and in case they are not able to do so the authentication services will be allowed subject to following conditions:

- i. AUAs shall be completely responsible for ensuring security of the applications if they continue to use existing non-registered devices after 31st May 2017
- ii. AUAs shall complete at least one successful authentication transaction in Pre-production using registered device by 31st July 2017
- iii. AUAs shall pay Rs 0.20 per authentication transaction w.e.f. 1st August 2017 for using existing non-registered devices
- iv. No authentication transactions using existing non-registered devices shall be allowed after 30th September 2017

AUAs using Aadhaar authentication services with existing non-registered devices after 31st May 2017 shall be deemed to have accepted above mentioned conditions.

ASA Requirements:

ASAs must upgrade their system to support registered devices by 31st May 2017 and in case they are not able to do so the authentication services will be allowed subject to following conditions:

- i. ASAs shall complete at least one successful authentication transaction in Pre-production using registered device by 30th June 2017
- ii. ASAs shall upgrade to support registered device transaction on production by 31st July 2017
- iii. ASAs shall pay Rs 0.10 per authentication transaction done with non-registered devices w.e.f 1st August 2017
- iv. UIDAI shall recover the transaction charges from ASAs for authentications done with non-registered devices w.e.f. 1st August 2017 with respect to liabilities of both ASA and the AUAs using its services. UIDAI will raise the bill for AUAs to ASAs only and it will be the responsibility of ASAs to collect charges from their AUAs and pay to UIDAI.
- v. No authentication transactions using existing non-registered devices shall be allowed after 30th September 2017

ASAs using Aadhaar authentication services with existing non-registered devices after 31st May 2017 shall be deemed to have accepted above mentioned conditions.

Device Provider Requirements:

Device providers shall get their devices certified as registered devices by 31st May 2017 and in case they are not able to do so their device certification will be allowed subject to following conditions:

- i. Device providers shall get provisional certification of their devices by 15th July 2017
- ii. Provisional certification scheme expires on 15th July 2017 and device providers agree to pay Rs 10,000 per day for any delay thereafter

5. In this regard, attention is invited to Regulations 8(1), 14(d), 14(n) and 19(o) of Aadhaar (Authentication) Regulations, 2016, whereby, device providers, AUAs and ASAs are required to employ only those devices, equipment, or software, which are duly registered with or approved or certified by the Authority and also comply with any contractual terms, regulations, policies, procedures, specifications, standards and directions issued by the Authority, for the purposes of using the authentication

facilities provided by the Authority. Violation of these Regulations constitutes criminal offence under section 42 and 43 of the Aadhaar Act, 2016 punishable with imprisonment and fine.

Therefore, all AUAs, ASAs and device providers are again directed to take necessary action at their end to implement Registered Device services.



(Ajai Chandra)
Assistant Director General

F. No. K-11022/630/2017-UIDAI (Auth-II)
Unique Identification Authority of India
Government of India

9th Floor, Tower I,
Jeevan Bharati Building
Connaught Circus
New Delhi – 110001

Dated: 31st May 2017

CIRCULAR

The Aadhaar (Authentication) Regulations, 2016 under the Aadhaar Act, 2016 have been notified on 12th September 2016. Regulations 12, 24 and 25 of ibid Regulations provide for appointment of Authentication User Agencies (AUAs), e-KYC User Agencies (KUAs) and Authentication Service Agencies (ASAs), provisions for continuation of existing entities and imposition of disincentives for contravention of provisions of the Aadhaar Act, 2016 and its Regulations, Agreements etc.

2. The Authority in exercise of the provisions of the Regulations 12(1) and 12(2) of Aadhaar (Authentication) Regulations, 2016, has approved the Agreements for the AUAs, KUAs and ASAs to avail Aadhaar authentication services provided by UIDAI. This inter alia includes schedule of disincentives, depositing of bank guarantee, levying of license fees etc. The Agreements viz. Authentication User Agency Agreement v4.0, Authentication Service Agency Agreement v4.0, set of applications and appointment letters are available on UIDAI website.

3. In view of the decisions taken by the Authority, following directions are issued for compliance by AUAs, KUAs and ASAs:

- i. Existing AUAs and KUAs: The entities who have already signed Agreement with UIDAI and are availing authentication service either in pre-production or production or both shall be required under Regulation 24(2) of Aadhaar (Authentication) Regulations, 2016 to fulfill following requirements:
 - a. The entities availing the production environment facility for authentication shall be required to deposit license fees of Rs 20 lakh which shall be valid for 2 years w.e.f 1st June 2017.
 - b. The entities availing pre-production environment facility shall be required to deposit license fees of Rs 5 lakh which shall be valid for 3 months w.e.f 1st June 2017. The entities which desire to continue using pre-production facility beyond 3 months shall be required to renew their pre-production license key after depositing license fees of Rs 5 lakh each time which shall again be valid for a period of 3 months.

