AADHAAR (AUTHENTICATION AND OFFLINE VERIFICATION) REGULATIONS, 2021

UNION OF INDIA
India
The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

AADHAAR (AUTHENTICATION AND OFFLINE VERIFICATION) REGULATIONS, 2021

Regulation 2 of 2021

- Published in Gazette of India : Extraordinary on 8 November 2021
- Commenced on 8 November 2021
- [This is the version of this document from 8 November 2021.]

No. K-11020/240/2021/Auth/UIDAI (No. 2 of 2021).—In exercise of the powers conferred by sub-section(1), and sub-clauses (a), (ba), (ca), (cb), (f), (fa), (fb) and (w) of sub-section (2) of Section 54 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 as amended vide the Aadhaar and Other Laws (Amendment) Act, 2019 (No.14 of 2019) and in supersession of the Aadhaar (Authentication) Regulations, 2016 except as respects things done or omitted to be done before such supersession, 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 and Offline Verification) Regulations, 2021.(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;(aa)“Aadhaar number” means an identification number issued to an individual under sub-section (3) of section 3 of Aadhaar Act, and includes any alternative virtual identity generated under sub-section (4) of that section;(b)“Aadhaar number holder” means an individual who has been issued an Aadhaar number under the Act;(ba)“Aadhaar Number Capture Service Token or ANCS Token” means an encrypted

number generated for an Aadhaar number by the Authority for completion of an authentication transaction. ANCS Token shall be valid for a short period of time as prescribed by the Authority;(bb)“Aadhaar Paperless Offline e-KYC” means a digitally signed document generated by the Authority containing last 4 digits of Aadhaar number, demographic data like name, address, gender, and date of birth, and photograph of the Aadhaar number holder etc.;(bc)“Aadhaar Secure QR Code” means a quick response code generated by the Authority which contains digitally signed data like last 4 digits of Aadhaar number, demographic data like name, address, gender, and date of birth, and photograph of the Aadhaar number holder etc.;(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 authenticating the Aadhaar number along with demographic information or biometric 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 a licensed entity providing necessary infrastructure for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility provided by the Authority;(g)“Authentication User Agency” or “AUA” means a requesting entity that uses the Yes/ No authentication facility provided by the Authority;(h)“Authority” means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Act;(i)“Central Identities Data Repository” or “CIDR” means a centralised database in one or more locations containing Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;(ia)“child” means a person who has not completed eighteen years of age;(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 full or limited demographic information and/or photograph of an Aadhaar number holder. The e-KYC data may contain full or masked Aadhaar number;(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;(ma)"Offline Verification” means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations;(mb)“Offline Verification Seeking Entity” or “OVSE” means any entity desirous of undertaking offline verification of an Aadhaar number holder;(mc)“Offline Aadhaar Data” means the data relating to offline Aadhaar verification, having characteristics as specified by the Authority from time to time including the requirement of masking Aadhaar numbers before storing;(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;(na)“Registered Devices” means biometric devices that are registered with the

Authority;(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;(oa)“Sub-AUA” means a requesting entity that uses the Yes/ No authentication facility provided by the Authority through an existing AUA;(ob)“Sub-KUA” means a requesting entity that uses e-KYC authentication facility provided by the Authority through an existing KUA;(oc)“UID Token” means a 72-character alphanumeric string generated by the Authority mapped to the Aadhaar number and specific to a requesting entity;(od)“Virtual Identifier” means an interchangeable 16-digit random number mapped with the Aadhaar number of the Aadhaar number holder; 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 Facilities.—

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).

3A. Types of Offline Verification.—

1. There shall be following types of Offline Verification services provided by the Authority, namely—

(i)QR Code verification,(ii)Aadhaar Paperless Offline e-KYC verification,(iii)e-Aadhaar verification,(iv)Offline Paper based verification, and(v)Any other type of Offline verification introduced by the Authority from time to time. Offline Verification as above may be carried out by the entity as per the specifications given by the Authority from time to time.

2. The Authority shall provide various means to download QR Code, e-Aadhaar or Aadhaar Paperless Offline e-KYC through website, mobile application or other means.

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.

