मेरा आधार
मेरी पहचान

Compendium of Instructions

Issued by

Unique Identification Authority of India

MARCH 2026

CONTENTS

A - ENROLMENT & UPDATION

5.4	Clarification regarding usage of Aadhaar	20.12.2018	E-8
5.5	Guidelines on use of Aadhaar under section 7 of the Aadhaar Act 2016(as amended by the Aadhaar and Other Laws (Amendment) Act, 2019) by the State Governments for the schemes funded out of Consolidated Fund of State	25.11.2019	E-10
5.6	Use biometric modality in non-assisted mode	13.01.2023	E-19
5.7	Phase out of existing fingerprint L0 Registered Devices from Aadhaar Authentication ecosystem	27.01.2023	E-20
5.8	e-KYC Setu System	23.03.2023	E-22
5.9	Renewal of License Fees of Sub-AUAs/Sub-KUAs	27.03.2023	E-28
5.10	Rationalization of Sub-AUA/Sub-KUA	31.03.2023	E-29
5.11	Revising License Fees for AUA/KUA based on their transaction volume	05.04.2023	E-31
5.12	Chargeability of FMR/FIR auth. Error code	06.04.2023	E-33
5.13	Pricing of Aadhaar authentication transactions	03.05.2023	E-34
5.14	Authentication/verification of Aadhaar	19.06.2023	E-37
5.15	Availing Aadhaar authentication modalities by Requesting Entities	11.07.2023	E-42
5.16	Clarifications on issues relating to sharing of Aadhaar and related data amongst Government departments	08.08.2023	E-43
5.17	Migration of fingerprint L0 registered devices to fingerprint L1 devices	18.09.2023	E-45
5.18	Advisory regarding improving Auth Success rate of OTP failures	10.10.2023	E-47
5.19	Revision of fees for performance of authentication transactions by AUA/KUA other than TSPs	16.01.2024	E-51
5.20	Revision of fees for performance of authentication transactions by TSPs	16.01.2024	E-53
5.21	Clarification regarding usage of Aadhaar as proof of date of birth	23.04.2024	E-55
5.22	Extension of deadline for sunset of existing L0 Fingerprint Registered Devices deployed in Aadhaar authentication ecosystem	28.06.2024	E-57
5.23	Revised specifications of Mobile and Tabled based Child Enrolment Lite Client (CELC)	01.07.2024	E-59
5.24	Revised specifications of Aadhaar Enrolment Kit (AEK)	01.07.2024	E-63
5.25	Phase out of existing L0 Registered Devices from Aadhaar Authentication Ecosystem	27.09.2024	E-76
5.26	Guidelines on requiring Aadhaar number for receipt of subsidy, benefit or service under Section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies , Benefits and Services) Act, 2016	20.12.2024	E-79
5.27	Rationalization of Sub-AUA/Sub-KUA	26.12.2024	E-82
5.28	Execution of Supplementary Agreement or Agreement to supplement AUA Agreement under sub-regulation (3A) of regulation 9 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021	01.01.2025	E-83
5.29	Appointment of Sub-Authentication User Agency and Sub-eKYC User Agency	07.02.2025	E-89
5.30	Submission of Declaration and Undertaking regarding general chapter of management and the financial condition of the applicant entity under regulation 12(6) of the Aadhaar (Authentication and Offline Verification) Regulations, 2021	17.02.2025	E-105
5.31	Guidelines on requiring Aadhaar number in the interest of Good Governance, preventing leakage of public funds, promoting ease of living of residents and enabling better access to services by them for the purposes prescribed under sub-rule (1) of rule 3 of the Aadhaar Authentication for Good Governance (Social welfare, Innovation, Knowledge) Rules, 2020	18.03.2025	E-119

5.32	Phase out of existing L0 Registered Devices from Aadhaar Authentication Ecosystem	25.03.2025	E-124
5.33	Technical and functional upgrade of of fingerprint L1 registered devices	16.04.2025	E-126
5.34	Annual declaration to be submitted by AUA/KUA for a financial year	05.05.2025	E-128
5.35	Revision of license fee for Authentication Service Agency on their transaction volume	29.05.2025	E-130
5.36	Streamling the process of onboarding the Authentication Service Agency (ASA) with revised ASA Agreement and compliance checklist	29.05.2025	E-132
5.37	Changes in e-KYC response (PDF and XML format) for Foreigner enrolled Aadhaar number holders	09.06.2025	E-206
5.38	Aadhaar Status Notification Framework Documentation	31.07.2025	E-208
5.39	Customization of RD service for UIDAI Sandbox Environment	09.06.2025	E-210
5.40	Revised clarification on Face Authentication Implementation	15.07.2025	E-212
5.41	Partial Modification on Face Authentication Implementation	15.07.2025	E-213
5.42	Revised guidelines for hosting Aadhaar Data Vault (ADV), Hardware Security Module (HSM) and Authentication application on premises and cloud infrastructure for Aadhaar Authentication Ecosystem	18.07.2025	E-214
5.43	Aadhaar Status Notification Framework Documentation	31.07.2025	E-216
5.44	UIDAI framework for onboarding of State Co-Operative banks (StCBs) and District Central Co-Operative Banks (DCCBs) in Aadhaar Authentication Ecosystem	01.08.2025	E-230
5.45	Introduction of L1 Complaint Iris Authentication Registered Devices in Aadhaar Authentication Ecosystem	15.09.2025	E-235
5.46	Extension to Authentication Service Agency facilities to other requesting entities	14.10.2025	E-237
5.47	Execution of Supplementary Agreement or Agreement to supplement AUA Agreement under sub-regulation (3A) of regulation 9 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021	24.10.2025	E-239
5.48	Guidelines on publishing Gazette Notification, under provision of Section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016	03.11.2025	E-254
5.49	Revised guidelines for hosting Hardware Security Module (HSM), Aadhaar Data Vault (ADV) and authentication application on premises and cloud infrastructure for Aadhaar Authentication Ecosystem	04.11.2025	E-255
5.50	Revision of fees for performance of authentication transactions by requesting entities other than Telecom Service Providers	08.12.2025	E-264
5.51	Implementation of Unique Identifiers for Aadhaar-based Authentication Transactions	12.01.2026	E-265
5.52	Aadhaar face authentication onboarding audit checklist version 2.0 for requesting entities	03.03.2026	E-270

F - ENFORCEMENT

Sr. No.	Subject	Date of Issue	Page No.
6.1	Guidelines for making complaints before Adjudicating Officer	02.08.2022	F-2
6.2	Appointment of Nodal Officer for referring the complaints to Secretary, Ministry of Electronics and Information Technology (MeitY) regarding blocking of access of unauthorised websites	22.11.2022	F-4

A
ENROLMENT
& UPDATION

F. No. 4(4)/57/268/2015-E&U-II 1116270635

Ministry of Electronics & Information Technology (MeitY)
Government of India
Unique Identification Authority of India

2nd Floor, Tower-I, Jeevan Bharati Building,
Connaught Place, New Delhi – 110001
Dated: 18.09.2017

To

The Deputy Director General,
ROs, UIDAI & Tech Centre, Bengaluru
(As per list)

Sub: Guidelines for Cancellation (Omission) and Suspension (deactivation) of Aadhaar of Resident - reg

Sir,

I am directed to refer to the cases received by ROs regarding cancellation (Omission) and suspension (deactivation) of Aadhaar of the resident. In reference to this, it is to inform that prior to the enactment of the Aadhaar Act, and Aadhaar (Enrolment & Update) Regulation, 2016, UIDAI HQ had issued separate guidelines to all ROs and Tech Centre, Bengaluru vide letter No. 4(4)/57/19/2014-E&U-II (Part)(i) and No. 4(4)/57/19/2014-E&U-II(Part) dated 01st December, 2014 to deal with the issues relating to Aadhaar Life Cycle Management (ALCM) for suspension and cancellation of Aadhaar number of the resident.

2. As per Para 5 of ALCM Guidelines, ROs are empowered to initiate necessary action for cancellation/suspension of Aadhaar number. Now, it has been decided by the Competent Authority in UIDAI that henceforth approval for Cancellation (omit) and Suspension (deactivation) of Aadhaar number based on complaints received at UIDAI HQ/RO would be granted by UIDAI HQ only.

3. The Standard Operating Procedure (SOP) for the same is outlined below:-

a) All the cases received at ROs either directly or through UIDAI HQ are to be investigated by ROs as per rule 29 & 30 of Aadhaar (E&U) Regulation, 2016 within 14 days of the receipt of the case.

b) The investigation report of the cases are to be approved by DDG of the concerned ROs and approved investigation report alongwith RO's recommendations (e.g. No action/cancellation/suspension/any other action) to be sent to UIDAI HQ within 21 days of initiation of case.

INDEX

c) ROs recommendation will be examined by UIDAI, HQ and case(s) disposed off within 28 days of the case initiation and executive orders will be given by UIDAI HQ to Tech Centre, Bengaluru for taking necessary action (Cancellation (omit)/suspension (deactivation)/any other) under intimation to UIDAI HQ and concerned Regional Office.

4. Further, ROs are requested to forward Monthly report (as per Performa attached) of cases related to cancellation (omission)/suspension (deactivation) received and disposed by them from 1st Jan, 2017 to till date. The status of the cases related to cancellation/suspension is to be given in the following manner **(Performa – A)** as below:-

a) Nature of Complaint in brief – e.g. Duplicate Aadhaar, Biometrics matching with other resident, Biometrics given by relatives etc.
b) Brief of Investigation report
c) Decision taken by RO (Cancellation/Suspension/any other action)
d) Final disposal i.e. whether Aadhaar Cancelled/Suspended.

6. This issues with the approval of the Competent Authority in UIDAI.

Encl: Performa 'A'

18/9/17

(P.K.Jha)
Deputy Director (E&U-II)
praween.jha@uidai.net.in

Copy to:

i. ADG, Tech Centre, Bengaluru
ii. PS to DDG(E&U) — Arora 20/09/17
iii. All DDG (ROs)
iv. DDG (Tech Centre)

INDEX

L Additional Guidelines for Assistance towards ICT Infrastructure

1. Introduction

1.1 The Government Notification dated 28th January 2009 creating the Unique Identification Authority of India (UIDAI) and defining its mandate and responsibilities has laid down that the UIDAI has the responsibility, among others, for defining mechanisms and processes for interlinking UID with partner databases on a continuous basis, coordinating/liaising with the implementation partners and user agencies as also define conflict resolution mechanism, defining usage and applicability of UID for delivery of various services and issuing necessary instructions to agencies that undertake creation of databases, to ensure standardization of data elements that are collected and digitized and enable collation and correlation with the UID and its partner databases. The Prime Minister's Council of the UIDAI, in its first meeting held on 12 August 2009 decided to designate the UIDAI as the Apex body to set standards in the area of biometric and demographic data structures.

1.2 The Prime Minister's Council in its first meeting also approved, in principle, the proposal to provide necessary support to the registrars/other departments in their budgets to enable them to make necessary investments in creating ICT infrastructure. The Committee of Secretaries met on 9 October 2009 to review action taken on the first meeting of the PM's Council on UIDAI and decided that UIDAI will advise concerned Ministries/Departments in the enrollment process, to suitably incorporate their requirements for creation of necessary infrastructure into their budget proposals for 2010-2011. It was also decided that UIDAI will coordinate the proposals of individual Ministries/Departments to ensure that there is no duplication between the agencies with respect to creation of requisite infrastructure.

1.3 UIDAI has deliberated a lot on this matter and has also had consultations with several Ministries and State Governments. In the interest of establishing uniformity and also ensuring that the partners' databases/

ICT infrastructure are UID compliant, it was decided that UIDAI should seek funds in the UIDAI scheme and budget for assisting the Registrars/Other Departments.

1.4 Given the complexity in determining, with reasonable accuracy, the cost of integration of State level applications with that of UIDAI, a normative amount of Rs. 10 crore (Rs.2 crore each for five State level applications estimated to be taken up) was provided for in the EFC proposal, which has been approved by the Cabinet Committee on UIDAI related issues. However, both the number of applications taken up in each State and the cost of their integration can vary depending upon the nature and extent of integration of the various applications.

1.5 ICT Guidelines were framed by UIDAI and circulated to all the States in September 2010. Under these guidelines, UIDAI has since provided assistance to several State Governments & Union Territories to help set up infrastructure for integration of schemes with Aadhaar and several States have already started providing Aadhaar enables services and benefits like PDS, pensions, etc.

2. Current Scenario

2.1 Aadhaar enrolments have crossed 104 crores across the country as on 15.08.2016 and Aadhaar is being recognized as a platform for online verification of the identity of a resident through the process of Aadhaar authentication and e-KYC and as a financial address through Aadhaar Payments Bridge. Demand for Aadhaar based service delivery has grown exponentially in recent times with 20 crore authentication transactions and 1.5 crore e-KYC transactions being done on average every month. It is expected that in the near future, Aadhaar would become a way of life for the residents for day-to-day transactions, both financial and non-financial , through Aadhaar based online authentication using biometric devices at the Service Delivery Points.

2.2 With most States on way to rolling out Aadhaar enabled subsidies, services and benefits, there is a felt need to increase focus on enabling targeted enrolment and facilitating service delivery at the Point of Sale/Service (PoS).

2.3 Though the overall Aadhaar saturation of adult population is almost 98%, resident services are required to be provided for enrolment of the left over population, and in respect of the new-borns and children, whose coverage is presently much lower and who in addition need biometric update at ages 5 and 15 years. Aadhaar update services are also required for residents who want to update addresses, registered mobile numbers, e-mails etc. This is essential for efficient and effective delivery of Aadhaar based services and benefits. In this regard, in March 2016, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 has been enacted by Parliament. As per Section 7 of the Act, the Central or a State Government may make identification based on Aadhaar authentication a condition for availing Government subsidy, service or benefit and for persons not having Aadhaar, he/she makes an application for enrolment. This would necessitate that State Governments build capability to ensure that enrolment facilities are easily accessible and available across board for enabling such targeted enrolment. Therefore, as the need for Aadhaar based authentication for service delivery increases, UIDAI needs to support the endeavour of the State Governments in setting up infrastructure and establishing capabilities for enrolment and update services, of left out population, infants and children including their biometric updates at 5 and 15 years, and demographic/biometric/mobile data updates by Aadhaar holders, as well as for value added services such as seeding, printing of e-Aadhaars on demand or on account of updates, grievance redressal relating to enrolment and authentication, etc.

2.4 Accordingly, in modification of the existing ICT Guidelines, a new stream of ICT Assistance would be provided to States for procuring enrolment kits. These will be primarily used for targeted enrolment, especially of new-borns and school children, and their mandatory biometric

update at ages 5 and 15 years and would be deployed to various schools, anganwadis. The assistance will also be used for the enrolment of adult beneficiaries of other direct benefit programmes who have not got Aadhaar.

3. *Quantum of Assistance*

3.1 For setting up of infrastructure in States/UTs to enable updations, enrolments of leftover population, new-borns and other value added services, a **maximum** of 50% of total ICT Assistance of the State, viz, Rs 5 crore (50% of maximum admissible amount of Rs 10 crore) would be made available.

3.2 However, the above condition may be relaxed by competent authority in exceptional circumstances, subject to adequate justification from the concerned State/UT Government.

3.3 States that have already availed funds under the existing ICT guidelines may obtain funds under these provisions for the balance amount of ICT Assistance that is admissible to them on submission of fresh or amended DPR in this regard. They may also utilize funds that they have obtained but have not utilized against the previous DPR by submitting revised proposal in this regard.

4. *Process of ICT Assistance*

4.1 The process of providing assistance to State Governments for targeted enrolment would involve the following stages:

- Identification of left over population or children requiring enrolment
- Identification of quantum of biometric updates of children at 5 and 15 years required
- Identification of schemes requiring targeted enrolment and/or seeding
- Receipt of DPR from Nodal Department
- Recommendations of the Regional Office on the DPR

- Due diligence at UIDAI Headquarters and approval.

5. *Receipt of DPR from State Governments*

5.1 The State UID Implementation Committee (UDIC) should obtain a DPR comprising a project plan and a detailed monthly enrolment plan from the State Registrars/Departments implementing various social sector schemes where making the existing ICT infrastructure UID compliant will improve the efficiency and accountability of the delivery mechanisms.

5.2 In case the State Government has appointed a Nodal department that would collect and integrate data for the entire State, then the Nodal Department would prepare the DPR and the funds would be released to the Nodal Department, which will be responsible for coordinating the implementation of the project under the overall guidance of the State UDIC.

5.3 The specific sections of the society such as the BPL families, senior citizens, school children, tribals socially weaker sections bonded labour etc targeted should be captured, which would define the reach of the project and would provide maximum returns in terms of efficiency and social returns. Geographical areas like remote, inaccessible areas, disturbed areas, backward or tribal areas may also be given priority. The schemes/sectors/areas that have a greater social impact and higher spin off effects like Women and Child Development schemes, school education programmes, old age pensions, etc may be given priority.

5.4 The proposal should have the following information as per Format enclosed:

(i) Number and type of equipment being procured
(ii) The overall outlay and timelines for deployment
(iii) The proposed deployment of the equipment across departments/ districts
(iv) The schemes proposed to be covered under targeted enrolment
(v) The total number of enrolments planned upto March 2017.

INDEX

6. Evaluation of DPR

6.1 The DPR received from the State Nodal Department should be evaluated by the respective Regional Office on the basis of the status of enrolment, deployment of existing enrolment/facilitation centres and the roll-out plans of Aadhaar based services/subsidies in the State.

7. Recommendations of the Regional Office

7.1 After comprehensively evaluating the DPR and the detailed monthly enrolment plan received from the State UID Implementation Committees, the respective Regional Offices will send their recommendations distinctly indicating the components that require financial assistance.

8. Due diligence by Headquarters and approval

8.1 The recommended proposals received from Regional Offices would be scrutinized at UIDAI Headquarters and assistance to the Registrars/Nodal department under ICT Assistance would be approved by UIDAI Headquarters, keeping in view the availability of funds and inter-se prioritization. Priority would be accorded for Departments that envision a broader reach and preparedness, which would maximize the impact on universal enrolment and service delivery.

9. Components for ICT Assistance to State Governments

9.1 ICT Assistance would be provided Enrolment Kits at PECs/Facilitation Centres, comprising of:

(i) Computer/Laptop (with provision for dual screen)
(ii) Web Cam for resident photograph
(iii) Slap Scanner
(iv) Dual Iris scanner

(v) Scanner for documents

(vi) Printer.

These kits should be compatible with ECMP as well as CELC software of UIDAI for enrolment and update as well as be compatible with Authentication API 1.6 and above for enabling seeding at these stations.

9.2 All biometric equipment must be STQC certified. State may refer to detailed technical requirements for devices as may be specified by UIDAI from time to time.

9.3 The rate of assistance would be maximum Rs 1 lakh per enrolment kit.

9.4 The States may procure the devices at rates specified by the DGS&D. If a particular device is not available with DGS&D, then the State may do price discovery after following standard financial and procurement procedures of the Government.