If an existing AUA or KUA, in either pre-production or production or both environments, continues to use Aadhaar authentication services beyond 15th June 2017, it shall be deemed to have agreed to the terms and clauses of the AUA Agreement v4.0 and shall be required to deposit the license fees and bank guarantee by 30th June 2017. In case it does not agree with the terms and clauses of the Agreement, it may discontinue use of Aadhaar authentication

services and shall intimate to UIDAI by 15th June 2017 for termination of their Agreement as per Regulations 24(3) and 24(4) of Aadhaar (Authentication) Regulations, 2016.

- ii. Existing ASAs: The ASAs who have already signed agreement with UIDAI and are availing authentication service either in pre-production or production or both shall be required under Regulation 24(2) of Aadhaar (Authentication) Regulations, 2016 to fulfill following requirements:

- a. The ASAs availing the production environment facility for authentication shall be required to deposit a license fees of Rs 1 crore which shall be valid for 2 years w.e.f 1st June 2017.
- b. The ASAs availing pre-production environment facility shall be required to deposit license fees of Rs 10 lakh which shall be valid for 3 months w.e.f 1st June 2017. The ASAs which desire to continue using pre-production facility beyond 3 months shall be required to renew their pre-production license key after depositing license fees of Rs 10 lakh each time which shall again be valid for a period of 3 months.

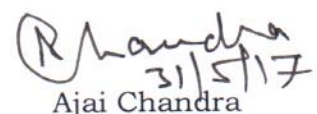
If an existing ASA, either in pre-production or production or both environments continues to use ASA services beyond 15th June 2017, it shall be deemed to have agreed to the terms and clauses of the ASA Agreement v4.0 and shall be required to deposit the license fees and bank guarantee by 30th June 2017. In case it does not agree with the terms and clauses of the Agreement, it may discontinue use of Aadhaar authentication services and shall intimate to UIDAI by 15th June 2017 for termination of their Agreement as per Regulations 24(3) and 24(4) of Aadhaar (Authentication) Regulations, 2016.

4. The above mentioned license fee is non-refundable under any circumstances including but not limited to the event of the entity (AUA/KUA/ASA) closing its business before the period for which fee has been paid or in case the Authority cancels the License / Agreement.

5. UIDAI has received a number of applications for appointment as AUAs and ASAs, which are yet to be approved or pending for Agreement signing. The application fees for such cases shall be returned and these entities will be required to apply afresh as per new format.

6. Bank Guarantee of Rs 25 lakh for AUAs and Rs 50 lakh for ASAs shall be valid for a period of 10 years from the date of signing of the agreement for new entities. In case of existing entities agreeing to continue authentication services, the bank guarantee shall be valid for period of 10 years w.e.f 1st June 2017.

7. The completed Application Form, License Fee and Bank Guarantee alongwith the required documents may be submitted to Deputy Director (Authentication) 9th Floor, Tower-1, Jeevan Bharati Building, Connaught Circus, New Delhi - 110001.


31/5/17

Ajai Chandra
Assistant Director General

File No. K-11020/198/2017-UIDAI (Auth-I)
Government of India
Unique Identification Authority of India

9th Floor, Tower 1
Jeevan Bharti Building
Connaught Circus
New Delhi-110001

Dated: 9th June 2017

CIRCULAR

Reference is invited to this office circular no. K-11020/198/2017-UIDAI (Auth-II) dated 16.05.2017 regarding UIDAI certification for Registered Device. It is pertinent to mention here that Registered Device service involves new specifications, introduction of HSM, device key rotation etc and it is possible that after their deployment in the field small enhancements may be required. Such enhancements may not require undergoing complete certification and testing procedure again.

2. Therefore, the Competent Authority has approved the Delta Certification Process for certification of Registered Device service in case of small enhancements, which may be required in following scenarios:


- i. A bug identified in Registered Device service after it is provisionally certified.
- ii. Functionality enhancements which requires changes in the code and its MD5 checksum.
- iii. Any other reasons which will cause a change to the executable certified and hence its MD5 checksum e.g. change in the specifications which requires a change in the code and subsequently its MD5 checksum etc.

3. The above possible changes are categorized as following:

1. **Category 1:** No changes to the solution architecture/traceability matrix:

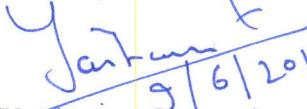
For such cases Device provider will submit the details of the changes to STQC, which shall be reviewed and decided by Solution Architecture Review Committee as to:

- a) If there are only minor changes to the solution/code it may approve the change and allow Device provider to continue to have the certification.
- b) If there are major changes (without any change in solution architecture), the committee may obtain an undertaking from the Device provider stating there are no architectural changes to the solution and allow them to continue to have the certification. If the committee finds major changes with or without any change in the solution architecture, it may push the case to the category 2 as below.