4A. Virtual Identity number (VID).—

(1)Authority shall provide an alternate identification number mapped with Aadhaar number for the purpose of authentication.(2)Aadhaar number holder may generate or retrieve his/her VID through UIDAI website, SMS, mobile application, eAadhaar download and any other means as provided by Authority from time to time.(3)The Aadhaar number holder may use VID in lieu of Aadhaar number for online authentication or e-KYC.(4)No entity shall store Virtual ID in its system.

5. Information to the Aadhaar number holder.—

(1)At the time of authentication or Offline Verification, a requesting entity or Offline Verification Seeking Entity(OVSE) respectively shall inform the Aadhaar number holder or in case of a child, inform the parent or guardian, of the following details:—(a)the nature of information that will be shared by the Authority upon authentication with the requesting entity;(b)the uses to which the information received during authentication or offline verification may be put; and(c)alternate and viable means of submission of identification and that no service to the resident will be denied for refusing to, or being unable to, undergo authentication or offline verification.(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.(3)A requesting entity or OVSE shall ensure that the no service is denied to any resident for refusing to or being unable to undergo authentication or offline verification provided that the resident is able to identify himself through a viable alternative means as suggested by the requesting entity under sub-regulation (1)(c)above.

6. Consent of the Aadhaar number holder.—

(1)After communicating the information in accordance with Regulation 5, a requesting entity or Offline Verification Seeking Entity (OVSE) shall obtain the consent of the Aadhaar number holder or in case of achild, the consent of the parent or guardian of the child for the authentication or verification.(2)A requesting entity or OVSE 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.(1a)All biometric devices used for authentication shall be Registered Devices as per the standards specified by the Authority from time to time.(1b)All the biometric devices shall be registered with the server of the requesting entity.(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 specificationsissued, 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 conformto 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 ismapped to Aadhaar number and necessary demographic and / or biometric information and/ or OTP fromthe Aadhaar number holder, the client application shall immediately package and encrypt these inputparameters 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 theAuthority for this purpose.(2)After validation, the server of a requesting entity shall pass the authentication request to the CIDR, throughthe server of the Authentication Service Agency as per the specifications laid down by the Authority. Theauthentication request shall be digitally signed by the requesting entity and/or by the Authentication ServiceAgency, as per the mutual agreement between them.(3)Based on the mode of authentication request, the CIDR shall validate the input parameters against the datastored therein and return a digitally signed Yes or No authentication response, or a digitally signed e-KYCauthentication response with encrypted e-KYC data, as the case may be, along with other technical detailsrelated to the authentication transaction.(4)In all modes of authentication, the Aadhaar number is mandatory and is submitted

along with the inputparameters 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 theauthentication device as per the processes and specifications laid down by the Authority.

10. Notification/Acknowledgement of authentication or offline verification to Aadhaar number holder.—

(1)The Aadhaar number holder shall be notified by the requesting entity about any authentication, throughemail and/or SMS and/or other digital means and/or paper based acknowledgement about success or failureof authentication on each request. Such notification/acknowledgement shall include requesting entity's name,date and time of authentication, auth response code, last 4 digits of Aadhaar number and purpose ofauthentication, as the case may be.(2)The Aadhaar number holder shall be notified by the OVSE about any offline verification, through emailand/or SMS and/or other digital means and/or paper based acknowledgement about success or failure ofoffline verification on each request.(3)In case of authentication failure the requesting entity should, in clear and precise language, inform theresident about the reasons of authentication failure such as Suspended/Cancelled Aadhaar orBiometric/Aadhaar Locking.

11. Biometric locking.—

(1)The Authority may enable an Aadhaar number holder to permanently lock his biometrics andtemporarily unlock it when needed for biometric authentication.(2)All biometric authentication against any such locked biometric records shall fail with a "No" answerwith 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 tillcompletion of the authentication transaction, whichever is earlier.(4)The Authority may make provisions for Aadhaar number holders to remove such permanent locks atany point in a secure manner.

11A. Aadhaar locking.—

(1)The Authority shall enable an Aadhaar number holder to lock his/her Aadhaar number and unlock itwhen needed for authentication.(2)All authentication requests using Aadhaar number against any such locked Aadhaar number shall resultwith a "No" answer with an appropriate response code.(3)In case of a locked Aadhaar, the Authority will allow the resident to authenticate using Virtual ID orother means.