9.5 A maximum of Rs 2.50 crore would be released to a State in a single tranche, and the balance released after deployment and UCs for the previous equipment is received.

9.6 Assistance may be provided only on equipment; cost of other infrastructure, deployment of personnel, operating expenses, maintenance, etc may be borne by the State.

10. Implementation

10.1 Funds would be released to the designated State Nodal Department designated, which would procure the equipment centrally and allocate the same to various Departments/Agencies as per approved plan of the State Government in this regard.

10.2 The Nodal Department may also ensure that the enrolment kits and tablets are on-boarded on the UIDAI enrolment system through the State

INDEX

Registrars/State Enrolment Agencies and that certified operators/supervisors are engaged and trained to ensure optimum efficient working of these devices.

10.3 Nodal Department will also monitor the implementation of the project and submit necessary progress reports and Utilisation Certificates to the UIDAI.

10.4 States will submit the Utilisation Certificates as soon as the funds released are utilized, along with physical progress report against the targets and milestones in the DPR.

10.5 The State Governments may contact the concerned ROs for technical assistance and guidance. ROs will monitor the progress of implementation of the States under their jurisdiction.

*****

Annexure: Planned Deployment of Enrolment Kits

Department/ Agency	No. of Enrolment Kits	No. of Districts where proposed to be deployed	No. of Schools/ Anganwadis/ Service Centres/ Other Locations	Details of Location of Deployed Enrolment Kit	Whether Certified Operators Available at Location	Enrolment/ Updates targeted	Seeding	Outlay (Rs in lakh)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Total								

F. No. 4(4)/57/268/CROs/2018-E&U-II

Government of India
Ministry of Electronics & Information Technology (MeitY)
Unique Identification Authority of India

7th Floor, Aadhaar Building,
Bangla Sahib Road, Behind kali Mandir,
New Delhi-110001
Dated: 12.07.2018

To
The DDGs,
All ROs (As per list attached)

Subject: Formats for referring Aadhaar Life Cycle Management (ALCM) cases for Cancellation/Suspension.

Reference: 1. UIDAI HQ letter No. F. No. 4(4)/57/19/2015-E&U-II (Part) II) dt 01 Dec 2014.

2. UIDAI HQ letter No. F. No. 4(4)/57/268/2015-E&U-II dt 18 Sep 2017.

Sir,

I am directed to refer to UIDAI O.O No. 4(4)/57/268/2015-E&U-II dated 18.09.2017 through which instructions for cancellation/suspension of Aadhaars were circulated. As per ibid instructions it has been decided that all cases for cancellation/suspension of Aadhaar are to be sent by ROs to UIDAI HQ for obtaining approval of competent authority.

2. Subsequent to issue of these instructions a large number of requests for cancellation and suspension are being received at UIDAI HQs in different formats. Based on the analysis of past cases, sample formats (attached as **Annexure**) have now been prepared for most of the common type (5 Nos.) of cases. The list is by no means is exhaustive and many other cases may be encountered over a period of time.

3. It is expected that these formats would ensure that all necessary inputs are gathered and submitted/considered for cancellations/suspensions for ensuring speedier disposal of these cases.

4. All ROs are therefore requested to forward their cases after ensuring complete information as enumerated in the annexure attached.

This issueds with the approval of competenet authority.

12.7.18
(Praween Jha)
Deputy Dir. (E&U-II)

Copy to: 1) PS to DDG (E&U)
2) ADG (QC), All ROs
3) Guard File

INDEX

Annexure

Formats for Omission/Suspension of Aadhaar Number

Case 1 – Bio mix between complainant and candidate

S. No.	Name of Resident/Complainant	Summary of the case	Regional office Recommendation
1.	**Complainant/Applicant** R1(name) has his/her biometrics matching with **candidate** R2 (name) having Aadhaar No. XXXX XXXX XXXX. R1 not able to get his/her Aadhaar made.	1. Complaint/Request received from Sh./Ms..... for-------- vide letter No.---- dt----- that R1 is not able to..... 2. **EID Details**:- (a) of R1 (i) (ii) (b) of R2 (i) (ii) 3. Status of the R2 UID - Active/Suspended 4. Relationship between R1 & R2---- 5. If not related or unknown – is R2 contactable or not? --- 6. **Findings of Field Enquiry by RO office as per Aadhaar Act 2016 (Regulations 29 & 30) :-** (a) **Tech center report obtained and its recommendations :-** (i) Confirmed bio mix in which UID – (ii) Full or partial match & details thereof - (iii) Feasibility of 'Whitelisted update' – Yes/No. (iv) Recommendation of the Tech Center. (b) Interaction details with the candidate---- (c) Circumstances leading to mixing up of biometrics---------- (d) Whether enrolment/update was tried in presence of RO officials so as to ensure correct biometrics input? (e) In case R2 is reported not alive has RO carried out verification of death----------.	Recommendation duly approved by DDG of the RO ----------

INDEX

		(f) Opportunity provided to candidate/NOK, in case his/her UID is being recommended for omission or deactivation / suspension---------- (g) Consent of the candidate/NOK on omission/suspension / suspension of UID ----- (h) Any other information----- **Note: 1. Attach photocopies all relevant documents with each case for reference at UIDAI HQ.** **2. Strike out which are not applicable.**	
Case 2 – Bio mix between complainant and multiple candidates			
2.	**Applicants** R1, R2...(names) have their biometrics matching with **candidate** (name) having Aadhaar No. XXXX XXXX XXXX. R1, R2.... are not able to get their Aadhaar made.	1. Complaints/Requests received from Sh./Ms..... for-------- vide letter No.---- dt---- - that they are not able to..... 2. **EID Details:-** (a) of R1 (i) (ii) (b) of R2 (i) (ii) (c) of Candidate (i) (ii) 3. Status of the candidate UID – Active/Suspended 4. Relationship between R1, R2.... and the candidate ---------- 5. If not related or unknown – is the candidate contactable or not? ---- 6 **Findings of Field Enquiry by RO office as per Aadhaar Act 2016 (Regulations 29 & 30) :-** (a) **Tech center report obtained and its recommendations :-** (i) Confirmed bio mix in which UID – (ii) Details of bio match – (iii) Feasibility of 'Whitelisted update' – Yes/No. (iv) Recommendation of the Tech Center. (b) Interaction details with the candidate--------	Recommendation duly approved by DDG of the RO ---- --------

INDEX

		--. (c) Circumstances leading to mixing up of biometrics---------- (d) Whether enrolment/update was tried in presence of RO officials so as to ensure correct biometrics input and result thereof. (e) In case R2 is not alive - verification of death certificate ----------. (f) Opportunity provided to candidate/NOK, in case his/her UID is being recommended for omission or deactivation---------- (g) Consent of the candidate/NOK on omission/suspension of UID ---- (h) Any other information------ **Note: 1. Attach photocopies all relevant documents with each case for reference at UIDAI HQ.** **2. Strike out which are not applicable.**	
Case 3 – Bio mix between complainant and candidate (Candidate has two Aadhaars)			
3	**Applicant** R1(name) has his/her biometrics matching with **candidate** R2 (name) having two Aadhaars No. XXXX XXXX XXXX & XXXX XXXX XXXX. R1 not able to get his/her Aadhaar made.	1. Complaint/Request received from Sh./Ms..... for-------- vide letter No.---- dt---- that R1 is not able to..... 2. **EID Details**:- (a) of R1 (i) (ii) (b) of R2 (i) (ii) 3. Status of the R2 UIDs - Active/Suspended 4. Relationship between R1 & R2---- 5. If not related or unknown – is R2 contactable or not? ---- 6. **Findings of Field Enquiry by RO as per Aadhaar Act 2016 (Regulations 29 & 30) :-** (a) **Tech center report and recommendations** :- (i) Confirmed bio mix in which UID -	Recommendation duly approved by DDG of the RO ---- --------

INDEX

		(ii) Full or partial match & details thereof (iii) Feasibility of Whitelisted update – Yes/No. (iv) Specific reasons in case earlier issued Aadhaar is being recommended for cancellation ---- (v) Confirmation that duplicate Aadhaar has been generated and likely reason for duplicate Aadhaar generation. (b) Interaction details with the candidate ------ (c) Circumstances leading to mixing up of biometrics ---------- (d) Whether enrolment/update was tried in presence of RO officials so as to ensure correct biometrics input? ---- (e) In case R2 is not alive - verification of death certificate ---------- (f) Opportunity provided to candidate/NOK, in case his/her UID is being recommended for omission or deactivation ---------- (g) Consent of the candidate/NOK on omission/suspension of UID ----- (h) Any other information- - - (i) In case earlier issued Aadhaar is to be cancelled justification for the same. **Note: 1. Attach photocopies all relevant documents with each case for reference at UIDAI HQ.** **2. Strike out which are not applicable.**	

Case 4 – Omission/Suspension of Duplicate Aadhaar

4	**Applicant** R1(name) has been issued with two Aadhaars No. XXXX XXXX XXXX & XXXX XXXX XXXX.	1. Resident him/herself informed receipt of two Aadhaar numbers vide letter No.---- dt----- Or Information has been received from------ that R1 has been issued with two UIDs with details thereof.... 2 **Findings of Field Enquiry by RO as per Aadhaar Act 2016 (Regulations 29 & 30) :-** (a) Interaction details with the complainant & candidate ---- (b) EID Details:- (i)	Recommendation duly approved by DDG of the RO ---- ------.

(ii)

(c) Present status of both the UIDs ·····

(d) Circumstances leading to issue of two Aadhaars ·····

(e) **Tech center report of analysis and recommendation on omission:**-

(i) Confirmation that resident has been issued with two UIDs.

(ii) Whether resident biometrics have been captured in both UIDs or one?.

(iii) If Yes, what is the quality of bio in both? Or is poor in one & usable in other (UID No. xxxx xxxx xxxx)

(iv) Reason for generation of two UIDs····

(v) Recommendation for cancellation with reasons.

(g) Any other information·····

3. Specific reasons in case earlier issued Aadhaar is being recommended for cancellation- ·····

4. In case earlier issued Aadhaar is to be cancelled justification for the same.

Note: 1. Attach photocopies all relevant documents with each case for reference at UIDAI HQ.

2. Strike out which are not applicable.

Case 5 – Omission/Suspension of Duplicate Aadhaar of children.

5	**Applicant** R1 (name) has been issued with two Aadhaars No. XXXX XXXX XXXX & XXXX XXXX XXXX.	1. Resident him/herself informed receipt of two Aadhaar numbers vide letter No.···· dt····. Or Information has been received from····· that R1 has been issued with two UIDs with details thereof.... 2. **Findings of Field Enquiry by RO as per Aadhaar Act 2016 (Regulations 29 & 30) :-** (a) Interaction details with the complainant & candidate ····· (b) EID Details:- (i) (ii)	Recommendation duly approved by DDG of the RO ···· ·····

INDEX

(c) Present status of both the UIDs --------

(d) Circumstances leading to issue of two Aadhaars to Miss/Master ----------

(e) **Tech center report of analysis and recommendation on omission:-**

(i) Confirmation that the child has been issued with two UIDs.

(ii) Whether he/she has biometrics in both UIDs.

(iii) If Yes, what is the quality of bio in both? Or is poor in one & usable in other (UID No. xxxx xxxx xxxx)

(iv) Reason for generation of two UIDs----

(v) Recommendation for cancellation with reasons.

(g) Any other information------

3. Specific reasons in case earlier issued Aadhaar is being recommended for cancellation- --------

4. In case earlier issued Aadhaar is to be cancelled justification for the same.

Note: 1. Attach photocopies all relevant documents with each case for reference at UIDAI HQ.

2. Strike out which are not applicable.

F.No.4 (4)/57/268/2015-E&U-II
Government of India
Ministry of Electronics & IT
Unique Identification Authority of India
(E&U-II Divison)

7th Floor, Aadhaar Building,
Behind Kali Mandir, Bangla Sahib Road,
New Delhi-110001
Dated: 30.07.2018

Subject:-Grievance redressel mechanism for Cancellation (Omission) and Suspension (deactivation) of Aadhaar number & Identity information-regarding.

The undersigned is directed to refer to this office letters of even number dated 18.9.2017 & 12.7.2018 on the subject cited above and to inform that Regulation 27 to 31 of Aadhaar (Enrolment & Update) Regulation, 2016 provide for omission or deactivation of Aadhaar number for reasons specified therein, its Communication to the Aadhaar number holder and rectification action required by the resident.

2. UIDAI has instituted a mechanism for residents to report Aadhaar numbers for omission/ deactivation. In addition, UIDAI has also put in place automated systems which identify Aadhaar numbers to be omitted or deactivated.

3. In regard to the same, attention is invited to Regulation 29 of the Aadhaar (Enrollment and Update) Regulations, 2016, which reads as "Any case reported or identified as a possible case requiring omission or deactivation may require field inquiry which may include hearing the persons whose Aadhaar number is sought to be omitted or deactivated". The cases, identified by the automated process generally don't require field enquiry or hearing of the person whose Aadhaar number is identified to be omitted or deactivated.

4. Pursuant to regulation 29 of the Aadhaar (Enrolment & Update) Regulation, 2016, Deputy Director in-charge of the State in respective Regional Office of UIDAI is designated as inquiry officer for carrying field inquiry including hearing the concerned person whose Aadhaar number is sought to be omitted or deactivated. The inquiry officer after due field inquiry and hearing the concerned persons shall submit its report/recommendation through DDG of concerned regional office to UIDAI HQ. The Nodal division of UIDAI HQ upon receiving the report/recommendation of inquiry officer duly recommended by DDG of ROs, may initiate necessary action to omit or deactivate an Aadhaar number.

INDEX

5. The resident shall be communicated about the omission or deactivation of his/her Aadhaar or its revocation as the case may be through SMS/registered e-mail/tele-calling/letter/any other means as deemed fit by UIDAI.

6. Further, any resident whose Aadhaar has been omitted or deactivated due to any reason specified in the regulation will have an option to represent to UIDAI against the decision of omission or deactivation through the grievance redressal mechanism. Accordingly, DDG E&U Division at Head quarter UIDAI is designated as Appellate Authority. The appellate authority shall consider the representation of the residents and convey its recommendation to the UID Authority. The Authority based on recommendation of Appellate Authority shall decide the revocation of omission or deactivation of the Aadhaar number.

7. In case of omissions of Aadhaar number, residents, if entitled, shall have option to re-enroll. In case of deactivation, residents shall be required to update their identity information partially or fully as the case may be, to activate their Aadhaar.

8. This issues with the approval of CEO, UIDAI

(P.K.Jha) 30.7.18
Deputy Director (E&U-II)
Praween.jha@uidai.net.in

Copy to :-
1. All DDGs, RO UIDAI (As per list)
2. DDG (E&U)
3. DDG, Tech Centre, B'lore
4. PS to CEO, UIDAI
5. ADG(E&U-I)/ADG (E&U-II)
6. DD(Legal)
7. Guard File

K -11015/05/2011-UIDAI (ICT)
भारतीय विशिष्ट पहचान प्राधिकरण (यूआइडीएआइ)
अधिप्रमाणन विभाग

तृतीय तल, यूआइडीएआइ मुख्यालय
काली माता मंदिर, बंगला साहिब रोड,
गोल मार्केट, नई दिल्ली - 110001
दिनांक 19.09.2018

Office Memorandum

The Competent Authority in UIDAI has approved revised ICT guidelines for ICT assistance to State governments, Kendriya Vidyala, Javahar Navodaya Vidyalaya and Bharat Sanchar Nigam Limited for creating ICT infrastructure for enrolment. In this regard, guidelines for ICT assistance to states were issued in September 2010 which provisioned for financial assistance up to Rs 10 crore to each state as per EFC approval. Subsequently, additional guidelines were issued in September 2016 for procurement of enrolment kits for supporting enrolment of new born kids and school children, their mandatory biometric update at ages 5 and 15 years and cover remaining adult enrolment/update. Under the additional guideline, States were entitled to receive a maximum of Rs 5 crore (50% of total ICT assistance of Rs 10 crore) for provisioning equipment @ maximum Rs 1.0 Lakh (Rs One Lakh) per enrolment kit.

2. Aadhaar coverage for adult population is reaching saturation barring few states. However, there will be a continuous requirement of enrolment of new born or children between 0 – 5 years of age and mandatory requirement of biometric update at ages 5 and 15 years. These Phase II of ICT guidelines provide assistance to state governments, Kendriya Vidyala Sangathan and Navodaya Vidyalaya Samiti for provisioning of Aadhaar Enrolment Kits (AEKs) to be deployed dedicatedly for enrolment of new born or children between 0 – 5 years of age and mandatory requirement of biometric update at ages 5 and 15 years and their mandatory updates. These revised guidelines also provision for providing assistance to Bharat Sanchar Nigam Limited to set up two Aadhaar Enrolment Kits in each of its Customer Service Centre to provide enrolment and update services to all residents.

3. In this scheme, under the assistance provided to State Education Departments two AEKs per block will be supported which would be moved across various schools and shall be stationed at suitable locations within the designated blocks like Panchayat Samiti, Block Education Officer,

INDEX

Tehsildar office etc. Likewise, the assistance provided to Kendriya Vidyala Sangathan and Navodaya Vidyalaya Samiti would be used to procure and station one AEK in each of KVs/JNVs on a permanent basis. The support provided to BSNL would be used for procuring and deploying two AEKs in each of its Customer Service Centre. In this scheme, financial assistance to the tune of Rs 1.5 lakh per kit would be provided.

4. The funds released under these ICT Guidelines are over above the existing ICT assistance provided to the states.

Encl: Phase II of ICT Assistance guidelines

(दीपाली शर्मा)
सहायक महानिदेशक (अधिप्रमाणन)

To

1. **All Secretaries of State Education Departments**
2. **Commissioner, Kendriya Vidyala Sangathan**
3. **Commissioner, Navodaya Vidyalaya Samiti**
4. **All DDGs of ROs**

Copy to:

1. **All DDGs, Hqrs**
2. **OSD to CEO, UIDAI**

Phase II - Guidelines for Assistance towards ICT Infrastructure for AEK in Schools, Jawahar Navodaya Vidyalaya, Kendriya Vidyalaya, and BSNL Customer Service Centers.

These guidelines are issued in continuation of existing ICT guidelines that were approved in September 2010 and September 2016. The assistance provided under Phase II of additional guidelines is over and above the assistance extended through earlier guidelines.

1. Introduction

1.1 The Government Notification dated 28th January 2009 creating the Unique Identification Authority of India (UIDAI) and defining its mandate and responsibilities has laid down that the UIDAI has the responsibility, among others, for defining mechanisms and processes for interlinking UID with partner databases on a continuous basis, coordinating/liaising with the implementation partners and user agencies as also define conflict resolution mechanism, defining usage and applicability of UID for delivery of various services and issuing necessary instructions to agencies that undertake creation of databases, to ensure standardization of data elements that are collected and digitized and enable collation and correlation with the UID and its partner databases. Further, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 has been enacted by Parliament in March 2016.