9/6/2017

2. **Category 2:** Changes to the solution architecture/traceability matrix:
For such cases Device provider will submit the revised solution architecture and details of changes to STQC, which shall be reviewed by Solution Architecture Review Committee. The Committee will decide whether complete certification process needs to be repeated or a part of it. Accordingly, device provider would need to again undergo the tests/process etc. and obtain fresh certification from STQC and UIDAI.

All Device Vendors are hereby directed to follow the above mentioned procedure for Delta Certification.


9/6/2017

(Yashwant Kumar)

Assistant Director General (Auth)

To

1. DG STQC
2. All AUAs/KUAs and ASAs
3. STQC Certified Device Providers
4. Tech Centre, Bengaluru

सं.के-11020/204/2017- यूआईडीएआई (ऑथ-1)

भारत सरकार

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथेंटिकेशन डिवीज़न

जीवन भारती भवन, टॉवर I, नवां तल,

कनॉट सर्कस, नई दिल्ली -110001

दिनांक: 22.06.2017

Circular

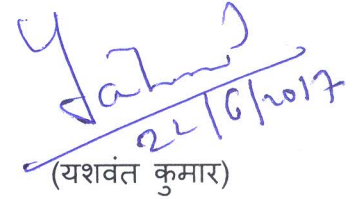
UIDAI offers two types of Authentication facilities viz. Yes/No authentication and e-KYC authentication. Authentication devices deployed by Authentication User Agency / e-KYC User Agency (AUA/KUA) initiate the authentication request and create encrypted PID block before forwarding it to authentication server of AUA/KUA for processing of domain specific transaction and creation of auth XML as per UIDAI authentication API. Further, upon receiving the auth XML from AUA, Authentication Service Agency (ASA) forwards it to CIDR. To ensure the integrity and non-repudiation, Authentication Server at CIDR, as a mandatory requirement, accepts only digitally signed auth XML through ASA. As mentioned in authentication API document and Regulation 9(2) of Aadhaar (Authentication) Regulations, 2016, *"Authentication request shall be digitally signed by the requesting entity (AUA/KUA) and/or by the Authentication Service Agency, as per the mutual agreement between them"*.

2. In e-KYC service, UIDAI encrypts the e-KYC response data using KUA public key and subsequently forwards the encrypted response to KUA. On receiving the encrypted response, the KUA decrypts the data using their own private key.

3. To further enhance the security of Aadhaar authentication eco-system, under Regulations 14(n) and 19(o) of Aadhaar (Authentication) Regulations, 2016, it is hereby decided to mandatorily use Hardware based Security Module (HSM) for digital signing of Auth XML and decryption of e-KYC data.

4. For digital signing of Auth XML, Authentication request shall be digitally signed by the requesting entity (AUA/KUA) and/or by the ASA using HSM, as per the mutual agreement between them. However, to decrypt the e-KYC response data received from UIDAI, the KUA shall necessarily use its own HSM. The HSM to be used for signing Auth XML as well as for e-KYC decryption should be FIPS 140-2 compliant.

5. Therefore, all AUA/KUA/ASA shall ensure the implementation of HSM in Aadhaar authentication services in aforesaid manner before 31st August, 2017 and submit the compliance report. Any non-compliance in this regard will amount to violation of Aadhaar Act, 2016, its Regulations and AUA / ASA Agreement (including schedule of financial disincentives) making the concerned liable for appropriate penal action as provided therein which shall be in addition to any other legal action as per relevant laws.


(यशवंत कुमार)

सहायक महानिदेशक

दूरभाष : 011-23462606

To

1. All AUAs/KUAs and ASAs.
2. UIDAI Tech Center, Bengaluru

F-No. K-11022/460/2016-UIDAI (Auth-II)
Unique Identification Authority of India
Government of India

9th Floor, Tower I,
Jeevan Bharati Building
Connaught Circus
New Delhi-110001

Dated: 06.07.2017.

To

All AUAs/KUAs

Subject: Appointment of Sub-AUA.

This is in continuation to this office letter F-No. K-11022/460/2016-UIDAI (Auth-II) dated 28.02.2017 where in all AUAs were asked to take permission from UIDAI before appointment of an entity as their Sub-AUA. Further, the AUAs were required to take permission for already appointed Sub-AUAs.

In this regard all AUAs are required to submit their request for appointment of an entity as Sub-AUA.

The draft copy of letter, application form and undertaking is attached.



(Gracy James)
Deputy Director

Letter Head of AUA

To,
Deputy Director (Authentication)
9th Floor, Tower I,
Jeevan Bharati Building
Connaught Circus
New Delhi-110001

Subject: Appointment of M/s _____ as Sub-AUA.