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 Authorityshall apply for appointment as requesting entities in accordance with the procedure as may be specified bythe Authority for this purpose from time to time. Only those entities that fulfill the criteria laid down in A are eligible to apply. The Authority may by order, amend Schedule A from time to time so as to modify the eligibility criteria.(1A)Requesting entity and ASA shall meet technical and security criteria as specified by the Authority fromtime to time.(2)Entities seeking appointment as Authentication Service Agencies shall apply for appointment to theAuthority in accordance with the procedure as may be specified by the Authority for this purpose. Onlythose entities that fulfill the criteria laid down in Schedule B are eligible to apply. The Authority may byorder, 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 mattersrelevant 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 thetime as may be specified in this regard by the Authority.(5)While considering the application, the information furnished by the applicant and its eligibility, theAuthority may verify the information through physical verification of documents, infrastructure, andtechnological 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;andb. enter into appropriate agreements with the entity or agency incorporating the terms and conditionsfor use by requesting entities of the Authority's authentication facility, or provision of services byASAs, 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 theirappointment, including application fees, annual subscription fees and fees for individual authenticationtransactions.(8)The Authority may from time to time, determine requesting entities which may be allowed to store Aadhaarnumber or masked Aadhaar number.(9)The Authority may from time to time, determine the data fields to be provided as part of e-KYC response toparticular requesting entities.(10)The Authority may from time to time, determine if requesting entities will be allowed to performauthentication using Aadhaar number or Virtual ID or UID Token or ANCS or any other identifier.

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

(1)In the event an application for appointment of requesting entity, Authentication Service Agency, as the casemay be, does not satisfy the requirements specified by the Authority, the Authority may reject theapplication.(2)The decision of the Authority to reject the application shall be communicated to the applicant in writingwithin 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 ofthirty 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 performingauthentication;(b)establish network connectivity with the CIDR, through an ASA duly approved by the Authority, forsending authentication requests;(c)ensure that the network connectivity between authentication devices and the CIDR, used for sendingauthentication requests is in compliance with the standards and specifications laid down by theAuthority for this purpose;(ca)ensure that the Aadhaar number/Virtual ID/ANCS Token provided by the resident for authenticationrequest shall not be retained by the device operator or within the device or at the AUA server(s);(cb)ensure that the provision of authentication using Virtual ID is provided;(d)employ only those devices, equipment, or software, which are duly registered with or approved orcertified by the Authority or agency specified by the Authority for this purpose as necessary, and arein 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 theterms and conditions, standards, directions, and specifications, issued and communicated by theAuthority, in this regard, from time to time,(f)ensure that persons employed by it for performing authentication functions, and for maintainingnecessary systems, infrastructure and processes, possess requisite qualifications for undertaking suchworks.(g)keep the Authority informed of the ASAs with whom it has entered into agreements;(ga)obtain approval from the Authority before appointing any third party entity as Sub-AUA/Sub-KUA.(h)ensure that its operations and systems are audited by information systems auditor certified by arecognised body on an annual basis to ensure compliance with the Authority's standards andspecifications and the audit report should be shared with the Authority upon request;(i)implement exception-handling mechanisms and back-up identity authentication mechanisms toensure seamless provision of authentication delivery of services to the residents;(j)in case of any investigation involving authentication related fraud(s) or dispute(s), it shall extend fullcooperation to the Authority, or any agency appointed or authorised by it or any other authorisedinvestigation agency, including, but not limited to, providing access to their premises, records,personnel and any other relevant resources or information as well to assist the Authority indisseminating information to the general public about any Aadhaar data related fraud to enableAadhaar number holders to evaluate whether they were victims of the fraud and take remedialaction;(k)in the event the requesting entity seeks to integrate its Aadhaar authentication system with its localauthentication system, such integration shall be carried out in compliance with standards andspecifications issued by the Authority from time to time;(l)shall inform the Authority of any misuse of any information or systems related to the Aadhaarframework or any compromise of Aadhaar related information or systems within their network. Ifthe requesting entity is a victim of fraud or identifies a fraud pattern through its fraud analyticssystem related to Aadhaar authentication, it shall share all necessary details of the fraud with theAuthority as well as to affected Aadhaar number holders without undue delay;(m)shall be responsible for the authentication operations and results, even if it sub-contracts parts of itsoperations to third parties. The requesting entity is also responsible for ensuring that theauthentication related operations of