1.2 UIDAI was asked to provide support to the Registrars/other departments in their budgets to enable them to make necessary investments in creating ICT infrastructure, for which, fund approvals were provided to UIDAI under UID Scheme. Accordingly, UIDAI had framed policy for ICT assistance in September 2010 that provisioned for support of financial assistance up to Rs 10 crore to each state. Subsequently, additional guidelines were issued in September 2016, wherein States were entitled to receive a maximum of Rs 5 crore (50% of total ICT assistance of Rs 10 crore) for provisioning enrolment kits @ maximum Rs 1.0 Lakh (Rs. One Lakh), for supporting enrolment of new born kids and school children, their mandatory biometric update at ages 5 and 15 years and covering remaining adult enrolment/update.

1.3 Under these guidelines, UIDAI has since provided assistance to several State Governments & Union Territories to help set up infrastructure for integration of schemes with Aadhaar and several States have already started providing Aadhaar enables services and benefits like PDS, pensions, etc. Further, additional support provided under Additional ICT guidelines in 2016 had increased focus on enabling targeted enrolment and update.

2. Current Scenario

2.1 Aadhaar enrolments have crossed 122.33 crore across the country as on 31.08.2018 and Aadhaar is being recognized as a platform for online verification of identity of a resident through the process of Aadhaar authentication and e-KYC; and as a financial address through Aadhaar Payments Bridge. Demand for Aadhaar based service delivery has grown exponentially in recent times and around 91 crore authentication transactions and 22 crore e-KYC transactions are being done every month on an average. It is expected that demand for Aadhaar authentication for availing various services and benefits would increase in future.

2.2 Though the overall Aadhaar saturation of adult population is more than 99%, resident services are required to be provided for enrolment of the left over population, in particular, of the children and new-borns, whose coverage is presently much lower (nearly 52% for 0-5 years and 79% for 5-18 years as on 31 August 2018); and who in addition need mandatory biometric update at ages 5 and 15 years. Therefore, a need is felt to devise a revised scheme to provide assistance to government agencies for provisioning of Aadhaar Enrolment Kits (AEK) to be deployed dedicatedly for enrolment of infants and children including their mandatory biometric updates at 5 and 15 years and ongoing enrolment and update requirement of Aadhaar holders. Accordingly, UIDAI has prepared these additional guidelines for phase II of ICT assistance. The following three categories have been identified to extend financial assistance from UIDAI under Phase II of additional guidelines-

i) **State Governments**- A new stream of ICT Assistance would be provided to States for procuring two AEKs per block in each state. These will be used **only** for targeted enrolment of school children, and their mandatory biometric update at ages 5 and 15 years. These kits would be moved across various schools, and shall be stationed at suitable locations within the designated blocks like Panchayat Samiti, Block Education Officer, Tehsildar office etc. There are nearly 6612* blocks in India as in the year 2012.

ii) **Kendriya Vidyalaya and Navodaya Vidyalaya**- There are a total of around 1200* functional number of KVs in the country[1] and around 600* Jawahar Navodaya Vidyalaya in the country[2]. It has been proposed to provide support for one AEK per school, which will be stationed in the school and used for enrolment/update of Aadhaar data of children belonging to these schools as well as nearby schools.

[1] http://kvsangathan.nic.in/ICTInfrastructure.aspx
[2] http://www.aeparc.org/sites/default/files/resources/AEPMIS%20INV_%20ID.pdf
http://mhrd.gov.in/nvs

INDEX

iii) **Bharat Sanchar Nigam Limited**-Post Offices and Banks have established Aadhaar Enrolment and Update Centres to ensure enrolment/update at trusted locations. Now it has been decided to support the public operator i.e. Bharat Sanchar Nigam Ltd for putting two machines in each of its Customer Support Centre (CSC) which are around 3000* in number.

3. *Quantum of Assistance*

3.1 In this scheme, financial assistance to the tune of Rs 1.5 lakh per AEK would be provided considering that high end computer, duly certified devices with latest technical specifications and enhanced technological features like online ECMP client, GPS systems etc are to be incorporated in the kit for security of the system.

3.2 There are nearly 6612 blocks in India as in the year 2012[3], 1200 KVs, 600 JVNs and 3000 BSNL Customer Service Centre. Hence, an approximate support of around Rs 315 crore for installing 21,024 AEKs at the rate of two in each block and BSNL Customer Service Centre and one in each of the KVs and JNVs. The exact number of blocks, KVs, JVs and CSCs may be provided to UIDAI as in Annexure 1.

3.3 Financial assistance shall be provided only for purchase of AEKs and cost of other infrastructure, deployment of personnel, operating expenses, maintenance, depreciation, replacement of machines at a later date etc may be borne by the respective nodal agency. It is also stated that UIDAI will reimburse the cost of successful Aadhaar generation and update at UIDAI prescribed rates. This will generate revenue which will help meeting the operating expenses of the Aadhaar centres.

3.4 If the nodal agency requires more assistance for setting up higher number of enrolment and update centres for schools and BSNL Customer Service, they may submit their proposal to UIDAI for further assistance.

3.5 The approved fund allocation for enrolment kits as approved in Additional guidelines issued in 2016 is enhanced to Rs 1.5 lakh per kit (maximum).

Nodal Officers and their key responsibility areas for this scheme

i) **State Education Department** -The State Education Department will be Nodal Department and Secretary, State Education Department would be the nodal officer for this category. The funds for procurement of

[3] https://data.gov.in/catalog/number-districts-drdas-blocks-villages-country

* The exact number to be informed by the concerned nodal agency in their requirement proposal as per Annexure 1.

INDEX

AEKs would be released to the Nodal Department for procurement and further distribution of kits in each block in the state. At the district level, the District Magistrate/ District Collector or any other officer as designated by the State Education Department would be the officer in-charge who would decide the movement plan/stationing of the kits. The DM/DC would be empowered to re-distribute the AEKs among blocks in his/her district as per local requirement. The DM/DC will ensure proper implementation and utilization of kits in each block. The District nodal officer will constitute a committee of taluka/block level officials headed by a block nodal officer which will prepare a calendar of dates of camp/deployment of Aadhaar machines in the taluka/block. It should be endeavoured that each school should be covered by Aadhaar camp at least twice a year. It is suggested that a qualified data entry operator may be hired on contract for every Aadhaar machine that will travel from school to school and hold camps in the schools at the designated dates. It shall be ensured that the machines shall be deployed only for enrolment and update of school children and other children below the age of 18.

ii) **Kendriya Vidyalaya and Navodaya Vidyalaya** – The Kendriya Vidyalaya Sangathan and Navodaya Vidyalaya Samiti would be nodal departments and the Commissioner, Kendriya Vidyalaya Sangathan and Commissioner, Navodaya Vidyalaya Samiti would be the respective nodal officers for KVs and JNVs. The funds for procurement of AEKs would be released to the respective Nodal Departments for procurement and further distribution of kits in various schools, where an AEK would be deployed permanently.

iii) **Bharat Sanchar Nigam Limited** – The Chairman and Managing Director, BSNL would be the Nodal Officer. The funds for procurement of AEKs would be released to BSNL and CMD would be the Nodal Officer for procurement and further distribution of kits in various Customer Service Centres across the country, wherein two AEK would be permanently deployed in each Service Centre.

The UIDAI Regional Office of concerned state will closely monitor the implementation of the scheme in the state and also coordinate with the concerned Nodal Department/Nodal Officer for proper utilization of funds released for procuring enrolment kits.

4. Due diligence by UIDAI Headquarters and approval

The Nodal Agency for each category within this scheme would provide the details of number of blocks/schools/CSCs where these AEKs are to be deployed and provide Bank Account details for transfer of funds as given in **Annexure 1**.

INDEX

5. Aadhaar Enabled Kits: composition and procurement guidelines

ICT Assistance would be provided for AEKs comprising of:

(i) Computer/Laptop (with provision for dual screen)
(ii) Web Cam for resident photograph
(iii) Slap Scanner
(iv) Dual Iris scanner
(v) Scanner for documents
(vi) Printer
(vii) GPS Device

The equipment should be purchased only from GeM as detailed in Annexure 2

6. Implementation

6.1 The Nodal Agency for each category within this scheme would provide the details of number of blocks/schools/CSCs where these AEKs are to be deployed and provide Bank Account details for transfer of funds as given in Annexure 1. Funds would be released to the designated Nodal Department, which would procure the equipment centrally and allocate the same to various blocks/schools/CSCs.

6.2 The Nodal Department shall also ensure that the enrolment kits are on-boarded on the UIDAI enrolment system through the State Registrars/State Enrolment Agencies and that certified operators/supervisors are engaged and trained to ensure optimum efficient working of this equipment. The Nodal Department may also become UIDAI Registrars if required.

6.3 The Nodal Department will also monitor the implementation of the project and submit quarterly progress reports and Utilisation Certificates to the concerned UIDAI Regional Offices.

6.4 The UIDAI Regional Offices will obtain the Utilisation Certificates as soon as the funds released are utilized. They will also closely monitor implementation of the scheme by concerned nodal agencies in the states under their jurisdiction.

6.5 The State Governments may contact the concerned ROs for technical assistance and guidance.

*****

INDEX

Annexure 1

F. No.
(Office Name of the State Department/Organization)
(Address of the State Department/Organization)
Date: ...Sep, 2018

To,

Assistant Director General,
Authentication Division,
3rd Floor, UIDAI HQ
Bangla Sahib Road
Behind Kali Mandir, Gole Market
New Delhi-110001

Sub: ICT Assistance for procurement of Aadhaar Enrolment Kit under Phase II of Additional ICT guidelines.

In accordance of UIDAI ICT policy issued vide..... dated..... The school education department (SED)/Kendriya Vidyalaya Sangathan (KVS)/ Navodaya Vidyalaya Samiti (NVS)/ Bharat Sanchar Nigam Limited (BSNL)want to deploy XX (no. of) Aadhaar Enrolment Kits in every block/KV/JNV/CSC for Aadhaar enrolment/Update of children/remaining population in schools/ BSNL's CSCs. The SED/KVS/NVS/BSNL shall engage the operator/supervisor/verifier as per UIDAI policy. The SED will organise camps in schools twice a year. Accordingly fund may be released as per following details:-

a) Name of Organisation/Department:-
b) No. of Proposed blocks/Schools/CSCs to be covered (Provide state/UT/ district wise list):-
c) Total no. of Aadhaar Enrolment Kit proposed to be procured:-
d) Total Amount @ Rs. 1.5 Lakh per Aadhaar enrolment kit:-
e) Bank Details
    i) Bank Name:-
    ii) Account Name:-
    iii) Account Number:-
    iv) IFSC Code:-

(Attached copy of cancelled cheque leaf)

2. Undertaking-

(a) The Department shall procure the AEKs from GeM Portal.

(b) SEDs/KVs/JNVs will use kits only for enrolment/update of school going children or of such age.

(.....)

(Name, Designation, Seal of the Nodal Officer)

Copy to:

Annexure 2

Procurement of Aadhaar Enrolment Kits

1. Aadhaar Enrolment Kit (AEK) shall be procured only from GeM portal (https://gem.gov.in/).

2. UIDAI in consultation with GeM has prepared specifications for AEK & the same has been made available at GEM portal under product name.

3. As per the specification numbered 122 of AEK at GeM portal, there is a requirement to get UIDAI certification from Regional Offices of UIDAI for the working of AEK. (Aadhaar Enrolment Kit comprising of specific make/model of device shall be UIDAI certified for its working with latest UIDAI's enrolment client (ECMP)).

4. Large no of Aadhaar enrolment kits are already certified by Regional Offices of UIDAI and are available at GeM portal.

5. ICT fund shall only be utilized for procurement of Aadhaar enrolment kit from the GeM portal only. In case, there is saving in the fund after procurement of two kits per block, the balance shall be refunded.

6. The AEK shall be used for organizing Aadhaar Enrolment camps in every school twice a year, for enrolment and biometric update of school children only.

F. No 4(4)/57/268/RO-DLI/2017-E&U-II/92
Government of India
Unique Identification Authority of India
******

7th Floor, Aadhaar Building,
Bangla Sahib Road, Gole Market,
New Delhi 110001
Date: 06.02.2019

To

The DDGs, All ROs of UIDAI
(As per list attached)

Sub:-Standard Operating Procedure (SOP) for dealing with cases of deactivation (suspension) of Aadhaar Number of illegal migrants and Fraudulent enrolments/Updates.

*****

Sir,

I am directed to refer to the subject cited above and to inform that competent authority in UIDAI has approved the **Standard Operating Procedure** (SOP) for deactivation of Aadhaar Number of foreign Nationals and fraudulent enrolment/updates. A copy of the same is enclosed as **Annexure-A** herewith for information and necessary action.

Encl: Annexure-A

(S Agrawal)
Asst. Director General(E&U-II)
Tel. 011-23478437.

Copy to:-

(i) MHA(Foreigners' division)
(ii) PS to CEO, UIDAI
(iii) PS to DDG (E&U)
(iv) PS to DDG (Legal)
(v) PS to DDG(Tech)
(vi) PS to DDG(Enf)
(vii) ADG (E&U-I)
(viii) ADG I/C (Tech Centre), UIDAI, Blore
(ix) Guard File

INDEX

Annexure-A

F. No 4(4)/57/268/RO-DLI/2017-E&U-II

Sub:-Standard Operating Procedure (SOP) for dealing with cases for deactivation of Aadhaar Number of Illegal Immigrants and fraudulent enrolments/updates.

*****

Brief:-

1. The Hon'ble Supreme in the matter of Justice K.S. Puttaswamy & Anr. v. Union of India & Ors. in Writ Petition (C) No. 494 of 2012, has directed UIDAI to take suitable measures to ensure that illegal immigrants are not able to take benefits of getting Aadhaar. Also, UIDAI in past has received number of cases from Central/State Ministries, FRRO/FRO, State police, Law enforcement agencies or other Central/State departments for deactivation of Aadhaar issued to Foreign Nationals on the grounds that these Aadhaar numbers have been obtained by them while they were illegal immigrants or over stayed visa period in India. In light of the Judgement of the Hon'ble Supreme Court and in light of cases received for deactivation of the Aadhaar issued to illegal immigrant, it is necessary to device a mechanism to tackle with such cases.

2. **Foreigners** (including foreigners of Indian origin) visiting India on long term (more than 180 days) Student Visa, Medical Visa, Research Visa and Employment Visa are required to get themselves registered with the Foreigners Regional Registration Officer (FRRO)/Foreigners Registration Officer (FRO) concerned having jurisdiction over the place where the foreigner intends to stay, within 14 days of arrival (different periods for residents of certain countries). Ministry of Home Affair (MHA) has also delegated powers to State Governments/UT Administrations/FRROs/ FROs for various visa related services.

3. It may be possible that the foreigners have not registered themselves with the FRRO/FRO or there may be cases where foreigners have entered illegally. Foreigners are bound by the Foreigners Act, 1946. Accordingly, any violations of these provisions by foreigners are dealt under relevant FRRO laws/rules by the authorities concerned.

4. In addition to the Aadhaar enrolment done by illegal immigrants, UIDAI has also received few cases of obtaining Aadhaar fraudulently. UIDAI is committed to ensure that no Aadhaar is issued to illegal immigrant or to anyone who obtains it fraudulently. Hence, this Standard Operating Procedure (SOP) is for dealing with cases for deactivation of Aadhaar Number of Illegal Immigrants and fraudulent enrolments/updates as per the Aadhaar Act and Rules and Regulations framed there under.

Legal Provisions on Aadhaar:

5. After coming into force of the Aadhaar Act, 2016 and Regulations framed thereafter, all issues related to Aadhaar number deactivation are to be dealt in light of the extant provisions contained therein.

6. Section 3 (1) of the Aadhaar Act, 2016, which inter-alia lays down that "every resident shall be entitled to obtain an Aadhaar number by submitting his demographic information and biometric information by undergoing the process of enrolment." Further, Section 2 (v) of the Aadhaar Act defines 'Resident' as "an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment".Aadhaar Act, 2016, Chapter III, Section 9 states that "The Aadhaar Number or the authentication thereof shall not, by itself, confer any right of, or be proof of, citizenship or domicile in respect of an Aadhaar Number holder".

7. **Category of Such Cases**. The cases of issue of Aadhaar to a foreign national may fall into one of the four possible categories and need to be dealt accordingly:-

Case A: Foreigners who have entered the country legally through a valid visa. Such cases are dealt by FRRO/FRO/Police/ Law enforcement agencies. These cases may be sub divided into two categories:-

Case A1: Aadhaar was obtained during valid visa period however the individual has overstayed the Visa duration. In such cases upon receiving complaint, Aadhaar may be deactivated after conducting independent enquiry by RO in terms of Regulation 29 of Aadhaar (Enrolment and Update) Regulations, 2016.

Case A2: Aadhaar was obtained after expiry of valid Visa period. In such cases, upon receipt of complaint, Aadhaar may be deactivated after conducting independent enquiry by RO in terms of Regulation 29 of Aadhaar (Enrolment and Update) Regulations, 2016.

Case B: Foreigners who have entered the country illegally. Such cases are dealt by the FRRO/FRO/Police/ Law enforcement agencies. These cases may be sub divided into two categories:-

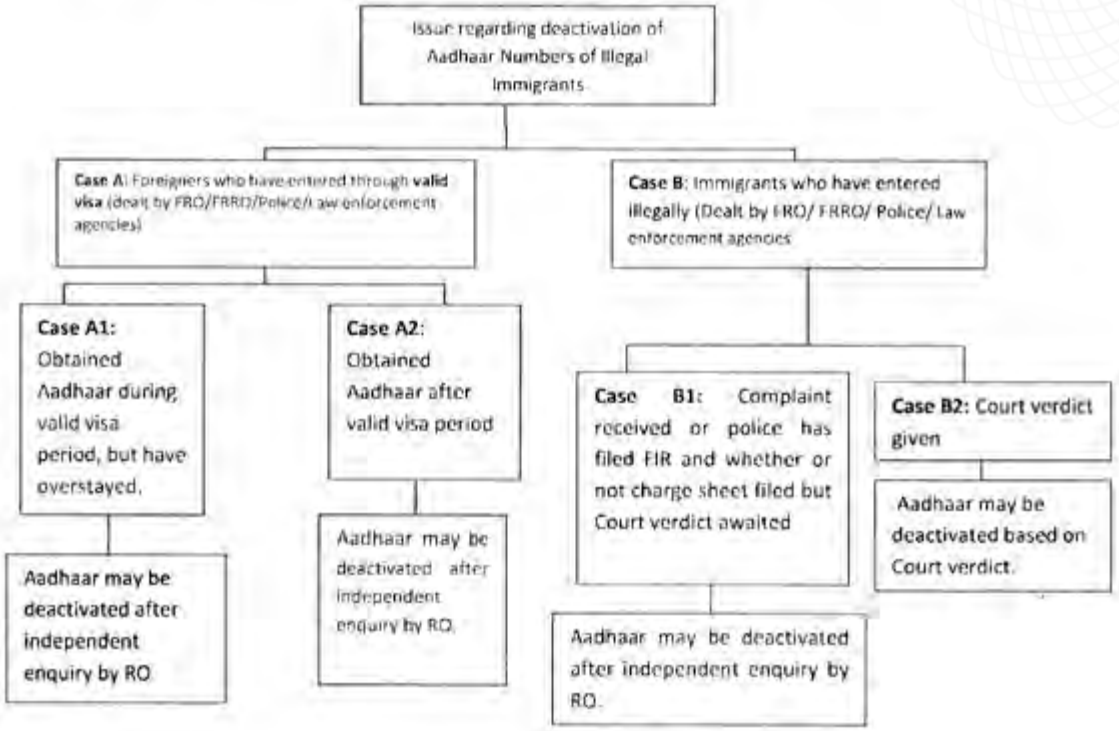
Case B1: Complaint received or Police have filed FIR and whether or not Charge sheet has been filed but verdict is awaited.
In such cases, upon receipt of the complaint or FIR or on the receipt of the information pertaining to framing of the charge sheet, Aadhaar may be deactivated after conducting independent enquiry by RO in

INDEX

terms of Regulation 29 of Aadhaar (Enrolment and Update) Regulations, 2016.