This is w.r.t. UIDAI letter No. F-No. K-11022/460/2016-UIDAI (Auth-II) dated 28-02-2017 where in AUAs were asked to take permission from UIDAI before appointment of an entity as Sub-AUA.

In this regard we request you to grant permission for appointment of M/s _____ as Sub-AUA.

Thanks & Regards
(Authorized Signatory)

Name
Designation
Mobile no.

Enclosure: 1. Application Form along with Undertaking

**Application for SUB AUA under Regulation 15 of Aadhaar
(Authentication) Regulations, 2016**

| Sub AUA Organization Details | |
|---|----------|
| Name of the Sub AUA | |
| Sub AUA Code | |
| Registered Office address | |
| Correspondence address | |
| Management Point of Contact | |
| Technical Point of Contact | |
| Purpose for which Authentication Services will be used. | 1. 2. |

(Authorized signatory: Sub-AUA)

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

All the details mentioned above are verified by AUA

(Authorized signatory: AUA)

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

Joint Undertaking

We (AUA Organization name) intend to appoint (Sub AUA organization name) as Sub Authentication User Agency (Sub AUA) and both of us are fully aware and understand the provisions of The Aadhaar (Targeted Delivery of Financial And Other Subsidies, Benefits and Services) Act, 2016 and Regulations made thereunder and further warrant that we shall at all times abide by the same.

We (AUA Organization name) and (Sub AUA organization name) jointly and severally certify that the information filled up in the application form and supplied therewith has been read over and verified to be true and correct to our personal knowledge and belief and no particulars have been concealed.

By this writing, the undersigned on behalf of (AUA Organization name) and (Sub AUA Organization name) affirm, declare and undertake the following:

1. We (AUA Organization name) shall ensure that the Aadhaar authentication services are used by Sub AUA (Sub AUA Organization name) only for the purpose as mentioned in the application form.
2. (AUA Organization name) shall create separate License Key and assign unique Sub-AUA code to the Sub-AUA (Sub AUA Organization name), which shall not further be shared with any other person or entity for any purpose.
3. (AUA Organization name) shall ensure that the Sub AUA (Sub AUA Organization name) complies with the provisions of the Aadhaar Act, 2016 and its Regulations, processes, standards, guidelines, specifications and protocols of the Authority that are applicable to the requesting entity.
4. We, (AUA Organization name) and (Sub AUA Organization name) shall be jointly and severally liable for non-compliance of the Aadhaar Act, 2016 and its Regulations, processes, standards, guidelines and protocols of the Authority and shall be liable for disincentives and penalties as per the schedule of disincentives of AUA agreement and other provisions of the Aadhaar Act, 2016 and its Regulations.
5. We (AUA Organization name) shall ensure that the client application to be used for Aadhaar authentication is developed and digitally signed by us OR Sub-AUA (Sub AUA Organization name) shall integrate digitally signed SDK developed by us in their client application for

capturing Aadhaar information like Aadhaar number, biometric details, demographic details etc.

6. (AUA Organization name) shall ensure that the (Sub AUA Organization name) client application or SDK, as the case may be, for Aadhaar authentication is audited, at the time of appointment of (Sub AUA Organization name) and also every year thereafter, by information systems auditor(s) certified by STQC / CERT-IN and compliance audit report is submitted to UIDAI
7. (AUA Organization name) and (Sub AUA Organization name) have ensured that the declared information filled up in the application form as well as this undertaking was placed before the board of directors / partners of our respective organizations in their meetings dated _____ and dated _____ and has been read over and verified to be true and correct.
8. No particulars have been concealed and upon verification of the application, the board / partners have approved the same for submission at the hands of _____. Any change in the name, contact details, addresses etc. as filled up in this application form shall also be immediately conveyed to UIDAI.
9. The board resolutions / minutes of the meetings dated _____ and dated _____ approving the application form and authorizing _____ to submit the same are being annexed herewith.
10. The application form having been duly filled up and all its particulars having been verified by all the directors / partners, each one of them shall be jointly and severally liable for any discrepancy in the information supplied herein above and as may be found by the authority.

This undertaking is being executed on this _____ day of _____ 2017 at _____.

| | |
|---|---|
| <p>Authorized signatory of (AUA Organization name)</p> <p>Signature: _____</p> <p>Name: _____</p> <p>Designation: _____</p> <p>Organization: _____</p> <p>Date: _____</p> | <p>Authorized signatory of (Sub AUA Organization name)</p> <p>Signature: _____</p> <p>Name: _____</p> <p>Designation: _____</p> <p>Organization: _____</p> <p>Date: _____</p> |
|---|---|

भारत सरकार

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथेंटिकेशन डिवीजन

जीवन भारती भवन, टॉवर I, नवां तल,

कनॉट सर्कस, नई दिल्ली -110001

दिनांक: 25.07.2017

Circular

Aadhaar Number is being used as primary ID of the residents by various user organizations like Banks, Telecoms, Government departments, Income Tax department, Private Sectors, etc. To avail the different benefits/services, Aadhaar Number Holder has to share the Aadhaar Number to various entities and the entities store the Aadhaar Numbers as reference key to deliver their services/benefits.