such third party entities comply with Authority standards andspecifications and that they are regularly audited by approved independent audit agencies;(ma)may agree upon the authentication charges for providing authentication services to its customer, withsuch customer, and the Authority shall have no say in this respect, for the time being; however, theAuthority's right to prescribe a different mechanism in this respect in the future shall be deemed tohave been reserved;(mb)Aadhaar numbers collected through physical forms or photocopies of Aadhaar letters shall bemasked by the requesting entity by redacting the first 8 digits of the Aadhaar number before storingthe physical copies.(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 ofusing the authentication facilities provided by the Authority.(o)shall take specific permission of the Authority and sign appropriate agreement with the Authority, ifrequiring storage of Aadhaar number for non-authentication purposes. Aadhaar number shall bestored in a secure manner as specified by the Authority from time to time(p)extend full co-operation to the Authority for any mass awareness programmes that the Authoritymay undertake to sensitize Aadhaar number holders about the nature of data being used inauthentication, the scope of misuse as well as steps to protect against such misuse or fraud

14A. Obligations of Offline Verification Seeking Entities.—

(1)An OVSE shall have the following obligations:—(a)ensure compliance of Aadhaar Act and Regulations framed thereunder as well as relevantpolicies, manuals, procedures, specifications, standards, and directions issued by the Authority;(b)shall not collect, use or store Aadhaar number or biometric information of any individual forany purpose or share offline Aadhaar data with any other entity except in accordance with theAct and Regulations framed thereunder;(c)in case of any investigation involving Aadhaar data related fraud(s) or dispute(s), it shall extendfull cooperation to the Authority, or any agency appointed or authorised by it or any otherauthorised investigation agency, including, but not limited to, providing access to theirpremises, records, personnel and any other relevant resources or information as well to assistthe Authority in disseminating information to the general public about any Aadhaar data relatedfraud to enable Aadhaar number holders to evaluate whether they were victims of the fraud andtake remedial action;(d)shall inform the Authority, without undue delay and in no case beyond 72 hours after havingknowledge of misuse of any information or systems related to the Aadhaar framework or anycompromise of Aadhaar related information. If the OVSE is a victim of fraud or identifies afraud pattern through its fraud analytics system related to Offline Verification, it shall share allnecessary details of the fraud with the Authority as well as to affected Aadhaar number holderswithout undue delay;(e)shall be responsible for the Offline Verification operations and results, even if it sub-contractsparts of its operations to third parties. Further, the OVSE is responsible for ensuring that theOffline Verification related operations of such third-party entities comply with the Authoritystandards and specifications;(f)extend full co-operation to the Authority for any mass awareness programmes that theAuthority may undertake to sensitize Aadhaar number holders about the nature of data beingused in offline verification, the scope of misuse as well as steps to protect against such misuseor fraud.

15. Use of Yes/ No authentication facility.—

(1)A requesting entity may use Yes/ No authentication facility provided by the Authority for verifying theidentity 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 generatingand sharing a separate license key for every such entity through the portal or any other mechanism providedby the Authority to the said requesting entity. For the avoidance of doubt, it is clarified that such sharing oflicense key is only permissible for performing Yes/ No authentication, and is prohibited in case of e-KYCauthentication.(3)Such agency or entity:a. shall not further share the license key with any other person or entity for any purpose; andb. 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.(3A)AUAs/KUAs/Sub-AUAs/Sub-KUAs shall use their client application for Aadhaar authentication whichshall be digitally signed by the requesting entity.(4)It shall be the responsibility of the requesting entity to ensure that any entity or agency with which it hasshared 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 hasshared a license key, for non-compliance with the regulations, processes, standards, guidelines and protocolsof 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 dataof the Aadhaar number holder for its own purposes.(2)A KUA shall obtain specific permission from the Authority by submitting an application for sharing ofe-KYC data with Sub-KUA and such data may be shared in encrypted form as per the guidelines issued bythe Authority from time to time, with specific consent of Aadhaar number holder.(3)The Sub-KUA with whom the KUA has shared the e-KYC data of the Aadhaar number holder shall notshare it further with any other entity or agency.(4)The Aadhaar number holder may, at any time, revoke consent given to a KUA/Sub-KUA for storing hise-KYC data, and upon such revocation, the KUA/Sub-KUA shall delete the e-KYC data in a verifiablemanner and provide an acknowledgement of the same to the Aadhaar number holder.(5)In addition to the restriction on further sharing contained in sub-regulation (3), all other obligations relatingto the personal information of the Aadhaar number holder, data security and other relevant responsibilitiesapplicable to requesting entities, shall also apply to the Sub-KUA with whom e-KYC data has been shared inaccordance with this regulation 16.(6)The KUA shall maintain auditable logs of all such transactions where e-KYC data has been shared with Sub-KUAs, for a period specified by the Authority.