Case B2: Police have filed a charge sheet and Court verdict has been given. In such cases deactivation of Aadhaar may be done upon receipt of Court verdict.

The issue is also explained with the help of a flowchart:-



INDEX

8. **Fraudulent enrolments/Updates** : All such cases which appears to have been enrolled/updated with fraudulent methods/documents, falls within the purview of Regulation 27(1)(iv) of Aadhaar (enrolment and update) regulations 2016,under which Aadhaar shall be cancelled owing to enrolment appearing fraudulent to the Authority. However, before cancellation, the Aadhaar may be deactivated under Regulation 28(1)(f) of Aadhaar (Enrolment and Update) regulations, 2016 after conducting an inquiry under Regulation 29 of the Aadhaar (Enrolment and Update) Regulations, 2016. Action for cancellation of fraudulent cases shall be taken by the Authority after deactivation of the these Aadhaars.

9. In case of all above cases, except case B2, independent enquiry has to be conducted by concerned RO, as notified vide our letter No. 4(4)/57/268/2015-E&U-II dated 31.07.2018 and based on recommendations of RO, decision shall be taken at UIDAI HQ for deactivation of such Aadhaars. During the enquiry by RO if any fraudulent Enrolment/Update is detected, in that case there may be a need of filing FIR by UIDAI (provided no FIR already stands filed in this case), but FIR shall be filed only after approval of UIDAI HQ, through Enforcement division.

10. **Technical issues**: Deactivation of Aadhaar(s) covered under the SoP shall not result in automatic activation post Update by resident. Accordingly, if upon receipt of the required documents/ justification, RO is satisfied that the situation which led to deactivation of Aadhaar as per the above grounds has changed, then on the recommendation of the RO, Aadhaar may be re-activated as per the provisions of the Aadhaar (Enrolment and Update) Regulations, 2016.

11. To deal with deactivation of such cases Central/State Ministries, FRRO/FRO, State police, Law enforcement agencies or other Central/State departments shall approach UIDAI ROs ,located at 8 different locations(Pl refer website uidai.gov.in for address and contact numbers of ROs),under whose jurisdiction their area falls.

12. Immigrants who have been granted the status of refugee may not fall under the category of illegal immigrants and their cases will have to be dealt with separately.

(S Agrawal)
ADG(E&U-II)
Tel. 011-23478437.

5

F.No. 4(4)/57/161/2018/UIDAI-E&U-II(Vol-2)/741
Government of India
Unique Identification Authority of India
(Enrolment & Update Division)
******

7th Floor, Aadhaar Building,
Bangla Sahib Road, Behind Kali Mandir,
New Delhi-110001
Dated: 21.05.2019

To

The DDG
All Regional Offices of UIDAI (As per list attached).

Subject : - Fraudulent Documents Scenarios-reg.
Reference: Letter No. 4(4)/57/363/2018-E&U-II dated 02.04.2019 on Revised Aadhaar Data Quality Check Manual and Guidelines V 2.0 for Pre-ABIS QC- reg.

Sir/Madam,

I am directed to refer to Revised Aadhaar Data Quality Check Manual and Guidelines V 2.0 for Pre-ABIS QC circulated vide Letter No. 4(4)/57/363/2018-E&U-II dated 02.04.2019 and to convey that following amendment are made in guidelines issued vide above quoted letter;

(a) Para 7.2 (1) (h) "Tampered document (Overwriting/Edited/Superimposed details without any attestation by authorising authority) is deleted intoto.
(b) Para 6.3(7) under column "description" is completely modified as under:-

i) **Document of other Person (Excluding Parents/Guardian /persons of same family)**
ii) **Scanning of Object/Screenshot/Picture etc**
iii) **Only Enrolment slip/form is attached in place of Proof documents**
iv) **Tampered Document (Overwriting/Edited/Superimposed details without any attestation by authorising authority)**

2. This issues with the approval of competent authority in UIDAI.

(Manish Gade)
Section Officer (E&U-II)
011-23478408

Copy to:-

1. M/s Tech Mahindra Ltd, A6 Basement, Sector-64, Noida-201301 (Kind attn: Sh. Ateet Dhawan)
2. Writer Business Services Pvt. Ltd34/1-7, Kherki Daula,42nd Mileston NH-8, Gurgaon–122001 (Kind attn: Sh.Jitender Arora)
3. PS to DDG (E&U)
4. Guard file.

INDEX

F.No.4 (4)/57/122 /2012-E&U
Government of India
Ministry of Electronics & IT (MeitY)
Unique Identification Authority of India (UIDAI)
(Enrolment & Update-I)

सत्यमेव जयते

AADHAAR

UIDAI Hqrs. Building
Bangla Sahib Road, N.D.-01
Dated : 05.10.2020.

SUB: **SOP for whitelisted Aadhaar enrolment and update - reg.**

Sir,

Please find attached the revised SOP for whitelisted Aadhar enrolment and update, duly approved by the Competent Authority for further necessary action.

Yours faithfully,

(Prabhakaran C R)
Dy. Director (E&U)

To

1. All UIDAI Regional Office
2. UIDAI Tech Centre.

Copy to

1. PS to DDG (E&U)
2. Guard file.

INDEX

UIDAI

Unique Identification Authority of India
Govt. of India (GoI),
Bangla Sahib Rd, Behind Kali Mandir, Gole Market,
New Delhi - 110001

AADHAAR

SOP FOR WHITELISTED AADHAAR ENROLMENT AND UPDATE

FILE No. 4(4)/57/122/2012-E&U dated 05/10/2020

INDEX

CONTENTS

INDEX

Whitelisted Aadhaar Enrolments and Update

1 Introduction

The concept of whitelisted Aadhaar enrolment and update is an important procedure for UIDAI to resolve those enrolment and update cases which cannot be addressed satisfactorily at the Aadhaar Enrolment and Update Centers for various reasons like mixed biometric scenarios, anomalous biometrics, poor biometrics etc.

Mixed biometrics: It refers to multiple attempts of the same modality (say, fingerprints) belonging to two different individuals.

Anomalous biometrics: In this case, each modality is consistent but different modalities have been captured from different individuals.

Poor biometrics: It refers to the low quality of the biometrics captured.

During initial stages of Aadhaar implementation, in some cases, due to training issues, some of the operators may have partially given their own biometrics instead of the applicant's biometrics. In some other cases, it has been noticed that younger family member has provided her biometrics to senior member for enrolment; consequently, when the younger member tries to enroll, she faces the issue. In such cases matching Aadhaar is deactivated.

To resolve these cases, the matching candidate (who is another Aadhaar holder) needs to update the biometrics. Until the successful update of matching candidate/another Aadhaar holder biometrics, the resident will not get Aadhaar.

2 Objectives

The objective of whitelisted enrolment and update is to facilitate the residents who are unable to get Aadhaar for the above mentioned reasons. On many occasions, it was observed that the matching candidates/another Aadhaar holder are either not traceable or not willing to update or deceased. In such scenario, the resident will never get Aadhaar.

The genuine cases, which meet the pre-requisites requirement given in paragraph 3, would be considered for whitelisted enrollments. These enrolments and updates may be done in UIDAI premises like Regional Offices, Head Quarters, UIDAI run ASKs or any other Government premises. Demographic and biometrics data provided would be certified as genuine by UIDAI officer of the rank not below Assistant Section Officer (Government employee such as ASO, SO, PA, PS, DD etc) and Assistant Manager/Project Manager / Aadhaar Seva Kendra Manager (ASK Manager) or any other employee appointed through NISG. The enrolment / update shall be approved by officer not bellow the rank of Assistant Director General (ADG).

3 Pre-Requisites

3.1 For whitelisted enrolment

3.1.1 Applicant rejected multiple times for re-enrolment

The following scenarios may be referred for the above condition:

1. Multiple rejections of previous enrollments/updates due to biometric issue: UIDAI official should check this scenario thoroughly before white listed enrollment/update of the applicant on admin portal. All EIDs/URNs of new enrolments/updates rejected due to biometric issues shall be forwarded to Tech Support for analyzing the reasons. Tech Support shall suggest for whitelisted enrolment/update of applicant based on such analysis. Only after receipt of the confirmation from Tech Centre, whitelisted enrolment/update should be allowed.
2. The resident has multiple matching candidates as mix biometrics or anomalous biometric or poor biometrics etc. (who are deactivated) and all the candidates have not updated their biometrics. In this scenario, only after receipt of the confirmation from Tech Centre whitelisted enrolment/update should be allowed.
3. The resident's biometrics is of poor quality and is getting rejected as inconsistent. In this scenario also, only after receipt of the confirmation from Tech Centre whitelisted enrolment/update should be allowed.
4. The resident is mentally challenged and biometrics is of poor quality. Re-enrolment may be difficult considering the state of the resident. In such cases also, only after receipt of the confirmation from Tech Centre whitelisted enrolment/update should be allowed.
5. First time biometric update wherein child is updating biometrics at attaining the age of 5 will not be whitelisted.
6. Demographic update is not whitelisted.

3.2 For the whitelisted environment

1. The whitelisted enrolment and update will be done under in presence of UIDAI officer of the rank not below Assistant Section Officer (Government employee such as ASO, SO, PA, PS, DD etc) and Assistant Manager/Project Manager / Aadhaar Seva Kendra Manager (ASK Manager) or any other employee appointed through NISG. The enrolment / update shall be approved by officer not below the rank of Assistant Director General (ADG).
2. The authorization letter in the prescribed template (Annex A) may be scanned and added with other DMS documents during white listed enrolment/update for future references. In case the white listed enrolment is conducted outside RO premises, the following procedure may be followed:

a) The Government official attending whitelisted enrolment should send a scanned copy of the duly signed authorization letter to concerned ADG for approval through official mail id.
b) The ADG should send back the approved authorization letter through official mail id to the concerned official for incorporating the same in the packet along with other DMS documents.

3. Scanned copy of the authorization letter in the prescribed template (Annex A) may be shared along with other relevant documents to Tech Support post enrolment/update for record and future reference.

4 Process Flow

1. RO should share all EID/URN's details with Tech Centre where there are multiple rejections due to biometric issue. Tech Centre will identify the cases where whitelisted enrolments and updates are required and convey the details to RO.
2. UIDAI RO official shall send the request on whitelisted enrolments and updates to Tech Center on completion of enrolment/update.
3. A database table needs to be populated by PMU authorized by ADG Tech Centre for enrolments and updates marked as whitelisted by raising Service Request (SR) to CIDR team.
4. UIDAI RO official should forward the scanned copy of authorization forms and list of EIDs/URNs under whitelisted category to Tech Centre at the end of each day for insertion of these EIDs/URNs in the white listed table.
5. A confirmation from Tech Centre/authorized official for having inserted the EID in the table may be sent back to UIDAI RO official initiating the request.

5 MDD Policy for white listed enrolment/biometric update:

To process the whitelisted enrollments, the following policy changes are in place in manual deduplication (MDD):

5.1 Enrolment Policy Changes:

If there exists a face match and true duplicate biometric match between the whitelisted enrolment (applicant) and the matched enrolment (candidate):

- Applicant is rejected, since he has Aadhaar already. If multiple candidates, deactivate all Aadhaar except the oldest one.

If there exists a face match and anomalous biometric match between the whitelisted enrolment (applicant) and the matched enrolment (candidate):

- Applicant is given Aadhaar and the candidate's Aadhaar is deactivated. If there are multiple candidates, all such Aadhaars are deactivated.

If there is no face match and biometric match is anomalous or true duplicate between the whitelisted enrolment (applicant) and the matched enrolment (candidate):

- Applicant is given Aadhaar and the candidate is deactivated.

5.2 Biometric Update Policy Changes:

If there exists a face match and anomalous or true duplicate biometric match between the whitelisted biometric update and the matched enrolments/updates (candidates):

- Update is approved if it matches with its own master packet (original Aadhaar generated enrolment). Candidates with different Aadhaar numbers get deactivated.

If there exists a face match with master and no face match with other candidates and the biometric match is anomalous between the whitelisted biometric update and the matched enrolments/updates (candidates):

- Update is approved and candidate is ignored.

If there exists a face match with master and no face match with other candidates, biometric match is true duplicate between the whitelisted biometric update and the matched enrolments/updates (candidates):

- Update is approved and the candidates are deactivated.

6 Annexure A

AUTHORISATION FORM

(Ref No._____S.O.P for "Whitelisted Aadhaar enrolment/update", Ref No.: 4(4)/57/122/2012/E&U dated 05/10/2020

Certified that the enrolment /update having Enrolment No./URN _____, in respect of _____ that took place at this Regional Office Name/ HQ/ASK Name/Government Office Name on date : _____ has been carried out in the presence of the undersigned official, and meets the prerequisites mentioned in the S.O.P for "Whitelisted Aadhaar enrolment/update", Ref No.: 4(4)/57/122/2012/E&U dated 05/10/2020.

The detailed facts of the case are as under:

<The facts that necessitated the whitelisted enrolment/update may be mentioned>

The copy of the acknowledgement slip of the enrolment/update and other relevant documents are enclosed.

<Signature>

<Name>

<Designation>

<Signature>

<Name>

<Designation>

<Signature with name, ADG, UIDAI OFFICIAL>

/10505/2021

F.No.HQ-16024/1/2020-EU-I-HQ
Government of India
Ministry of Electronics and IT
Unique Identification Authority of India
****

7th Floor, UIDAI Headquarter,
Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi - 110001
Dated :03-11-2021.

CIRCULAR

Subject: Standard Operation Procedure (SOP) of Name & Gender Update Request under Exception Handling Process

I am directed to forward herewith the revised SOP in respect of Name & Gender Update Request under Exception Handling Process.

This issues with the approval of the CEO, UIDAI.

Yours faithfully,

Signed by Prabhakaran C.r.
Date: 03-11-2021 11:36:29
Reason: Approved

(Prabhakaran C.R.)
Deputy Director (E&U-I)

To,
1. All UIDAI Regional Offices.
2. UIDAI Tech Centre, Bengaluru.
3. All the Registrars and Enrolment Agencies.
4. File.

INDEX

I/10354/2021

HQ 16022/2/2020-EU-I-HQ-Part(1)

Government of India
Ministry of Electronics & Information Technology (MeitY)
Unique Identification Authority of India (UIDAI)
Enrolment & Update Division

Standard Operation Procedure (SOP) of Name & Gender Update Request under Exception Handling Process

NAME UPDATE : Residents can update their name in Aadhaar through the existing process of enrolling by submitting valid document with slight modification as under.

1. The existing practice of updation of Name, i.e., twice in a life time has been revised as under:

S. No.	Change Type	Current Provision	Recommended Provision
1.	Minor Name Edit / Change in initials, surname etc.	Name can be updated twice in a lifetime.	No Change.
2.	Full name change	No explicit guideline	In case of complete name change or change in the first name of the resident, the **Gazette Notification of name change** to be uploaded as PoI document.

2. The following cases shall not be counted as update request in terms of name update chances:

i. A Resident is requesting for updating (correcting) his/her Name, which is to fix a typo mistake by an enrolment operator.
ii. A resident requesting updating (correcting) his/her Name due to transliteration error.
iii. Name update consequent to update of Regional Language of the resident.
iv. ROs to initiate reprocess of such packets by forwarding such cases to Tech Centre with recommendation to reprocess the packet and not to count the update as a chance to update name. The resident shall be eligible for balance chances.

INDEX

I/10354/2021

A detailed workflow depicting the procedure to handle the Name update requests are given at **Annexure-I**. Update requests beyond allowed chances will only be considered through the exception handling process.

3. Name update exception handling cases:

In case of exhaustion of Name update chances, i.e., after exhausting the two chances, ROs may consider the request for Name update under exceptional handling, only if the following conditions are satisfied:-

i. Common scenario wherein Name update is sought at ROs is in case of marriage/divorce/adoption related change. Under exception handling, resident will have to submit the **marriage/divorce/adoption certificate** and request shall be considered by RO. This document will be uploaded under PoI.

ii. A resident may request to append/edit initials in name. For example: 'person named as B I Hirani, would like to expand his first name or last name or both. In such cases, RO may verify if its in-line to the clarifications issued vide letter no. F. No. 4(4)/57/363/2018/UIDAI-E&U-II (Vol. II) dated 30.09.2020(Attached) for Name update.

iii. Resident update his/her name to change the sequence of the existing name; i.e. Rajesh Prasad Sharma requests to update his name as Prasad Rajesh Sharma.

iv. A few cases where a resident might seek complete name change request, like from Pankaj Kumar to Abhinay K Singh. In case of complete name change the **Gazette Notification of name change** to be uploaded as PoI document.

Process to be followed for

i) For scenarios detailed in para 2 above, if the request is getting wrongly rejected during the process, the resident can raise the issue through any mode (directly to RO or through CRM by letter, mail or by calling 1947) and the concerned Regional Offices to reprocess the packet as per the process available for re-processing of wrongly rejected packets. If require, RO may instruct the resident to re-enroll with specific document and submit the EID for further process.

ii) For Scenarios detailed in Para 3,

a) Resident to enrol for Aadhaar update at the nearest enrolment centre with concerned document and intimate UIDAI through mail. In case the resident contacts through 1947, the resident should be advised to reenrol and submit the EID through mail.

b) Once the request received at RO, the request to be verified with due diligence and to be packet to be processed as per the process available for re-processing of wrongly rejected packets.

2

INDEX

I/10354/2021

iii. A detailed workflow depicting the procedure to handle the Name update requests in exception handling is as given at **Annexure II.**

GENDER UPDATE

The Gender related update requests will be handled as under:

i. In case the Gender mistakenly updated by error of enrolment Operator along with some other update:

a) The resident to reenroll for updating the corrected gender and once represent such cases to UIDAI through letter/mail or by calling 1947.

b) Such cases to be assigned to the concerned RO and RO to verify the case along with copy of enrolment form submitted with the packet.

c) ROs to initiate reprocess of such packets by forwarding such cases to Tech Centre with recommendation to reprocess the packet and change the status for number of gender update to zero.

ii. As per the present procedure, Gender update is permitted without any documentary support. Considering the restrictions on number of Gender update, the resident have to submit a medical certificate having photograph issued by surgeon or concerned Authority as POI document.

iii. In case of updation of gender to transgender, the resident will be required to submit a certificate issued by the Central/State Govt as POI document.

iv. A detailed workflow for exception handling in case of Gender update is given in **Annexure-III**.