In order to enhance the security level for storing the Aadhaar numbers, it has been mandated that all AUAs/KUAs/Sub-AUAs and other entities that are collecting and storing the Aadhaar number for specific purposes under the Aadhaar Act 2016, shall start using Reference Keys mapped to Aadhaar numbers through tokenization in all systems.

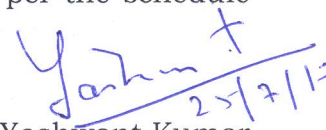
The course of action to implement the process by all AUAs/KUAs/Sub-AUAs and other entities is hereby outlined as below:

- (a) All entities are directed to mandatorily store Aadhaar Numbers and any connected Aadhaar data (e.g. eKYC XML containing Aadhaar number and data) on a separate secure database/vault/system. This system will be termed as "Aadhaar Data Vault" and will be the only place where the Aadhaar Number and any connected Aadhaar data will be stored.
- (b) Entities are allowed to store any relevant demographic data and/or photo of the Aadhaar Number Holder in other systems (such as customer database) as long as Aadhaar Number is not stored in those systems.
- (c) Each Aadhaar number is to be referred by an additional key called as Reference Key. Mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault.
- (d) All business use-cases of entities shall use this Reference Key instead of Aadhaar number in all systems where such reference key need to be stored/mapped, i.e. all tables/systems requiring storage of Aadhaar numbers for their business transactions should from now onwards maintain only the reference key. Actual Aadhaar number should not be stored in any business databases other than Aadhaar Data Vault.
- (e) Access to Aadhaar Data Vault shall be made secure and accessed through internal systems only.

Y. Jaiswal
25/7/17

- (f) The Aadhaar number and any connected data maintained on the Aadhaar Data Vault shall always be kept encrypted and access to it strictly controlled only for authorized systems. Keys for encryption are to be stored in HSM devices only.
- (g) Aadhaar numbers along with connected data if any (such as eKYC XML containing Aadhaar numbers and demographic data) shall only be stored in a single logical instance of Aadhaar Data Vault with corresponding reference key. Appropriate HA/DR provisions may be made for the vault with same level of security.
- (h) The Aadhaar Data Vault containing Aadhaar number/data and the referencing system must be kept in a highly restricted network zone that is isolated from any untrusted zone and other internal network zones.
- (i) Only trusted communications must be permitted in and out of the vault. This should ideally be done via API/Micro-service dedicated to get the mapping and controlling access to the API/Micro-service at application level. Any authorized users needing to access this mapping must go via applications allowing them to view/access this data with appropriate user authentication and logging.
- (j) The Aadhaar Data Vault must implement strong access controls, authentication measures, monitoring and logging of access and raising necessary alerts for unusual and/or unauthorized attempts to access.
- (k) The Aadhaar Data Vault should support mechanisms for secure deletion/update of Aadhaar number and corresponding data if any as required by the data retention policy of the entities.
- (l) The chosen Reference Key generation method is to ensure that the recovery of the original Aadhaar number must not be computationally feasible knowing only the reference key or number of reference keys. It is suggested that a UUID (Universally Unique Identifier represented via hex string) scheme be used to create such reference key so that from such reference key, Aadhaar number can neither be guessed nor reverse engineered.

Therefore in exercise of the provisions of Regulation 14(n) of the Aadhaar (Authentication) Regulations, 2016 and Regulations 5 and 6 of Aadhaar (Sharing of Information) Regulations, 2016, any non-compliance shall be dealt under Section 42 of the Aadhaar Act, 2016 and shall also attract financial disincentives as per the schedule of the AUA/KUA agreement.


 (Yashwant Kumar)
 Assistant Director General
 दूरभाष : 011-23462606

To

1. All AUAs/KUAs and ASAs.
2. UIDAI Tech Center, Bengaluru

File No. K-11022/667/2017-UIDAI (Auth-II)
Government of India
Unique Identification Authority of India
(Authentication Division)

9th Floor, Tower I, Jeevan Bharti Building,
Connaught Circus, New Delhi – 110001
Dated: 27th September, 2017

Circular

Subject: Whitelisting of Aadhaar based applications developed by AUAs, KUAs and Sub-AUAs

UIDAI provides Aadhaar authentication and e-KYC services to AUAs and KUAs. Various AUAs, KUAs and Sub-AUAs have developed Aadhaar based applications to extend authentication services to residents. However, it has been observed that a number of agencies who are not authorized by UIDAI have also developed applications which claim to do Aadhaar authentication and collect resident identity data in an unauthorized manner. Such activities pose grave threat to the privacy and security of residents' data.