16A. Use of Offline Verification facility.—

(1)An OVSE may use the Offline Verification facility provided by the Authority for obtaining the offlineAadhaar data of the Aadhaar number holder only for the purpose specified to the Aadhaar number holder atthe time of verification.(2)No entity shall perform Offline Verification on behalf of

another entity or person.(3)An OVSE may store, with consent of the Aadhaar number holder, offline Aadhaar data of the Aadhaarnumber holder, received upon Offline Verification, securely as per the guidelines issued by the Authorityfrom time to time.(4)The Aadhaar number holder may, at any time, revoke consent given to an OVSE for storing his/her offlineAadhaar data, and upon such revocation, the OVSE shall delete the offline Aadhaar data in a verifiablemanner and provide an acknowledgement of the same to the Aadhaar number holder.(5)The Authority in cases of default or breach or change in law or any other circumstance as may be deemedappropriate by it, may direct the OVSE to discontinue the use of Offline Verification services.

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 orpublished for any purpose whatsoever, and no copy of the core biometric information is retained withit;(b)the core biometric information collected is not transmitted over a network without creation of encryptedPID block which can then be transmitted in accordance with specifications and processes laid down bythe Authority.(c)the encrypted PID block is not stored, unless it is for buffered authentication where it may be heldtemporarily on the authentication device for a short period of time, and that the same is deleted aftertransmission;(d)identity information received during authentication is only used for the purpose specified to theAadhaar number holder at the time of authentication, and shall not be disclosed further, except with theprior 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 otherinformation generated during the authentication process is kept confidential, secure and protectedagainst 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 secureand 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 authenticationdevices, 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 thefollowing transaction details, namely:—(a)specified parameters of authentication request submitted excluding Aadhaar number, Virtual ID, ANCSToken or UID token;(b)specified parameters received as authentication response including full Aadhaar number or maskedAadhaar, as the case may be;(c)the record of disclosure of purpose for which the authentication was performed, to the Aadhaar numberholder or parent or guardian, in case of a child, at the time of authentication; and(d)record of consent of the Aadhaar number holder, or parent or guardian, in case of a child, forauthentication, 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 accordancewith 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 yearsor the number of years as required by the laws or regulations governing the entity, whichever is later, andupon expiry of the

said period, the logs shall be deleted except those records required to be retained upon theorder of a court not inferior to that of a Judge of a High Court or required to be retained for any pendingdisputes.(4)The requesting entity shall not share the authentication logs with any person other than the concernedAadhaar number holder upon his/her request or for grievance redressal and resolution of disputes or upon theorder of a court not inferior to that of a Judge of a High Court. The authentication logs shall not be used forany purpose other than those 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 these regulations shall continue to remain inforce 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 inthe manner as may specified by the Authority for this purpose;(b)perform basic compliance and completeness checks on the authentication data packet before forwarding itto CIDR;(c)on receiving the response from CIDR, transmit the result of the transaction to the requesting entity thathas placed the request;(d)only engage with the requesting entities approved by the Authority and keep the Authority informed ofthe list of requesting entities that it serves;(e)communicate to the Authority, all relevant information pertaining to any agreement that it may enter intowith a requesting entity;(f)ensure that the persons employed by it for performing authentication and for maintaining necessarysystems, 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 onan annual basis, and provide a certified audit report, to the Authority, confirming its compliance with thepolicies, processes, procedures, standards, or specifications, issued by the Authority in this regard, fromtime to time;(h)ensure that all infrastructure and operations including systems, processes, devices, software and biometricinfrastructure, security, and other related aspects, are in compliance with the standards and specificationsas 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 andother Information Technology infrastructure, processes, procedures, etc.(j)comply with all relevant laws and regulations relating, in particular, to data security and datamanagement;(k)any value added service that an ASA provides to a requesting entity under a contract shall not form partof the Aadhaar authentication process;(l)shall be responsible to the Authority for all its authentication related operations, even in the event theASA 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, includingproviding access to its premises, records, systems, personnel, infrastructure, any other relevant resource orinformation and any other relevant aspect of its authentication operations;(n)may agree upon the authentication charges for providing services to a requesting entity, with suchrequesting entity, and the Authority shall