4. The SOP shall be implemented as follows.

i) In the initial stage, the requests shall be processed under exceptional handling process (manually by verifying/collecting the original or scanned copy of the document) by the concerned Regional office through any mode.

ii) After obtaining Authority approval through E&U-II division, Tech Centre shall be requested to include the list of documents in the client.

iii) After necessary changes in the client, residents shall have provision to submit the documents through client at the time of enrolment.

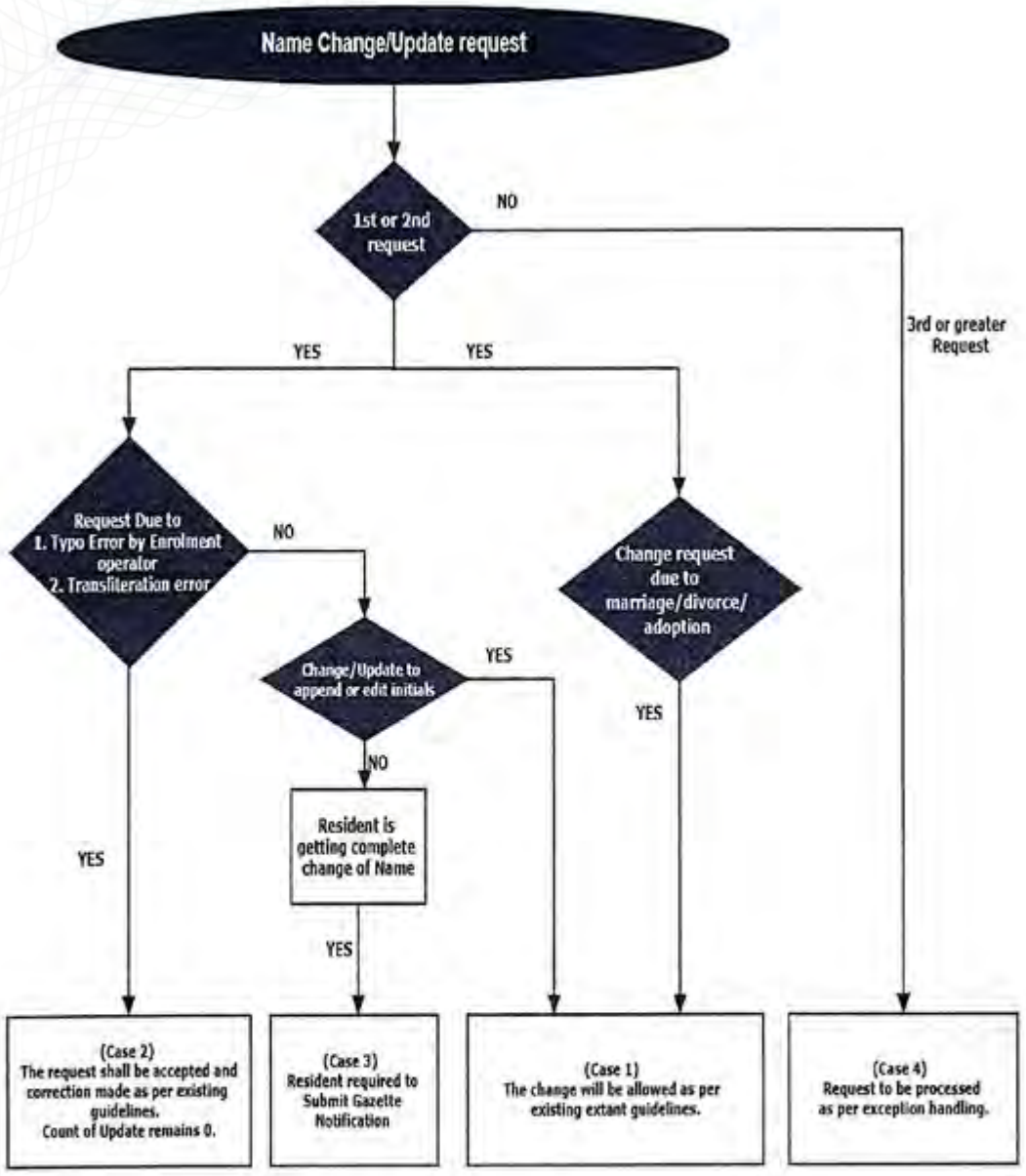
5. This issues with the approval of Competent Authority.

Signed by Prabhakaran C.r.
Date: 28-10-2021 09:05:34
Reason: Approved
Prabhakaran C R
Deputy Director (E&U-I)

INDEX

I/10354/2021

Annexure I

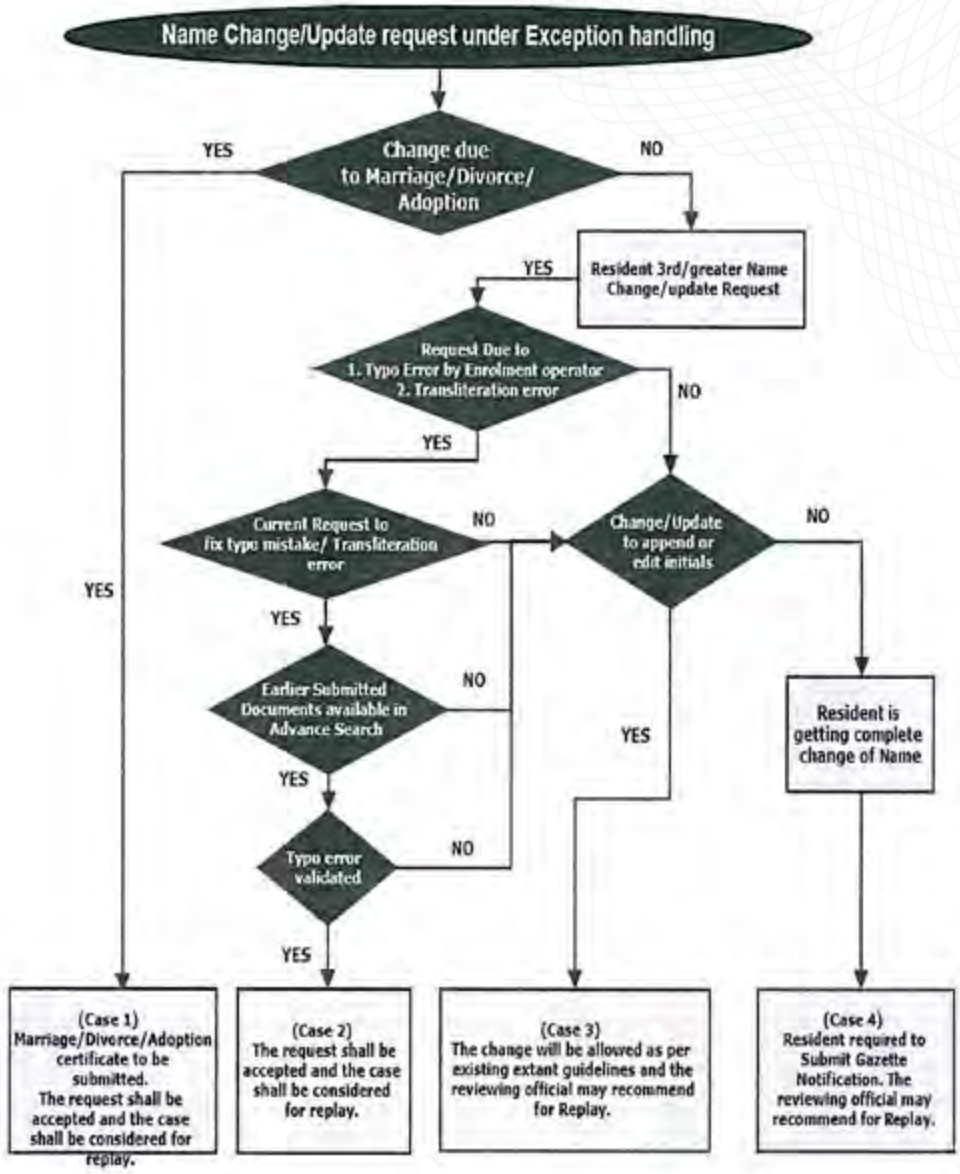


4

INDEX

I/10354/2021

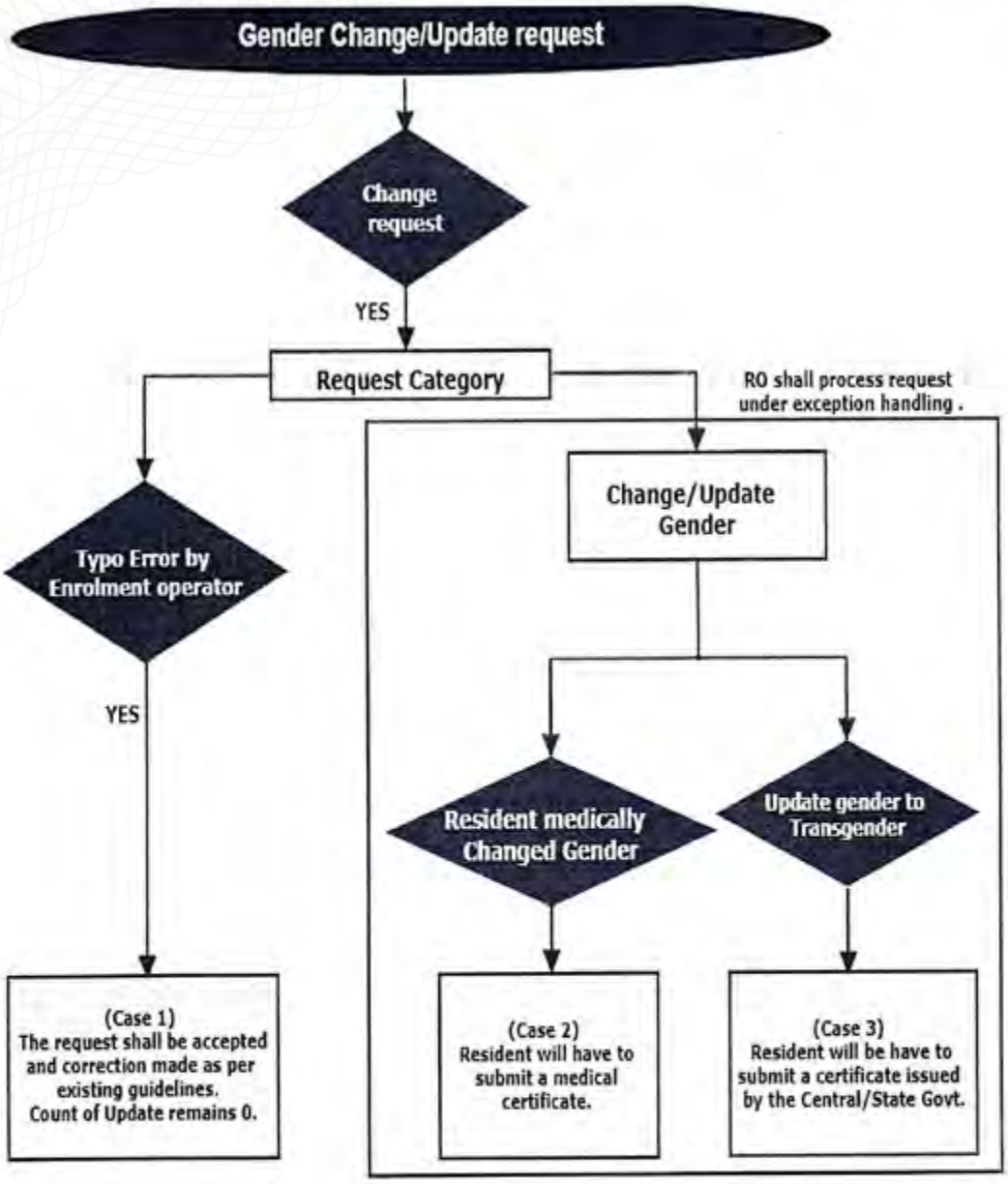
Annexure-II



5

INDEX

Annexure III



6

Guidelines for Assistance towards ICT Infrastructure for Child Enrolment Lite Client (CELC) Kits for Aadhaar Linked Birth Registration (Phase III policy)

These guidelines are issued in continuation of existing ICT guidelines that were approved in September 2010, September 2016 and September 2018. **The assistance provided here under is over and above the assistance extended through earlier guidelines.**

1. Introduction

1.1 The Government notification dated 28th January 2009 creating the Unique Identification Authority of India (UIDAI) and defined its mandate and responsibilities including generation and assignment of UID and defining mechanisms and processes for interlinking UID with partner databases on a continuous basis. Further, the role and responsibilities of UIDAI have been defined and granted statutory status vide 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.

1.2 UIDAI was asked to provide support to the registrars/other departments in their budgets to enable them to make necessary investments in creating ICT infrastructure, for which fund approvals were provided to UIDAI under UID scheme. Accordingly, UIDAI had framed policy for ICT assistance in September 2010 that provisioned for support of financial assistance up to Rs 10 crore to each State. Subsequently, additional guidelines were issued in September 2016, wherein States were entitled to receive a maximum of Rs 5 crore (50% of total ICT assistance of Rs 10 crore) for provisioning enrolment kits @ maximum Rs. one lakh per kit, for supporting enrolment of new born kids and school children, their mandatory biometric update at ages 5 and 15 years and covering remaining adult enrolment/update.

1.3 Under these guidelines, UIDAI has since provided assistance to the tune of Rs. 161.77 crore upto September 2020 to several State Governments & Union Territories to help set up infrastructure for integration of schemes with Aadhaar. Several States are providing Aadhaar enabled services and benefits like PDS, pensions, etc to a large extent. Further, additional

INDEX

support provided under additional ICT guidelines in 2016 had increased focus on enabling targeted enrolment and update.

1.4 Further, Phase II guidelines were approved for providing ICT assistance to State Governments, Kendriya Vidyalaya, Javahar Navodaya Vidyalaya and Bharat Sanchar Nigam Limited for creating ICT infrastructure for enrolment and update. These Phase-II guidelines provided assistance for provisioning of Aadhaar Enrolment Kits (AEKs) to be deployed dedicatedly for enrolment of new born or children between 0-5 years of age and mandatory requirement of biometric update at ages 5 and 15 years. The policy provisioned for assistance of Rs. 315 crore for providing 21,024 AEKs out of which assistance to the tune of Rs. 288.11 crore has been provided upto September 2020.

1.5 With continuous efforts by the State/UT Governments and UIDAI, Aadhaar enrolment has reached 126.43 crore as on 30.09.2020 (122.13 crore being live Aadhaar). Aadhaar is being effectively used for targeted delivery of subsidies, benefits and services as envisaged in the Aadhaar Act, 2016. Direct Benefit Transfer (DBT) portal (dbtbharat.gov.in) indicates savings/gains to the tune of Rs 1,70,377 crore up to December 2019, wherein Aadhaar has played a significant role in identification of beneficiaries and removal of fake/duplicate beneficiaries thereby plugging leakages.

2. Current Scenario

2.1 With 126.43 crore Aadhaar across the country, Aadhaar is being recognized as a simple and useful platform for online verification of identity of a resident through the process of Aadhaar authentication and e-KYC; and as a financial address through Aadhaar Payments Bridge (APB). Demand for Aadhaar based service delivery has grown over the years and around 108 crore authentication transactions and 28 crore e-KYC transactions are being done every month on an average. It is expected that the demand for Aadhaar authentication for availing various services and benefits would increase in future.

2.2 Though the overall Aadhaar saturation of adult population is nearly 89 % and that of 5-18 years is nearly 75%; resident services are required to be provided for enrolment of the left over population, in particular, for the children of 0-5 years age, whose coverage is presently much lower (nearly 24% as on 30.09.2020). Further, enrolment apparatus for this age group is

to be maintained on a regular basis as new population (un-enrolled) keeps adding to this bracket on account of births and enrolled population keeps shifting to 5-18 age bracket. These children can be covered better by providing enrolment facilities in health centres/hospitals & other institutions facilitating child birth and maternal care. Therefore, a need is felt to revise the scheme to provide assistance to Registrar of Births in States/UTs for provisioning of CELC kits (Tablet Computer Android Platform with Single Finger print scanner device) to be deployed dedicatedly for Aadhaar Linked Birth Registration (ALBR) of children (0 to 5 years). To enable integration of Aadhaar enrolment ecosystem with the RGI's birth registration system, CELC has a provision for Aadhaar Linked Birth Registration (ALBR) also. In view of above, UIDAI has prepared these additional guidelines to facilitate enrolment of 0-5 year children through CELC kits at strategic locations whereby Aadhaar number of a child will immediately be generated, with the consent of her parent or guardian, along with registration of her birth.

2.3 As per UIDAI's Child Enrolment Policy, the biometric attributes viz. fingerprint and iris images are not captured in case of children below 5 years of age, thereby making child enrolment process fairly simple in comparison to that of those above 5 years of age. In view of this, an Android based Child Enrolment Lite Client (CELC) has been developed by UIDAI to enable swift enrolment of children below 5 years and facilitate mobile update. The CELC client –

- is installed on handheld tablets for portability.
- facilitates enrolment of children by capturing just the photograph and few demographic details in addition to biometric authentication of parent and operator.
- Enrolment and Update Division issues specifications of the devices to be purchased for installing CELC which are readily available through GeM.
- enables integration with Birth Registration System of RGI- the application is integrated with RGI servers/CRS through an API where the demo details of the child are pulled by the CELC client from RGI server based on Birth Registration Number (BRN)/Birth Application Number (BAN) of the child.

2.4 Since, the Child Enrolment Lite Client runs on an android based tablet plus a single finger print scanner device called as CELC kit[1], financial

[1] CELC kit compatible with mobile handset and iris authentication devices to be specified by E&U Division

assistance for procurement of CELC kits by respective Governments is envisaged for enhancing Aadhaar enrolment of 0-5 year children across different States/UTs of India. In this regard, Women and Childcare Department, Ministry of Women and Child Development and some State Governments already provide assistance under various schemes. To further facilitate enrolment of 0-5 years, it has been decided by UIDAI to supplement the assistance provided by WCD/State Governments by providing financial assistance to Health/Women and Child Welfare Departments/any other Agency responsible for registration of births in the State/UT. These CELC kits will be used exclusively for targeted enrolment of children of 0-5 years of age through ALBR. These kits may be moved across Health Centres/Medical Institutions, Aanganwadis etc. to ensure maximum utilization as well as serving a larger population, the periodicity of which could be decided by the concerned Nodal Agency in coordination with respective Regional Office of UIDAI.