2. Therefore, in order to protect identity information of residents, UIDAI has decided to whitelist all Aadhaar based Web / Android / iOS or any other client applications in public domain along with AUA / Sub-AUA name, application name, logo and URL etc. Residents may refer to these applications on UIDAI website before providing their identity information to the agency.

3. In this regard, UIDAI had sent an email to all AUAs/KUAs on 1st September, 2017 seeking details of their Aadhaar based applications along with logo, name of application, application URL etc. developed by them or their Sub-AUAs. A number of AUAs/KUAs have already provided these details, however some of the AUAs are yet to submit this information.

4. Therefore all AUAs/KUAs are requested to provide the information for all their applications by **10th October, 2017** as per the following format:

| Name of Agency | Name of Sub-AUA (if any) | Logo of Application | Name of Application | URL of Application | Type of Application (Android / iOS / Web etc.) |
|----------------|--------------------------|---------------------|---------------------|--------------------|--|
| | | | | | |
| | | | | | |

Please note that it shall be the responsibility of AUAs to provide details of applications developed by their Sub-AUAs.

5. It may be noted that any application not listed on UIDAI website shall be treated as unauthorized Aadhaar application. The failure to comply with these instructions will be considered as violation of Regulations 14(n) of Aadhaar (Authentication) Regulations, 2016 and shall attract penalties @ Rs 1 lakh per day as per clause 7.2 of AUA Agreement v4.0, termination of Agreement, including without limitation, criminal prosecution under sections 42 and 43 of the Aadhaar Act, 2016.


(Ajai Chandra)

Assistant Director General

सं.के-11020/44/2011-यूआईडीएआई(ऑथ-I)

भारत सरकार

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथेंटिकेशन डिवीज़न

जीवन भारती भवन, टॉवर I, नवां तल,
कनॉट सर्कस, नई दिल्ली -110001

दिनांक: 03.10.2017

6/10/17

CIRCULAR

Reference is invited to this office circular no. K-11020/44/2012-UIDAI (Auth-I) dated 24.05.2017 which notified the timelines for upgradation of all public biometric devices to Registered Devices. It was clearly mentioned that all Authentication User Agencies (AUAs) including e-KYC User Agencies (KUAs) and Authentication Service Agencies (ASAs) shall upgrade to Registered Device and no authentication transaction shall be allowed on non-Registered Devices after 30.09.2017. It was also mentioned in the notification dated 24.5.2017 that from 1.08.2017 to 30.09.2017 all non-Registered Device transactions shall be charged @ Rs 0.20 and Rs 0.10 for AUAs and ASAs respectively.

2. Whereas a number of AUAs and ASAs have upgraded to Registered Devices, UIDAI has received requests from certain entities that they need some more time to complete the transition.

3. Therefore it has been decided to extend the timeline for Registered Device implementation by one month i.e. up to 31.10.2017 subject to the condition that non-Registered Device transactions shall continue to be charged @ Rs 0.20 and Rs 0.10 for AUAs and ASAs respectively as per notification dated 24.05.2017. UIDAI will issue notices for recovery of these charges and delay in deposit of these charges shall attract compound interest @ 1.5% per month.

4. It is reiterated that Registered Devices ensure encryption of biometrics of residents at time of capture. Therefore, in order to protect privacy and biometrics of the residents, it is absolutely essential to use only the Registered Devices. Any further use of non-Registered Devices will be putting residents' privacy at risk. Therefore, all AUAs and KUAs are requested to upgrade to Registered Devices at the earliest.


(Virender Prasad)
Assistant Director General 6/10/17

To

1. All AUAs/KUAs & ASAs.
2. All STQC Certified Device Providers
3. Tech Centre

DO's FOR AADHAAR USER AGENCIES/DEPARTMENTS

1. Read Aadhaar Act, 2016 and its Regulations carefully and ensure compliance of all the provisions of the Aadhaar Act, 2016 and its Regulations.
2. Ensure that everyone involved in Aadhaar related work is well conversant with provisions of Aadhaar Act, 2017 and its Regulations as well as processes, policies specifications, guidelines, circular etc issued by UIDAI from time to time.
3. Create internal awareness about consequences of breaches of data as per Aadhaar Act, 2016.
4. Follow the information security guidelines of UIDAI as released from time to time.
5. Full Aadhaar number display must be controlled only for the Aadhaar holder or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked.
6. Verify that all data capture point and information dissemination points (website, report etc) should comply with UIDAI's security requirements.
7. If agency is storing Aadhaar number in database, data must be encrypted and stored. Encryption keys must be protected securely, preferably using HSMs. If simple spreadsheets are used, it must be password protected and securely stored.
8. Access controls to data must be in place to make sure Aadhaar number along with personally identifiable demographic data is protected.
9. For Aadhaar number look up in database, either encrypt the input and then look up the record or use hashing to create Aadhaar number based index.
10. Regular audit must be conducted to ensure Aadhaar number and linked data is protected.
11. Ensure that employees and officials understand the implications of the confidentiality and data privacy breach.