have no say in this respect, for the time being; however, theAuthority's right to prescribe a different mechanism in this respect in the future shall be deemed to havebeen 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 Aadhaar number, Virtual Id, UID Token, ANCS Token, PID information, deviceidentity related data and e-KYC response data, where applicable shall not be retained.(2)Authentication logs shall be maintained by the ASA for a period of 2 (two) years, during which period theAuthority and/or the requesting entity may require access to such records for grievance redressal, disputeredressal and audit in accordance with the procedure specified in these regulations. The authentication logsshall 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 aperiod of five years, and upon expiry of the said period of five years or the number of years as required bythe laws or regulations governing the entity whichever is later, the authentication logs shall be deletedexcept those logs required to be retained by a court not inferior to that of a Judge of a High Court or whichare 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 inforce despite termination of appointment in accordance with these regulations.

20A. Optional Maintenance of Logs by Offline Verification Seeking Entity

(1)An Offline Verification Seeking Entity may maintain logs of the verification transactions processed byit, if deemed necessary by the OVSE and with consent of the resident, containing any of the followingtransaction details, namely:—(a)the offline Aadhaar data document shared by the resident in a suitably secure manner ;(b)any other data shared by the resident during the course of verification including mobile number,email id, photo etc;(c)local verification transaction logs between OVSE and the resident;(d)details of the notification related to the Offline Verification sent to the Aadhaar number holder.but shall not, in any event, store the Aadhaar number or Virtual ID of the Aadhaar number holder.(2)The OVSE shall not share the logs with any person other than the concerned Aadhaar number holder orfor grievance redressal and resolution of disputes in accordance with the provisions of the Act. Theverification logs shall not be used for any purposes other than those stated in this sub-regulation.

21. Audit of requesting entities, Authentication Service Agencies and Offline Verification Seeking Entities.—

(1)The Authority may undertake audit of the operations, infrastructure, systems and procedures, of requestingentities, including their Sub-AUAs and Sub-KUAs, Authentication Service Agencies and OfflineVerification Seeking Entities, either by itself or through audit agencies appointed by it, to ensure that suchentities are acting in compliance with the Act, rules, regulations, policies, procedures, guidelines issued bythe 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 ofsuch 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/orappointed by the Authority in the audit process, and provide to the Authority or any agency approvedand/or appointed by the Authority, complete access to its procedures, records and information pertaining toservices 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 tofurnish necessary clarifications and/or information as to its activities and may also require such entity eitherto rectify the deficiencies or take action as specified in these regulations.(5)Notwithstanding anything contained in clause (4), and without prejudice to any action which may be takenunder the Act, the Authority may initiate action under Regulation 25(1A) on identification of anydeficiency pursuant to the audit conducted.

22. Data Security.—

(1)Requesting entities and Authentication Service Agencies/OVSEs shall have their servers used forAadhaar authentication request formation and routing to CIDR/Offline Verification respectively, to belocated within data centres or cloud storage centres located in India.(1A)Authentication requests shall not be accepted from entities located outside the territorial borders ofIndia. For allowing authentication requests from outside India, the requesting entity shall take specificpermission from the Authority.(2)Authentication Service Agency shall establish dual redundant, secured leased lines or MPLSconnectivity with the data centres of the Authority, in accordance with the procedure and securityprocesses as may be specified by the Authority for this purpose.(3)Requesting entities shall use appropriate license keys to access the authentication facility provided bythe Authority only through an ASA over secure network, as may be specified by the Authority for thispurpose.(4)Requesting Entities, Authentication Service Agencies and Offline Verification Seeking Entities shalladhere to all regulations, information security policies, processes, standards, specifications andguidelines 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 theauthentication 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 requestingentity or ASA to satisfy the Authority about any matter necessary for smooth discontinuance or terminationof services, including–(a)the arrangements made by the requesting entity for maintenance and preservation of authenticationlogs and other documents in accordance