3. Quantum of Assistance

3.1 In this scheme, financial assistance to the tune of Rs 20,000 per CELC kits maximum would be provided considering that tablet, duly certified devices with technical specifications as specified by UIDAI are to be purchased for the CELC kit[1].

3.2 According to Rural Health Statistics for the FY 2018-19 published by Ministry of Health & Family Welfare, Government of India following is the number of different types of Health Centres as on 31.03.2019:

Category of Health Centre	Rural	Urban	Total
Sub-Centers	157411	3302	160713
Primary Health Centers (PHC)	24855	5190	30045
Community Health Centers (CHC)	5335	350	5685
Sub-Divisional/ Sub-District Hospitals (SDHs)		1234	
District Hospitals (DHs)		756	

The financial assistance will be provided from Community Health Centre onwards. The assistance will be for procurement of one CELC Kit per CHC. Further, considering relatively higher density of population in urban areas, financial assistance will be for 2 kits per Sub-Divisional/ Sub-District Hospital and 3 kits per District Hospital. In respect of Metro cities namely Delhi, Mumbai, Kolkata and Chennai, assistance will be one CELC kit per 2 lakh population. As per Census 2011, the cumulative population of the

aforementioned metro cities is around 5.8 crore which is estimated to be approximately 7 crore considering an increase of about 20% since 2011.

3.3 Thus, as depicted in table below, financial assistance of approximately Rs. 21.36 crore will be provided to State/ UT Governments for procurement and deployment of around 10,681 CELC Kits to be utilised exclusively for ALBR purposes.

Community Health Centres	5685
Sub-Divisional/ Sub-District Hospitals @ 2 Kits each	2468
District Hospitals @ 3 Kits each	2268
Metro cities as above (1 Kit @ per 2lakh of population)	350
Total	**10,681**
Total Assistance @ Rs. 20,000 per Kit	**Rs. 21,36,20,000**

3.4 Financial assistance shall be provided only for purchase of CELC Kits and cost of other infrastructure, deployment of personnel, operating expenses, maintenance, depreciation, replacement of machines at a later date etc may be borne by the respective nodal agency. It is also stated that UIDAI will reimburse the cost of successful Aadhaar generation at UIDAI prescribed rates to help meeting the operating expenses of such exercise.

3.5 The essential points regarding release of Assistance are given below:

(i) The assistance will be released in a phased manner with not more than 50% being released in first phase. Next tranche will be released only after getting Utilisation Certificate of previous release in appropriate format to the satisfaction of Authority.

(ii) The maximum assistance released in a single tranche shall not exceed Rs. 50 lakh.

(iii) The Assistance provided under these guidelines should be utilised within one year from the release of grant.

(iv) Any unspent part of the grant should be refunded to UIDAI as soon as the procurement of stipulated number of Kits is done as per the procedure.

(v) Any interest earned on assistance thus released shall be refunded to the Authority and shall not be utilised by the Grantee Agency *suo moto*.

4. Process of approving ICT Assistance

INDEX

The process of providing assistance to State governments for procuring and deploying CELC kits to enable targeted enrolment of 0-5 years' population would involve following stages-

i. Identification of left over population in this age group based on the number of child births per year and uncovered children so far.

ii. Gap analysis – considering the local requirements, States will calculate their requirement and aggregate it over the State. The final requirement to be supported by UIDAI may be arrived at after accounting for availability of kits supported by WCD or any other source. State Government in consultation with RO may consider distribution of kits beyond stipulations depending on local requirements like terrain and uncovered population and provide detailed justification for such consideration.

iii. For States, where existing mobile/tablet devices procured for other schemes are proposed to be used for child enrolment, requirements for only single FP device/iris device or both may be sent with detailed justification.

iv. Nodal Department will prepare a Detailed Project Report (DPR) containing

- WCD/other assistance used by the state,
- number of PHCs/CHCs/SDHs/DHs,
- number of kits required (as per gap analysis),
- justification for requirement,
- details of the Registrar and Enrolment Agencies that would be involved.
- plan of deployment of kits and;
- bank account details.

v. The proposal along with Annexure 1 and DPR is to be submitted to respective UIDAI Regional Office (RO). The proposal must be complete in respect of CELC kit deployment details, name of Registrar and deployment plan.

vi. Regional Office will send the proposal and DPR to HQ along with its due recommendations.

vii. Functional Division in UIDAI HQ will process the proposal based on RO recommendations.

viii. Nodal officer and Nodal Department for implementation of the scheme may be clearly mentioned in the proposal and also in Annexure 1 to be appended with the proposal. The funds for procurement of CELC Kits would be released to the Nodal Department for procurement and further distribution of kits in the state/ UT. The Secretary of the Nodal Department would be empowered to re-distribute the CELC Kits among Health Centres/ Medical Institutions as per local requirement. The Nodal officer will ensure proper implementation and utilization of kits as per DPR.

ix. The UIDAI Regional Office of concerned State will closely monitor the implementation of the scheme in the State and also coordinate with the concerned Nodal Department/Nodal Officer for proper utilization of funds released for procuring CELC Kits.

5. Due diligence by UIDAI Headquarters and approval

The detailed proposal/ request from the State/ UT Government is to be forwarded to UIDAI Headquarters through respective Regional Office along with its due recommendation. The RO will be free to examine the proposal/ request from all angles and may even recommend reduction of kits as requested by the State/ UT.

The Functional Division at UIDAI Headquarters shall consider the proposal and recommendation of RO on the same and only after due diligence in this regard, shall seek approval of the competent authority.

6. CELC Kits procurement guidelines

ICT Assistance under these guidelines would be provided for CELC Kits comprising of:

(i) Android Tablet/Mobile handset (CELC enabled)
(ii) Single fingerprint scanner device or Iris device[2]

The above equipment shall be procured as per the specification provided by the E&U Division, UIDAI in this regard and should be purchased only from GeM as detailed in Annexure 2.

7. Implementation

[2] Curently the CELC client is not compatible with iris devices. E&U division will introduce this compatibility.

INDEX

7.1 The Nodal Agency for each category within this scheme would provide the details of PHCs/CHCs/SDHs/DHs where these kits are to be deployed and provide bank account details for transfer of funds as given in **Annexure 1** (to be annexed with the DPR and proposal). Funds would be released to the designated Nodal Department, which would procure the equipment centrally and deploy them as per DPR.

7.2 The Nodal Department shall also ensure that the CELC kits are on-boarded on the UIDAI enrolment system through the State Registrars/State Enrolment Agencies and that certified operators/supervisors are engaged and trained to ensure optimum efficient working of this equipment. The Nodal Department may also become UIDAI Registrar, if required.

7.3 The Nodal Department will also monitor the implementation of the project and submit quarterly progress reports and utilization certificates to the concerned UIDAI Regional Offices.

7.4 The UIDAI Regional Offices will obtain the utilization certificates as soon as the funds released are utilized. They will also closely monitor implementation of the scheme by concerned nodal agencies in the States under their jurisdiction.

7.5 The State/UT Governments may contact the concerned ROs for technical assistance and guidance.

******

INDEX

Proposal for assistance under Guidelines for 'Assistance towards ICT Infrastructure for Child Enrolment Lite Client (CELC) Kits for ALBR (Phase III Policy')

Annexure 1

F. No.
(Office Name of the state Department / Organization)
(Address of the state Department/ Organization)

Date: ...

Sub: ICT Assistance for procurement of CELC kits under Guidelines for Assistance towards ICT Infrastructure for Child Enrolment Lite Client (CELC) Kits

In accordance of UIDAI Guidelines for 'Assistance towards ICT Infrastructure for Child Enrolment Lite Client (CELC) Kits for ALBR' issued vide.....dated..., the ..... Department, State/UT of ____ wants to deploy XX (no. of) CELC Kits in .....CHCs/SDHs/DHs for Aadhaar enrolment & update of children using CELC kits. The Department will engage the operator/supervisor/verifier as per UIDAI policy. Accordingly funds may be released as per following details:-

a) Name of Organisation / Department:-

b) No. of Proposed CHCs/SDHs/DHs other institutions to be covered (Provide list):-

c) Total no. of CELC Kit proposed to be procured:-

d) Total Amount @ Rs. 20,000/- per CELC kit:-

e) Name of Registrar (s)

f) Name of Enrolment Agency(ies)

g) Bank Details

I. Bank Name:-

II. Account Name:-

III. Account Number:-

IV. IFSC Code:-

(Attached copy of cancelled cheque leaf).

INDEX

2. **Undertaking-**

(a) The Department shall procure the CELC Kits as per the prescribed specifications from GeM Portal only.

(b) These kits will be used only for enrolment of 0-5 years of children under ALBR.

(c) The terms & conditions mentioned in the guidelines in this regard will be followed in totality and at all times.

(.....)

(Name, Designation, Seal of the Nodal Officer)

Annexure 2

Procurement of Child Enrolment Lite Client (CELC) Kits

1. Child Enrolment Lite Client (CELC) Kits shall be procured only from GeM portal (https://gem.gov.in/). The kits with latest version of Andriod /OS may be purchased.
2. UIDAI in consultation with GeM has prepared specifications for these kits and the same has been made available at GEM portal under product name.
3. As per the specification, there is a requirement to get UIDAI certification from Regional Offices of UIDAI for the working of CELC Kits. (CELC Kits comprising of specific make/model of device shall be UIDAI certified for its working with latest UIDAI's enrolment client (CELC).
4. Large no. of CELC kits are already certified by Regional Offices of UIDAI and are available at GeM portal.
5. ICT Assistance funds shall only be utilized for procurement of CELC kits from the GeM portal only.

INDEX

I/10918/2021

F. No.HQ-16024/1/2020-EU-I-HQ-Part(1)
Government of India
Ministry of Electronics & IT (MeitY)
Unique Identification Authority of India (UIDAI)
(Enrolment & Update-I)

UIDAI Hqrs., 7th Floor,
Bangla Sahib Road, NewDelhi-01
Dated : 26 November 2021.

Circular

Sub:- **Standard Operating Procedure (SOP)/ modifications on process for OBD Survey and Complaints received at CRM and Regional Offices : reg**

Ref. : i) Circular No;. F.No.4(4)/57/122/2012/E&U-Pt dated 30.07.2019 and 18.11.2020

1 . **Process to be followed for complaints received on overcharging against an operator through various modes.**

a. CRM to forward all complaints received on over charging by the Enrolment operator to the concerned RO. RO may forward the complaint to respective Registrar for investigation at their end.
b. In addition, ROs may compile complaints received through various channels, (including CRM) and forward the same to Tech Centre by next working day for getting required details for OBD calling. Additionally, ROs to issue show cause notices to the Registrars/EAs with direction to submit their explanation within 15 days of receipt of the notice.
c. On receipt of the information from RO, Tech support to provide the required calling details of the operator to OBD team by next working day. A minimum sample size of 60 mobile numbers of the Residents per operator to be shared as database for OBD survey.
d. CRM to conduct the OBD survey within two workings days and to furnish the details to Tech Centre.
e. The OBD team may obtain 5 or more Qualified Responses from Residents about corrupt practices against an Operator to treat it as fit case for initiation of action against the Operator by completing at least 10 qualified responses/5 overcharging confirmations whichever is earlier

INDEX

I/10918/2021

f. Tech Centre to provide the report to concerned RO by next day.
g. ROs to deactivate the operators reported corrupt with immediate effect and share the details with the SPOC (through email) of the concerned Registrar for immediate action.
h. UIDAI Regional offices may carry out their own investigation (including field investigation) in these cases considering severity of the case.
i. Registrars to furnish a detailed report to the UIDAI Regional Offices within 15 days of receipt of the complaint, which will be reviewed along with Regional Office's own investigation report (if any) and OBD survey report at the next Reconciliation committee (RC) meeting for fixing action against the erring operators and to impose penalty or otherwise against the Registrars as per the guidelines on subject.
j. In case there is no response by the Registrar, within 3 weeks of sharing the details, the case will be considered on merit by UIDAI Regional offices by their own investigation process and action will be taken at the next Reconciliation committee (RC) meeting for fixing action against the erring operators and to impose penalty or otherwise against the Registrars as per the guidelines on subject.

2. **Process to be followed for non complaint cases**

a. In addition to the cases referred through complaint, 3000 operators/supervisors shall be selected every month by Tech centre for OBD survey to get customer feedback. A minimum sample size of 60 mobile numbers of the Residents per operator to be shared as database for OBD survey to the team for conducting survey.
b. The number of operators will be selected in proportion to transactions done by an EA during the preceding month.
c. One operator if already included in previous three months, his data shall not be included for survey.
d. Tech centre to share the calling list to the OBD team of logistic division before 15th of every month
e. The OBD team may obtain 5 or more Qualified Responses from Residents about corrupt practices against an Operator to treat it as fit case for initiation of action against the Operator by completing at least 10 qualified responses/5 overcharging confirmations whichever is earlier. Vague or unclear responses should not be considered for initiating action. If only one resident

I/10918/2021

agrees to submit the complaint in writing and is being ready to participate in the enquiry process, such cases also to be treated as fit case.

f. After completing the survey, the logistic division should furnish the report before 10th of the next month to all ROs, with copy to E&U Division.

g. RO may share the details of the complainant agreed to participate in the enquiry process with Registrar/EA if required.

3. **Process to be followed for both cases.**

a. ROs to deactivate the operators reported corrupt with immediate effect and share the details with the SPOC (through email) of the concerned Registrar for immediate action.

b. ROs to issue show cause notices to the Registrars/EAs with direction to file explanation within 15 days of receipt of the notice

c. UIDAI Regional offices may carry out their own investigation (including field investigation) in these cases considering severity of the case.

d. Registrars to furnish a detailed report to the UIDAI Regional Offices within 15 days of receipt of the complaint, which will be reviewed along with Regional Office's own investigation report (if any) and OBD survey report at the next Reconciliation committee (RC) meeting for fixing action against the erring operators and to impose penalty or otherwise against the Registrars as per the guidelines on subject.

e. In case there is no response by the Registrar, within 3 weeks of sharing the details, the case will be considered on merit by UIDAI Regional offices by their own investigation process and action will be taken at the next Reconciliation committee (RC) meeting for fixing action against the erring operators and to impose penalty or otherwise against the Registrars as per the guidelines on subject.

f. ROs to submit the SRC report to Tech Centre by 10th of next month and Tech Centre to include the recommendations of the ROs in the Deficiency report.

g. Tech centre should shall the Deficiency report before 15th of every month

4. This issues with the approval of Competent Authority.

INDEX

I/10918/2021

Signed by Prabhakaran C.r.
Date: 26-11-2021 21:52:30
Reason: Approved

Prabhakaran C R)

Director (E&U-I)

To

1. All Regional Offices
2. CRM Division
3. Tech Centre

Copy to

1. DDG(E&U)
2. File

INDEX

F.No. HQ-16024/1/2020-EU-I-HQ
GOVERNMENT OF INDIA
Ministry of Electronics & IT
UNIQUE IDENTIFICATION AUTHORITY OF INDIA
(Enrolment & Update Division-I)
*****

7th Floor, UIDAI Headquarters,
Behind Kali Mandir, Bangla Sahib Road,
Gole Market, New Delhi – 110001
Dated : 27th May, 2022

Office Memorandum

Subject: Automated corrective action to strengthen the Aadhaar enrolment ecosystem - reg.
Ref: This office OM F.No. HQ-16024/1/2020-EU-I-HQ-Part(1) dated 25.02.2022 & 17.03.2022.

In continuation to the reference cited above, requests received from eco-system to re-consider the packet upload limit fixed for an operator, considering the fact that an operator is permitted to create 150 packets in a day and the client is permitted to hold up to 100 packets for upload. Accordingly, the OM F.No. HQ-16024/1/2020-EU-I-HQ-Part(1) dated 25.02.2022 modified vide OM of even number dated 17.03.2022 stands revised as under:

Sl.	Criteria	Threshold	Action to be taken
01	Operator doing more than 150 Enrolments/ Update or uploading more than 250 packets in a day	1. Operator creating more than 150 packets in a day. 2. Operator Syncs and uploads more than 250 packets in a day	(a) Operator to be disassociated and machine to be blacklisted from the back end. (Action by Tech Development Division). (b) ROs to ensure enquiry against the operator/machine on priority and action to be initiated in the next SRC meeting. (c) ROs to ensure that the disassociated operators should not be on-boarded before completion of enquiry. [(b) & (c) Action by ROs].
02	Packets created after machine deactivation/ operator disassociation	All the packets created by a disassociated operator from date and time of disassociation of operator/ deactivation of machine.	Packets created after the disassociation/suspension/blacklisting of operator/machine should be rejected. (No change in present practice being followed by Tech Development Division)

INDEX

03	Permission to upload packets after machine deactivation/ operator disassociation	Maximum of 100 packets from a machine/client.	Packets created over and above the threshold should not be accepted.

2. UIDAI MIS Team, GRCP and Fraud Management team to submit the reports regarding Fraudulent Operator / Machine directly to Tech. Development Division with copy to E&U Division and all ROs.

3. Operator/Machines removed as part of cleaning activity can be activated only with RO recommendation.

4. In exceptional cases, Packets not accepted/rejected as per above provisions can be processed only with RO recommendation. Tech. Centre operation would handle few genuine exception cases only. In order to avoid additional burden, such cases should be compiled by RO and send to Tech. Operation Division only once in a month.

5. ROs to take further necessary action against the Registrar/disassociated operator as per the existing policy, as mentioned in OM dated 26.11.2021.

6. This issue with the approval of Competent Authority.

(Satish Kumar Bargujar) 27/05/22
Section Officer (E&U-I)

To,

i. Tech Development Division.
ii. Tech Operation Division.
iii. All UIDAI Regional Offices.

Copy to:

i. OSD to CEO.
ii. PS to DDG (E&U).
iii. CRM Division.
iv. File.

INDEX

HQ-16024/1/2021-EU-II-HQ (E-3469)
Government of India
Unique Identification Authority of India
(Enrolment & Update Division)
******

7th Floor, Aadhaar Building,
Bangla Sahib Road,
Behind Kali Mandir, New Delhi-110001
Dated: 08.04.2022

Office Memorandum

Subject:- Required changes/modifications in UIDAI processes of Child Enrolment, Mandatory Biometric Update and De-duplication for Universal Client.