12. An individual in the organization must be made responsible for protecting Aadhaar linked personal data. That person should be in charge of the security of system, access control, audit, etc.
13. Identify and prevent any potential data breach or publication of personal data.
14. Ensure swift action on any breach personal data.
15. Ensure no Aadhaar data is displayed or disclosed to external agencies or unauthorized persons.
16. Informed consent - Aadhaar holder should clearly be made aware of the usage, the data being collected, and its usage. Aadhaar holder consent should be taken either on paper or electronically.
17. Authentication choice - When doing authentication, agency should provide multiple ways to authenticate (fingerprint, iris, OTP) to ensure all Aadhaar holders are able to use it effectively.
18. Multi-factor for high security - When doing high value transactions, multi-factor authentication must be considered.
19. Create Exception handling mechanism on following lines-
20. It is expected that a small percentage of Aadhaar holders will not be able to do biometric authentication. It is necessary that a well-defined exception handling mechanism be put in place to ensure inclusion.
21. If fingerprint is not working at all even after using multi-finger authentication, then alternate such as Iris or OTP must be provided.
22. If the schemes is family based (like PDS system), anyone in the family must be able to authenticate to avail the benefit. This ensures that even if one person is unable to do any fingerprint authentication, someone else in the family is able to authenticate. This reduces the error rate significantly.
23. If none of the above is working (multi-finger, Iris, anyone in family, etc.), then agency must allow alternate exception handling schemes using card or PIN or other means.
24. All authentication usage must follow with notifications/receipts of transactions.

25. All agencies implementing Aadhaar authentication must provide effective grievances handling mechanism via multiple channels (website, call-center, mobile app, sms, physical-center, etc.).
26. Get all the applications using Aadhaar audited & certified for its data security by appropriate authority such as STQC/CERT-IN.
27. Use only STQC/UIDAI certified biometric devices for Aadhaar authentication.

DONT's FOR AADHAAR USER AGENCIES/DEPARTMENTS

1. Do not publish any personal identifiable data including Aadhaar in public domain/websites etc. Publication of Aadhaar details is punishable under Aadhaar act.
2. Do not store biometric information of Aadhaar holders collected for authentication.
3. Do not store any Aadhaar based data in any unprotected endpoint devices, such as PCs, laptops or smart phones or tablets or any other devices.
4. Do not print/display out personally identifiable Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate/any other certificate/document. Aadhaar number if required to be printed, Aadhaar number should be truncated or masked. Only last four digits of Aadhaar can be displayed/printed.
5. Do not capture/store/use Aadhaar data without consent of the resident as per Aadhaar act. The purpose of use of Aadhaar information needs to be disclosed to the resident.
6. Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity.
7. Do not locate servers or other IT storage system/ devices having Aadhaar data outside of a locked, fully secured and access-controlled room
8. Do not permit any unauthorized people to access stored Aadhaar data
9. Do not share Authentication license key with any other entity.

सं.के-11022/631/2017-यूआईडीएआई (ऑथ-II)

भारत सरकार

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथेंटिकेशन डिवीज़न

जीवन भारती भवन, टॉवर I, नवां तल,

कनॉट सर्कस, नई दिल्ली -110001


दिनांक : 27.11.2017

CIRCULAR

It has come to the notice of UIDAI that certain e-KYC User Agencies (KUAs) have been sharing the e-KYC data of the residents' with their Sub-AUAs and other entities by wrongly interpreting Regulation 16(2) of Aadhaar (Authentication) Regulations, 2016.

2. In exercise of the power conferred by Regulation 30 of the Aadhaar (Authentication) Regulations, 2016, UIDAI hereby clarifies that for sharing of e-KYC data with Sub-AUA or any other entity under Regulation 16(2), the KUAs shall obtain specific permission from UIDAI by submitting an application in this regard.

3. As per Regulations 14(n) of the Aadhaar (Authentication) Regulations, 2016, all KUAs shall comply with this circular with immediate effect and any non-compliance shall be dealt under Section 42 of the Aadhaar Act, 2016 and shall also attract financial disincentives as per the schedule of the AUA/KUA agreement.