with these regulations and procedures as may be specifiedby the Authority for this purpose;(b)the arrangements made by the requesting entity for making authentication record available to therespective 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 itsassociated 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 thecommencement of these regulations shall be deemed to be a requesting entity, and any AuthenticationService Agency (ASA) or e-KYC Service Agency (KSA) shall be deemed to be an AuthenticationService Agency, under these regulations, and all the agreements entered into between such agencies andthe Unique Identification Authority of India, established vide notification of the Government of India inthe Planning Commission number A-43011/02/2009-Admin. I, dated the 28th January, 2009 or anyofficer of such authority shall continue to be in force to the extent not inconsistent with the provisions ofthe Act, these regulations, and other regulations, policies, processes, procedures, standards andspecifications issued by the Authority.(2)Notwithstanding anything contained in sub-regulation (1), any deemed requesting entity or AuthenticationService Agency referred to in sub-regulation (1) shall be required to comply with the provisions of theAct, 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 authenticationfacility as specified in these regulations, it may immediately make an application for termination of itscredentials and stop its functions forthwith:Provided that in such cases, no compensation shall be payable to the agency or to the Authority upon suchtermination.(4)On discontinuance under sub-regulation (3), the concerned entity shall be required to comply with theclosure 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 issuedby 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 theapplication 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 stepsto impose disincentives on the requesting entity or an ASA for contravention of the provisions of the Act,rules and regulations thereunder, including suspension of activities of such entity or agency, or other stepsas 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 thetermination of appointment and discontinuance of its operations relating to Aadhaar authentication.(1A).Where

any Offline Verification seeking entity,(a)fails to comply with any of the processes, procedures, standards, specifications or directions issuedby the Authority, from time to time; is in breach of its obligations under the Act and theseregulations;(b)uses the Aadhaar Offline Verification facilities for purposes other than those specified;(c)fails to furnish any information required by the Authority for the purpose of these regulations; or(d)fails to cooperate in any inspection or investigation or enquiry or audit conducted by the Authority, 36. THE GAZETTE OF INDIA : EXTRAORDINARY [PART III—SEC.4] the Authority may, without prejudice to any other action which may be taken under the Act, including suchcriminal action as it may deem fit, take such steps to impose disincentives on the Offline Verificationseeking entity for contravention of the provisions of the Act, rules and regulations thereunder.Provided that the entity or agency shall be given the opportunity of being heard before any action istaken.(2)Any such action referred to in sub-regulation (1) may also be taken against any entity or Sub-AUA or sub-KUA.(3)Upon termination of appointment by the Authority, the requesting entity or the ASA shall, forthwith, cease touse the Aadhaar name and logo for any purposes, and in any form, whatsoever, and may be required tosatisfy 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)any authentication server side configurations as necessaryProvided that the Authority shall not, in any case, store the purpose of authentication or any meta data (other than process meta data) about any transaction.

27. Duration of storage. —

(1)Authentication transaction data shall be retained by the Authority for a period of 6 months. The Authority may prescribe procedure to archive and perform analysis, for research purposes, from aggregated and anonymised authentication transaction data in the form of circulars.(2)Upon expiry of the period of six months specified in sub-regulation (1), the authentication transaction data shall be deleted except when such authentication transaction data are required to be maintained by the order of a court not inferior to that of a Judge of a High 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 provisions of the Act.

Chapter V
MISCELLANEOUS

29. Repeal and savings.—

(1)All procedures, orders, processes, standards, specifications and policies issued and MOUs, agreements or contracts entered by the Unique Identity 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.(2)Notwithstanding the repeal of the Aadhaar (Authentication) Regulations, 2016, anything done or any action taken under the said Regulations shall be deemed to have been done or taken under the corresponding provisions of these Regulations.

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.

31. Power to issue policies, process documents, etc.-

The Authority may issue policies, orders, processes, standards, specifications 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.**SCHEDULE A**Eligibility criteria for appointment as requesting entitiesSee Regulation 12 (1)

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