1. A Committee was constituted vide Office Order F.No. HQ-16024/1/2021-EU-II-HQ (EE-3469) dt 29.06.2021 to review the required changes/modifications in UIDAI processes of Child Enrolment, Mandatory Biometric Update and De-duplication for Universal Client in view of the proposed Amendments to the Registration of Births and Deaths Act, 1969. The recommendations of the said Committee are attached as Annexure I.
2. The recommendations of the Committee were presented before the CEO, UIDAI in a meeting held on 09.02.2022 and the minutes of the said meeting are attached as Annexure- II and Annexure- III respectively.
3. Technology Development Division is, therefore, requested to implement following modification in the existing process in the Universal Client:

S. No.	Existing Process	Modifications required
i.	***Child Enrolment (Bal Aadhaar):*** Currently one parent or HOF Aadhaar number is captured and he/she has to authenticate physically.	***Child Enrolment (Bal Aadhaar):*** Provisions to be developed for cases of Child enrolment under HoF, Aadhaar number of both father and mother shall be captured into the system, while only one parent will be required to perform the authentication physically The required changes shall be incorporated in Universal Client to capture Aadhaar number of the parents. Other scenario needs to be managed as under: i. In case one parent is not available (single parent /window /divorced), other parent authenticates and provides the reason of non availability

INDEX

		of the other parent (as a remarks or dropdown list in the Universal client.) ii. In case both parents are not available (Orphan/other cases), guardian/HoF shall authenticate along with reasons of non availability of the parents (Death/Orphan etc.) and provides Aadhaar number of parents, if available. iii. For enrolment of a child (i.e. under 18 years) other than HoF also, it shall involve the collection of aadhaar of both the parents (or as per exceptions enumerated below).
ii.	**De-duplication Mechanism:** Individual biometric and his/her demographic information is used to identify the duplication in the enrolment process. There are cases where more than one Aadhaar have been issued to the child as in case of child enrolment (0-5yr), biometrics are not captured during the enrolment process. As per the current process, De-duplication is ensured by: i. Biometric De-duplication: Automatic biometric API is used to find possible duplicate and reject the packet. ii. Demographic De-duplication: Identification of possible duplicates based on demographic information and showing the matches in the QC portal for operator to identify the duplicates.	**De-duplication Mechanism:** To ensure De-duplication for child enrolment cases, below set of fields shall be used for identifying the possible matching of demographic de-duplication: i. Name of the Resident (Child) ii. DoB / Age iii. HoF Aadhaar number (In case of HoF) (Aadhaar of both parents- as suggested above) iv. District/State (Address)
iii.	**First MBU:** Currently parent or HoF authentication is not required for providing biometrics on attaining the age of 5 years (first MBU).	**First MBU:** Provisions to be developed for cases of First MBU (After attaining 5 yr, till the age of 18yrs). Provisions to be developed for cases of First MBU (After attaining 5 yr, till the age of 18yrs),

INDEX

		the parent/guardian who has provided his/her Aadhaar as HoF for the child Aadhaar creation, shall perform his/her biometric authentication to ascertain the identity of the child. Also Aadhaar number of both the parents shall be captured into the system, if not captured at the time of enrolment. Other scenario needs to be managed as under: i. In case, HoF is not available, one parent shall perform authentication and provides Aadhaar of the other parent along with the reason of non-availability of the HoF/parent. ii. In case, both parents are not available, guardian shall perform authentication and provides Aadhaar number of the parents (if available) along with the reason of the non availability.

4. A tentative timeline may be indicated by the Technology Development Division to complete the above activities on a priority basis.

R.V.N. Srinivas. 8/4/22

RVN Srinivas
(Director, E & U-II)

To :-
1. ADG , Technology Development.

Copy to:-
1. DDG, Technology Development
2. DDG, Technology Operations.
3. DDG , E & U, UIDAI HQ
4. All Committee Members
5. Guard File

INDEX

I/17382/2022

F.No.HQ-16024/4/2020-EU-I-HQ Part (1)
Government of India
Ministry of Electronics and Information Technology (MeitY)
Unique Identification Authority of India (UIDAI)
(E&U Division)
******

7th Floor, UIDAI Headquarters,
Near Kali Mata Mandir,
Gole Market, New Delhi – 110 001.
Dated: 21st **September, 2022**

Office Memorandum

Sub: Mechanism and protocol to be followed for new enrolment of children (up to the age of 18 years) -reg.
Ref: OM No. HQ-16024/1/2021-EU-II-HQ (E3469) dated 08.04.2022.

At the time of enrolment of a resident above the age of 5 years, demographic details (Name, Gender, DOB and Address) and biometric details (10 finger prints, 2 Iris and facial image) are collected.

2. Whereas in case of child under the age of 5 years, only demographic details and facial image of child are collected at the time of enrolment, alongwith Aadhaar number of one of the parents. This type of enrolment can be conducted through CELC or ECMP client and a Bal Aadhaar with validity upto attaining the age of 5 years is issued to the child.

3. In order to strengthen the Aadhaar ecosystem and reduce the chances of generation of duplicate Aadhaar, it has been decided to collect the Aadhaar number of both the parents along with biometric authentication of one parent at the time of enrolment. In the referred OM No. HQ-16024/1/2021-EU-II-HQ (E3469) dated 08.04.2022 modifications suggested in enrolment for children in the age group of 0-5 years. It has now been decided to extend similar modifications for the age group of 5-18 years also. These services to be extended in existing ECMP and CELC client.

4. In addition to the above, it is also proposed to restrict Birth Certificate only as Proof of Relationship (POR) for child enrolment up to the age of 18 years. Exception mechanism also to be created for accepting approved documents as POR and to collect and record the Aadhaar number of single parent or guardian, if the parents not available at the time of enrolment.

5. Accordingly, following protocol (in brief) is to be followed for new enrolment of children (up to the age of 18 years):

A.1. Aadhaar Enrolment Process for Children (0-5 years).
New Aadhaar enrolment for children between the 0-5 years of age group are carried through following modes:

INDEX

- CELC
  - **Birth Registration Number based Aadhaar Linked Birth Registration** (Currently available for 15 States/UT)
  - Without linking with BRN
- ECMP: Without linking with BRN

A.1.1. Birth Registration Number based Aadhaar enrolment: (Currently available for 15 States/UT, only on CELC, to be extended all States/UT):

- BRN provided by resident at the time of enrolment is sent to respective CRS and data is fetched.
- The Aadhaar number of both parents to be collected. One of the parents will authenticate through biometric authentication. Address of parent shall be fetched as address of the child.
- Valid Proof of Relationship document (Birth Certificate issued by RGI), is used as POR & DOB document.
- Facial image of Child is captured.

A.1.2. Without linking with Birth Registration Number (Aadhaar Linked Birth Registration) based: (both on CELC & ECMP)

- The Aadhaar number of both parents to be collected. One of the parents will authenticate through biometric authentication. Address of parent shall be fetched as address of the child.
- Child's demographics (Name, Gender, DoB) shall be entered in the client based on data in Birth Certificate.
- Valid Proof of Relationship document (Birth Certificate issued by RGI), is used as POR & DOB document.
- Facial image of Child is captured.

B. Aadhaar Enrolment Process for Children (5-18 years)

- The Aadhaar number of both parents to be collected. One of the parents will authenticate through biometric authentication. Address of parent shall be fetched as address of the child.
- Child's demographics (Name, Gender, DoB) shall be entered in the client based on data in Birth Certificate.
- Valid Proof of Relationship document (Birth Certificate issued by RGI), is used as POR & DOB document.
- Full biometric details i.e. facial image, 10 fingerprint and both Iris of child are to be captured.

INDEX

I/17382/2022

C. Exceptions:

Provision should be created in the client for following exceptions for enrolment.

Sl. No.	Scenario	Exception
01.	Provision to collect Aadhaar number and authentication of guardian after recording the reason for non-availability of parent/ parent Aadhaar number at the time of enrolment. (to be applicable for child under 0-18 age group).	• In case one parent is not available (single parent/ window/divorced), other parent authenticates and provides the reason of non availability of the other parent (as a remarks or dropdown list.) • In case both parents are not available (Orphan/ other cases), guardian/ HoF shall authenticate along with reasons of non availability of the parents (Death/Orphan etc.) and provides Aadhaar number of parents, if available.
02	Non availability of Birth Certificate as POR for children at Child Care Institutions (CCIs), born outside the country etc. (Age group of children in 0-18)	Provision to collect any other document as approved (such as Certificate issued by CCI, Passport etc), after recording reason for non availability of Birth Certificate.
03	Exception for Birth Certificate in the age group of 5-18 years	Provision to collect any of the following document after recording reason for non availability of Birth Certificate. 1. Passport 2. Ration card/PDS Card. 3.CGHS/ECHS/ESIC/Medi Claim Card with Photo issued by Central/State Govts/PSUs. 4. Any other Central/ State Government issued family entitlement document 5. Photo ID card issued by Central/State Govt. like Bhamashah, Jan- Aadhaar,

INDEX

I/17362/2022

		MGNREGA card, ARMY canteen card etc. 6. Any other document as approved by the Authority in this regard from time to time.

4. This exercise may be completed within 31st October 2022.

5. This issues with the approval of Competent Authority.

Encl: OM dated 08.04.2022 as stated above.

Signed by Psabhakaran C.r.
Date: 21-09-2022 10:43:49
Reason: Approved (C R)

Deputy Director (E&U-I)

To
The Director,
Tech Development Division,
UIDAI, Bengaluru.

Copy to

1. OSD to CEO
2. Tech Operations Division
3. All UIDAI Regional Offices.
4. Legal Division, UIDAI.
5. File.

INDEX

I/20186/2023

HQ-16024/4/2022-EU-I-HQ-Part (1)
Government of India
Ministry of Electronics & IT (MeitY)
Unique Identification Authority of India (UIDAI)
(Enrolment & Update-I)
*****

7th Floor, UIDAI Headquarters
Behind Kali Mandir, Bangla Sahib Road
Gole Market, New Delhi-110001
Dated: 12 January, 2023

OFFICE MEMORANDUM

Subject: Strengthening of Aadhaar Enrolment Ecosystem **- Aadhaar services by Registrars/EAs not working under in-house model-** reg.

Ref: OM No. HQ-16024/4/2020-EU-I-HQ Part (1) dated 14.10.2022.

1. This Office Memorandum is being issued in partial modification of OM dated 14.10.2022 mentioned under reference.
2. In order to ensure proper monitoring and to ensure enrolment at a secured environment, the concept of in-house model was introduced. The enrolment centres functioning under the following conditions shall be considered as working under **in-house model**:

   Category A- Ministries/Departments/Agencies of Central/ State Government:

   i. Machine (AEK) owned by the Registrar/EA (procured using ICT assistance from UIDAI/GoI or procured using own fund of State Registrar/EA)

   ii. AEK is located and functioning from Government premises under the overall supervision of a Government official.

   Category B- Other Registrars:

   i. Machine (AEK) owned by the Registrar/EA

   ii. Operator/Supervisor: Employee/contract employee on roll of the Registrar/EA or hired from a manpower hiring agency on salary basis.

3. **Registrar/EAs not working under in-house model shall be permitted to provide Aadhaar services in the manner**

INDEX

I/20186/2023

prescribed as under:

Cat-I	Registrar/EA not working under in-house model and willing to shift **en-masse** to in-house model within 31.03.2023.	The Registrar shall continue to provide all the enrolment and update services. The migration to in-house model to be completed by 31.03.2023. (*Adult enrolment shall be regulated as per OM No.HQ-16011/2/2022-EU-I-HQ. dated 21st Oct 2022*).
Cat-II	Registrar/EA not working under in-house model and proposing to shift to in-house model **partially** within 31.03.2023.	The Registrar shall continue to provide all the enrolment and update services under in-house model with the existing EA Code. The migration to in-house model to be completed by 31.03.2023. (*Adult enrolment shall be regulated as per OM No.HQ-16011/2/2022-EU-I-HQ. dated 21st Oct 2022*). Remaining operators not working under in-house model to be de-boarded from existing EA Code and shifted to new EA Code with fresh Registration within 31.03.2023. These operators shall be permitted to operate Update Client Lite (UCL) having provision for address update, mobile/email update and document update.
Cat-III	Registrar/EA not working under in-house model and also proposing not to shift to in-house model within 31.03.2023	Existing services will continue till 31.03.2023. Thereafter, the existing EA Code will be migrated to UCL with provision for address update, mobile/email update and document update.

4. Process to be followed by respective stakeholders:

i. Registrar to submit a plan for migration to new EA Code, if required, to Regional Office along with request for new EA Code by 31st Jan 2023.

0186/2023

ii. Request of Registrar for new EA Code to be forwarded to HQ with RO recommendation by 15th February 2023.

iii. HQ to allot new EA Code to the Registrar for migrating and ROs to complete on-boarding process by contacting Tech Centre as per the existing process.

iv. ROs to share the Station IDs of AEKs to be migrated to the new EA Code and Tech Centre to complete the registration process in a time bound manner.

v. The entire migration process to be completed by 31.03.2023.

5. Post 31.03.2023, the services available in UCL client shall be restricted to with provision for address update, mobile/email update and document update only.
6. The policy is applicable for ECMP/UCL clients only.
7. This issues with the approval of Competent Authority.

Signed by Prabhakaran C.r.
Date: 12-01-2023 14:41:24
Reason: Approved

(Prabhakaran C R)
Deputy Director (E&U-I)

To,

1. All UIDAI Regional Offices.
2. Tech Development Division and
3. Tech Operations Division.

Copy to:

1. All Registrar/EAs
2. ASK Service Providers
3. Legal Division

INDEX

I/20559/2023

HQ-16024/4/2020-EU-I-HQ-Part (1)
Government of India
Ministry of Electronics & IT (MeitY)
Unique Identification Authority of India (UIDAI)
(Enrolment & Update-I)
*****

7th Floor, UIDAI Headquarters,
Behind Kali Mandir, Bangla Sahib Road,
Gole Market, New Delhi-110001.
Dated: 30 January, 2023

OFFICE MEMORANDUM

Subject: Strengthening of Aadhaar Enrolment Ecosystem – Aadhaar services by Registrars/EAs not working under in-house model reg.

Ref: OM No. HQ-16024/4/2020-EU-I-HQ Part (1) dated 14.10.2022 & 12.01.2023.

1. This Office Memorandum is being issued in continuation to and partial modification of the OM dated 12.01.2023 on the subject cited above.

2. In order to ensure proper monitoring and to ensure enrolment at a secured environment, the concept of in-house model was introduced. The enrolment centres functioning under the following conditions shall be considered as working under **in-house model:**

Category A- Ministries/Departments/Agencies of Central/State Government:

i. Machine (AEK) owned by the Registrar/EA (procured using ICT assistance from UIDAI/GoI or procured using own fund of State Registrar/EA)
ii. AEK is located and functioning from Government owned/hired premises under the overall supervision of Government official.

Category B - Other Registrars:

i. Machine (AEK) owned by the Registrar/EA
ii. Operator/Supervisor: Employee/contract employee on roll of the Registrar/EA or hired from a manpower hiring agency on salary basis.
iii. AEK is located and functioning from Registrar/EA premises.

3. Registrar/EAs not working under in-house model shall be permitted

INDEX

20559/2023

to provide Aadhaar services in the manner prescribed as under:

Cat-I	Registrar/EA not working under in-house model and willing to shift **en-masse** to in-house model within 31.03.2023.	The Registrar shall continue to provide all the enrolment and update services. The migration to in-house model to be completed by 31.03.2023. (Adult enrolment shall be regulated as per OM No.HQ-16011/2/2022-EU-I-HQ. dated 21st Oct 2022).
Cat-II	Registrar/EA not working under in-house model and proposing to shift to in-house model **partially** within 31.03.2023.	The Registrar shall continue to provide all the enrolment and update services under in-house model with the existing EA code. The migration to in-house model to be completed by 31.03.2023. (Adult enrolment shall be regulated as per OM No.HQ-16011/2/2022-EU-I-HQ. dated 21st Oct 2022). Remaining operators not working under in-house model to be de-boarded from existing EA Code and shifted to new EA Code with fresh Registration within 31.03.2023. These operators shall be permitted to operate Update Client Lite (UCL) having provision for address update, mobile/email update and document update.
Cat-III	Registrar/EA not working under in-house model and also proposing not to shift to in-house model within 31.03.2023	Existing services will continue till 31st March, 2023. Thereafter, the existing EA code will be migrated to UCL with provision for address update, mobile/email update and document update.

4. Process to be followed by respective stakeholders:

i. Registrar to submit a plan for migration to new EA Code, if required, to Regional Office along with request for new EA Code by 31st Jan 2023.

ii. Request of Registrar for new EA Code to be forwarded to HQ with

59/2023

RO recommendation by 15th February 2023.

iii. HQ to allot new EA Code to the Registrar for migrating and ROs to complete on-boarding process by contacting Tech Centre as per the existing process.

iv. ROs to share the Station IDs of AEKs to be migrated to the new EA Code and Tech Centre to complete the registration process in a time bound manner.

v. The entire migration process to be completed by 31.03.2023.

5. Post 31.03.2023, the services available in UCL client shall be restricted to with provision for address update, mobile/email update and document update only.

6. The policy is applicable for ECMP/UCL clients only.

7. This issues with the approval of Competent Authority.

Signed by Prabhakaran C.r.
Date: 30-01-2023 16:06:53
Reason: Approved

(Prabhakaran C R)
Deputy Director (E&U-I)

To,

1. All UIDAI Regional Offices.
2. Tech Development Division and
3. Tech Operations Division.

Copy to:

1. All Registrar/EAs
2. ASK Service Providers
3. Legal Division

INDEX

21857/2023

F.No.HQ-16024/4/2020-EU-I-HQ-Part (1)
Government of India
Ministry of Electronics & IT (MeitY)
Unique Identification Authority of India (UIDAI)
(Enrolment & Update-I)
*****

7th Floor, UIDAI Headquarters,
Behind Kali Mandir, Bangla Sahib Road,
Gole Market, New Delhi-110001.
Dated: 23rd March, 2023

OFFICE MEMORANDUM

Subject: Partial Modification in Revised Terms of Engagement - reg.

Ref: Revised Terms of Engagement issued vide OM of even number dated 29.09.2022.

This Office Memorandum is being issued in continuation to and partial modification of the revised Terms of Agreement Engagement (ToE) issued vide OM F.No. HQ-16024/4/2020-EU-I-HQ-Part (1) dated 29.09.2022.

2. In view of clarifications sought by various ROs and the legal opinion received, the Competent Authority has accorded approval for following amendments in **Clause -5 and H** of the revised Terms of Engagement (ToE):

CLAUSE - 5

In the case of the Registrars who had signed the original MoU/ToE/ToA with UIDAI prior to execution of the Revised Terms of Engagement, the date of execution shall be accepted by both parties as the same date which was the date of execution of the original MoU/ToE/ToA. The Registrar may exit the Aadhaar Ecosystem as per the Exit Policy in Clause - I.

[H] Dispute Resolution

In the event of any dispute or difference between the parties hereto, such disputes or differences shall be resolved amicably, within 90 days, by mutual consultation. If such resolution is not possible, then unresolved disputes or differences shall be referred for arbitration by the sole arbitrator, to be mutually appointed by the parties.

INDEX

File No. HQ-16024/4/2020-EU-I-HQ-Part(1) (Computer No. 3657)

21857/2023

case of new Registrars or Registrars yet to sign the TOE, the amended TOE may be signed. (copy attached).

4. This issues with the approval of Competent Authority.

Geetha
23/03/2023
(Geetha Sreedhar)
Deputy Director (E&U)

To,

All UIDAI Regional Offices.