(अजय चन्द्रा)

सहायक महानिदेशक(ऑथेंटिकेशन)

To

All KUAs

File No. K-11022/631/2017-UIDAI(Auth-II)
Government of India
Unique Identification Authority of India
Authentication Division

9th Floor, Tower-I, Jeevan Bharti Building,
Connaught Circus, New Delhi-110001

Date: 27th November 2017

CIRCULAR

Sub: Discontinuation of the provision of partial match in Demographic authentication

UIDAI at present provides the facility of both exact match and partial match in demographic authentication to Authentication User Agencies (AUAs). The AUAs generally configure the option of exact or partial match of name and/or address and/or other demographic parameters in their respective client applications. However, it is observed that some entities are using partial matching whereby part of the name or partial address etc. is sent to UIDAI for the purpose of authentication. Such practice while may improve the authentication success rate of matching their domain database with Aadhaar database, there is always a scope for wrongful identity verification. UIDAI has also advised from time to time that the demographic information as per Aadhaar should be captured and used for performing demographic authentication.

2. In order to remove any chances of wrongful identity verification using demographic authentication, it is hereby decided to discontinue the provision of partial matching in demographic authentication w.e.f 1.12.2017 after which the demographic authentication shall be allowed only for exact match of name, address and other parameters as in Aadhaar.

3. It is reiterated that to achieve the best and accurate results in demographic data verification, AUAs should capture name, address and other demographic details as per Aadhaar to perform demographic authentication. The information as per Aadhaar may be captured directly either from Aadhaar letter or eAadhaar or mAadhaar using QR code reader.



(Yashwant Kumar)
Assistant Director General (Auth)

To,

All AUAs/KUAs & ASAs

सं.के-11020/44/2012- यूआईडीएआई(ऑथ-I)

भारत सरकार

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथेंटिकेशन डिवीज़न

जीवन भारती भवन, टॉवर I, नवां तल,

कनॉट सर्कस, नई दिल्ली -110001

दिनांक: 30.11.2017

CIRCULAR

Reference is invited to this office circular no. K-11020/44/2012-UIDAI (Auth-I) dated 24.05.2017 which notified the timelines for upgradation of all public biometric devices to Registered Devices. It was mentioned that all AUAs/KUAs and ASAs shall upgrade to Registered Device and no authentication transaction shall be allowed on non-Registered Devices after 30.09.2017. It was also mentioned in the notification dated 24.5.2017 that from 01.08.2017 to 30.09.2017 all non-Registered Device transactions shall be charged @ Rs 0.20 and Rs 0.10 for AUAs and ASAs respectively. Further, due to various requests received from AUAs for extension of Registered Device timelines, the timeline was first extended to 31.10.2017 vide circular dated 30.09.2017 and then extended to 30.11.2017 vide circular dated 31.10.2017 subject to the payment of non-Registered Device transaction charges i.e. @ Rs 0.20 and Rs 0.10 for AUAs and ASAs respectively.

2. Whereas a number of AUAs and ASAs have already upgraded to Registered Devices, UIDAI has received requests from certain entities that they are at various stages of Registered Devices rollout and need some more time to complete the transition.

3. Therefore it has been decided to extend the timeline for Registered Device implementation by one month i.e. up to 31.12.2017 subject to the condition that non-Registered Device transactions shall continue to be charged @ Rs 0.20 and Rs 0.10 for AUAs and ASAs respectively as per notification dated 24.05.2017. Please be advised that since most of the entities already have migrated to Registered Devices, no further extension for non-Registered Device transactions shall be given beyond 31.12.2017.

4. It is reiterated that in order to ensure encryption of biometrics of residents at time of capture, it is absolutely essential to use only the Registered Devices. Any further use of non-Registered Devices will be putting residents' privacy at risk. Therefore, all AUAs and KUAs are requested to upgrade to Registered Devices at the earliest.

(यशवंत कुमार)

सहायक महानिदेशक(ऑथेंटिकेशन)

To

1. All AUAs/KUAs
2. All STQC Certified Device Providers
3. Tech Centre

File No. K-11022/631/2017-UIDAI (Auth-II)
Government of India
Unique Identification Authority of India
Authentication Division

9th Floor, Tower-I, Jeevan Bharti Building,
Connaught Circus, New Delhi-110001

Date: 1st December 2017

CIRCULAR

Sub: Discontinuation of the provision of partial match in Demographic authentication

In continuation to UIDAI's Circular No. K-11022/631/2017-UIDAI (Auth-II) dated 27.11.2017 on the above mentioned subject, UIDAI has received a number of requests from various entities for continuing the provision of partial match in Demographic authentication.

2. Therefore, it has been decided to extend the provision of partial matching in demographic authentication by one month i.e. till 31.12.2017 after which the demographic authentication shall be allowed only for exact match of name, address and other parameters as in Aadhaar.



(Yashwant Kumar)
Assistant Director General (Auth)