I/22159/2023

F.No. HQ-16024/4/2020-EU-I-HQ-Part(1)
Government of India
Ministry of Electronics & IT (MeitY)
Unique Identification Authority of India (UIDAI)
(Enrolment & Update-I)
*****

7th Floor, UIDAI Headquarters,
Behind Kali Mandir, Bangla Sahib Road,
Gole Market, New Delhi-110001
Dated: 05 April, 2023.

OFFICE MEMORANDUM

Subject: Home Enrolment Service for senior citizens/ bedridden/ infirm/ persons with disabilities (Divyangjan) etc on chargeable basis -reg.

UIDAI has the mandate to issue unique identification number (UID) called "Aadhaar" to all eligible residents of India as well as NRIs on their arrival in India.

2. As the Aadhaar platform is being used to deliver various Government welfare services and benefits to the residents, the requirement of Aadhaar enrolment and update has emerged as a prime requirement among all segments of populace of the country.

3. UIDAI has been of late receiving requests from the residents for providing home enrolment facility, especially for senior citizens/bedridden/infirm/ persons with disabilities (Divyangjan) etc. Based on merit, UIDAI Regional Offices have been attending to such requests for home enrolment through the Registrars. However, considering the additional cost involved and absence of a specific policy or guidelines in this regard, the Registrars were reluctant to attend to such requests. The Authority noticed that this leads to inordinate delay or denial in providing home enrolment services to the needy residents.

4. As part of improving the ease of living and enhancing citizen centric approach, the Competent Authority approved the following process to address the home enrolment requests received by UIDAI Regional Offices through various channels.

General Guidelines:

a. The home enrolment service shall be extended on prior approval of the Regional Offices through UIDAI Registrars using ECMP client.

b. Home enrolment service will be extended only to senior citizens/ bedridden/infirm/ persons with disabilities (Divyangjan) on payment of service charges @Rs. 700/- (including GST).

c. While submitting the requests for home enrolment to Regional

INDEX

I/22159/2023

Offices, the resident to submit a copy of Medical Certificate from Registered Medical Practitioner, proof of age or copy of Disability ID card to prove the eligibility.

d. The home enrolment service charges will be charged in addition to normal fee applicable for each transaction of demographic/ biometric update in Aadhaar as notified by UIDAI from time to time. If the service is availed by more than one resident at the same address (as per Aadhaar), Rs 700/- service charge (including GST) will be charged for first resident and @ Rs 350/- (including GST) for each additional resident.
e. Residents opting for this service to make the payment at the time of enrolment and the Registrar to provide a Tax Invoice to the resident, clearly mentioning the charges applied.
f. In case of National Social Assistance Program (NSAP) Pension Scheme beneficiaries, a copy of the Pension Sanction Order containing Beneficiary ID (specimen attached) to be submitted along with the request. The home enrolment facility may be provided to such residents through the State Government Registrar in camp mode at regular intervals without any home enrolment service charges subject to willingness of the State Government Registrar. However, normal fee applicable for update of demographic/ biometric fields in Aadhaar as notified by UIDAI from time to time will be charged from such residents also. The eligibility of such beneficiaries to be verified by UIDAI RO at https://nsap.nic.in/statedashboard.do?method=intialize using the Beneficiary ID of the applicant.
g. Enrolments conducted outside the enrolment centres, without prior approval of Regional Office, shall be considered as irregular and be dealt with accordingly.
h. Regional Offices to map the service through the nearest Aadhaar enrolment centre available for home enrolment to make the service cost effective. In case UIDAI run ASKs are available at reasonable distance, the service to be arranged through ASK.
i. In case of request from residents for mobile number update, the possibility of updating mobile through IPPB to be explored. For address or document update services, the resident to be advised to avail of myAadhaar portal. UIDAI Regional Offices to consider home enrolment service for such cases only after due diligence.
j. Request for home enrolment shall not be considered as a matter of right and the service shall be arranged based on merit and other factors.

Home Enrolment Process:

a. The home enrolment request, along with valid supporting documents for Aadhaar enrolment/ update, should be submitted to the nearest UIDAI Regional Office/ State Office through email. The

INDEX

I/22159/2023

contact details of UIDAI Regional Offices/State offices are available at https://www.uidai.gov.in/en/contact-support/regional-offices.html

b. On receipt of home enrolment request, Regional Office to verify the submitted documents and approve or reject the request, as the case may be, and assign the task to the Registrar within 2 (two) working days under intimation to the resident. RO to also share a copy of the verified documents with the Registrar while assigning the task.
c. Once the Registrar is assigned the task, the Registrar shall fix the appointment with resident so as to complete the service within 7 days under intimation to the Regional Office. If slots are not available, the waiting time may go beyond 7 days (but not later than 15 days) for which the applicant and the Regional Office shall be informed by the Registrar within 2 (two) days of receiving the communication from the Regional Office.
d. The resident shall have option to cancel the request at least 48 hours prior to the scheduled appointment by intimating the Regional Office/ State Office concerned and the mapped Registrar/Operator.
e. In case where the services couldn't be completed due to issues at resident level (non-availability of the resident, non-production of valid document(s), non- availability of power etc.) the service charges to be paid by the resident.
f. On completion of the service, the same should be intimated to Regional Office along with details of EID for monitoring the request status.
g. In case the request is rejected due to technical issues, Regional Office to arrange re-processing of such requests by the Tech Operations.
h. In case resident's request is not successful due to any technical issues on first home enrolment service, and cannot be reprocessed, the Registrar to provide one more visit to the resident free of cost within 10 days from rejection of the request.

5. This issues with the approval of Competent Authority.

Signed by Prabhakaran C.r.
Date: 05-04-2023 12:06:04
Reason: Approved

(Prabhakaran C R)
Deputy Director (E&U-I)

To,

1. All UIDAI Regional Offices
2. UIDAI ASK Service Providers
3. All UIDAI Registrars /EAs

INDEX

I/22159/2023

Copy to:

1. All HQ Divisions
2. Tech Development Division
3. Tech Operations Division
4. File

INDEX

F. No. HQ-16011/2/2022-EU-I-HQ- Part (1)
Unique Identification Authority of India
Enrolment and Update Division

UIDAI Head Office Near Kali Mata Mandir
Gole Market, New Delhi – 110 001
Dated 8th December 2023

Office Memorandum

Subject: Aadhaar enrolment for persons with special needs and disabilities-reg.

In line with Government of India's commitment to ensure inclusion for digitally enabled access to benefits and services, UIDAI has made special provision in regulation 6 of the Aadhaar (Enrolment and Update) Regulations, 2016 and has issued Biometric Exception Enrolment Guidelines dated 1st August 2014 laying down the procedure for enrolling persons who have missing fingers, the biometrics of whose fingers cannot be captured due to any reason (such as a cut, bruise, bandage, worn-out or bent fingers due to old age or leprosy), or the biometrics of whose irises or both fingers and irises cannot be captured due to any reason. A person who is eligible for Aadhaar but unable to provide fingerprints may enrol using only iris scan. Similarly, an eligible person the biometrics of whose irises cannot be captured due to any reason may enrol using only her/his fingerprint. Further, an eligible person who is unable to provide both finger and iris biometrics may enroll without submitting any of the two.

2. For such persons, under the Biometric Exception Enrolment Guidelines, the name, gender, address and date/year of birth are to be captured along with the available biometrics while highlighting the missing ones in the enrolment software, a photograph is to be taken in the manner specified in the Guidelines to highlight the unavailability of finger(s) or iris(es) or both, and the Supervisor of the Aadhaar enrolment centre is to validate such enrolment as an exceptional enrolment. Thus, every eligible person who undergoes the enrolment process by submitting the required information may be issued an Aadhaar number, irrespective of any inability to provide biometrics.

3. However, an instance has recently come to notice of an eligible person undergoing the enrolment process but not getting an Aadhaar number since the Aadhaar enrolment operator did not follow the exception enrolment procedure.

4. In order to avoid recurrence of such processing, the Registrars and enrolment agencies are advised to take all necessary steps, including dissemination of knowledge and awareness and sensitisation through training, to ensure that all Aadhaar enrolment operators are made aware of the exceptional enrolment procedure, follow the same, and render the persons undergoing such enrolment necessary assistance.

INDEX

5. An informative poster in this regard, for public knowledge, is enclosed herewith. Display of the same may be ensured at all Aadhaar enrolment centres.

6. This issues with the approval of the Chief Executive Officer.

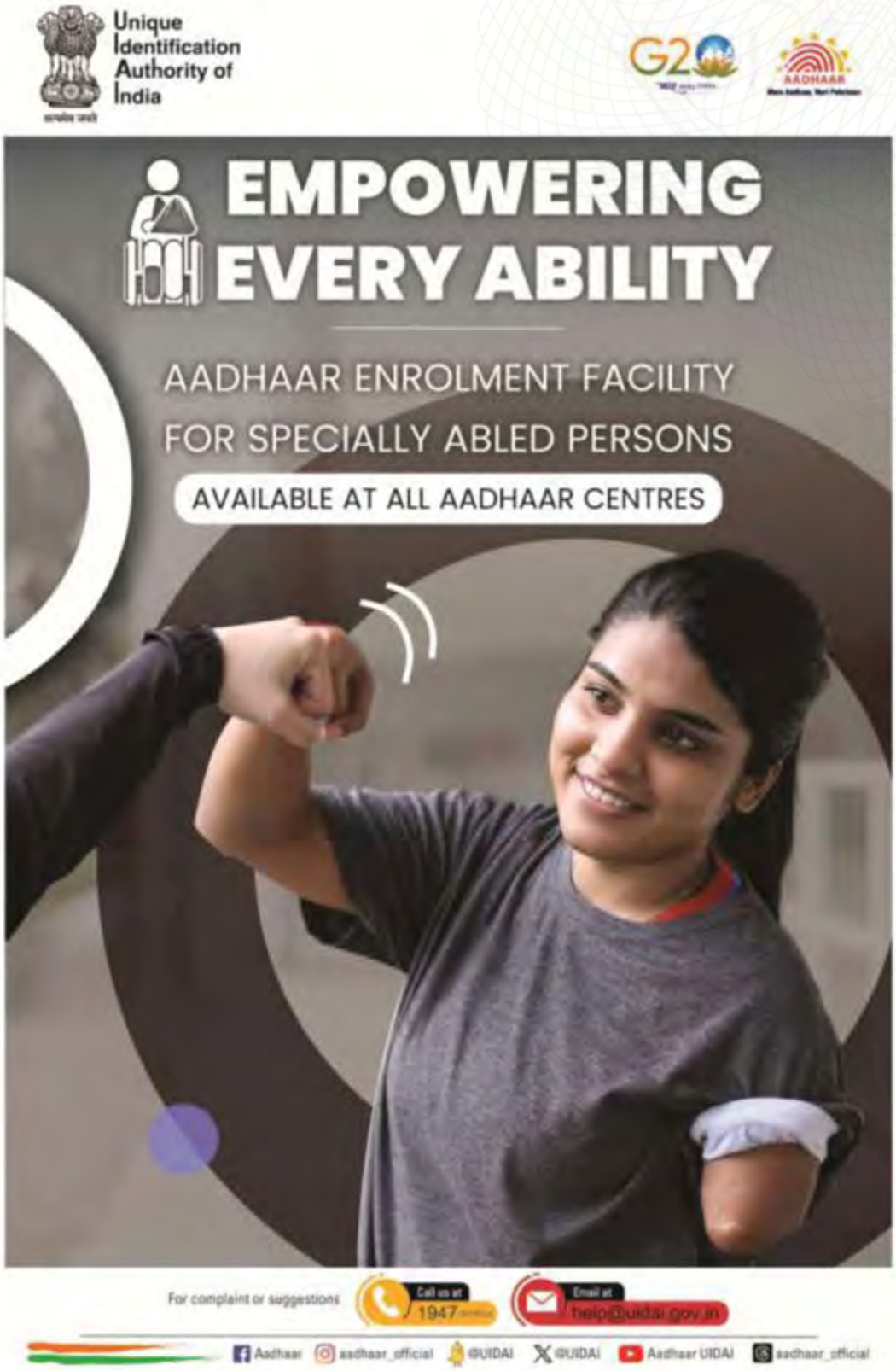
Encl.: as above

(Prabhakaran C. R.)
Deputy Director
Tel.: 011-23478444
Email: dd.eu1-hq@uidai.net.in

To:
All Registrars and Enrolment Agencies

Copy to:
1. All Deputy Directors General in charge of Regional Offices of UIDAI
2. Technology Centre, UIDAI, Bengaluru

A - ENROLMENT & UPDATION



INDEX

A - ENROLMENT & UPDATION

INDEX

HQ-16031/1/2021-EU-I-HQ 1/35258/2024

F. No. HQ-16031/1/2021-EU-I-HQ
Unique Identification Authority of India (UIDAI)
(Enrolment and Update I-Division)
*****

7th floor, UIDAI Head Office
Behind Kali Mandir, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated 1st July 2024

Office Memorandum no. 2 of 2024

Subject: Revised specifications of Mobile & Tablet based Child Enrolment Lite Client (CELC) - reg.

In order to cope with the technological advancements at hardware and software level and in accordance with UIDAI's security policies, competent authority has approved the revised specifications of Child Enrolment Lite Client (CELC).

2. System Integrators (SIs) and vendors are required to get the Mobile & Tablet based CELC kit along with single Fingerprint/Iris scanner devices, tested at UIDAI Regional Offices/Tech Centre for interoperability with the latest UIDAI's CELC application.

3. Regional Offices shall inform the Registrars to procure Mobile/Tablet/ Biometric device as per the latest specifications. Registrars can procure devices with higher/upgraded specification based on the local requirement and availability through GeM portal.

4. The revised specifications (enclosed), supersedes the existing CELC specifications issued vide Circular No. 4(4)/57/50/2011-Vol II dated 04.02.2021 and HQ-16031/1/2021-EU-I-HQ dated 17.12.2021.

5. This is issue with the approval of competent authority.

Encl.: as above

(Prabhakaran C R)
Dy. Director (E&U-I)

To:
1. All UIDAI Regional Offices and Tech Centre
2. All Registrars /EA.
3. All System Integrators/OEMs
4. Guard file

INDEX

SPECIFICATION FOR MOBILE & TABLET based on CHILD ENROLMENT LITE CLIENT (CELC)

S. No.	Name/Description	Mobile Specifications	Mobile Properties	Tablet Specifications	Tablet Properties
1	Screen	Minimum 5.5" touch screen	Mandatory	Minimum 7" touch screen	Mandatory
2	Screen Resolution	1280x720 or higher	Mandatory	1280x720or higher	Mandatory
3	Colors Supported	16 Million	Mandatory	16 Million	Mandatory
4	Scratch resistant front screen	Yes. Corning Gorilla Glass 5 preferred	Mandatory	Gorilla Glass	Mandatory
5	Processor speed minimum	2 GHz or higher, 64 bit architecture	Mandatory	2 GHz or higher, 64 bit architecture	Mandatory
6	RAM	4GB or Higher	Mandatory	4GB or Higher	Mandatory
7	Internal Storage	32GB or Higher	Mandatory	32GB or Higher	Mandatory
8	Expandable Storage through micro SD	64 GB or higher	Mandatory	64 GB or higher	Optional
9	GSM SIM card slot	Yes	Mandatory	Yes	Mandatory
10	Rear Camera with auto focus	8 M Pixel or higher	Mandatory	8 M Pixel or higher	Mandatory
11	Front Camera	5 M Pixel or higher	Mandatory	5 M Pixel or higher	Mandatory
12	Camera with LED flash	Yes	Mandatory	Yes	Mandatory
13	Micro USB Port/Type C Port	1	Mandatory	1	Mandatory
14	Support for USB OTG	Yes	Mandatory	Yes	Mandatory
15	Micro USB/Type C host cable	Yes	Mandatory	Yes	Mandatory
16	Connectivity	Wi-Fi IEEE 802.11 b/g/n/ac	Mandatory	Wi-Fi IEEE 802.11 b/g/n/ac	Mandatory

INDEX

17	GPS & AGPS or NavIC facility for capturing the location coordinates	Yes	Mandatory	Yes	Mandatory
18	Additional Charging port	Yes	Optional	Yes	Optional
19	Mobile Data Support	Minimum compliance to 4G LTE or above standards	Mandatory	Minimum compliance to 4G LTE or above standards	Mandatory
20	Battery Capacity	Minimum 5000 mAH	Mandatory	Minimum 5000 mAH	Mandatory
21	Battery Backup Time	Minimum 8 hours	Mandatory	Minimum 8 hours	Mandatory
22	Software Requirements for development support	Android 11.0 or above	Mandatory	Android 11.0 or above	Mandatory
23	SAR Value	Within acceptable limits permitted in India	Mandatory	Within acceptable limits permitted in India	Mandatory
24	Certifications Available	BIS, or any other relevant Indian Certificates	Mandatory	BIS, or any other relevant Indian Certificates	Mandatory
25	Certifications Available	UL	Optional	UL	Optional
26	BIS Registration under CRS of Meity	Yes	Mandatory	Yes	Mandatory
Note: Mobile/Tablets should not be made in China.					

INDEX

Single Finger Print Scanner Registered Device (RD)

II. Group	Name/Description	Specifications	Properties
1	Single Finger Print Scanner Registered Device (L1 Compliant)	Yes	Mandatory
2	Single Finger Print Scanner Registered Device for Aadhaar Authentication with STQC UIDAI certified RD Service	Yes	Mandatory
3	STQC Certified (STQC Certificate for the Registered device must be submitted)	Yes	Mandatory
4	STQC Certificate Number & its validity(L1 compliant)	Yes	Mandatory
5	Connector Cable to connect the Device to Micro USB/Type C Port	Yes	Mandatory
6	Finger Print Device Connectivity	Through Integrated USB 2.0 or higher	Mandatory
7	Finger Print Device Power	Through USB	Mandatory
8	Sample application for Android platform to test sensor/extractor	Yes	Mandatory
Note: (Refer approved **Single Finger Print Scanner Registered Device** on URL https://uidai.gov.in/images/resource/L1_RD_Devices.pdf			

Single Iris Scanner RD device

Note: (Refer approved **Single Iris Scanner RD devices** on URL

https://uidai.gov.in/images/resource/List_of_UIDAI_certified_Iris_device_vendors_01_04_2023.pdf)

INDEX

HQ-16031/1/2021-EU-I-HQ 1/35259/2024

F. No. HQ-16031/1/2021-EU-I-HQ
Unique Identification Authority of India (UIDAI)
(Enrolment and Update I-Division)
7th floor, UIDAI Head Office
Behind Kali Mandir, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated 1st July, 2024

Office Memorandum no. 1 of 2024

Subject: Revised specifications of Aadhaar Enrolment Kit (AEK) - reg.

In order to cope with the technological advancements at hardware and software level and in accordance with UIDAI's security policies, competent authority has approved the revised specifications of Aadhaar Enrolment Kit (AEK) functioning under Enrolment Client Multiple Platform (ECMP), Update Client Lite (UCL) and Universal Client (UC).

2. All the components/devices as mentioned in the revised specification (enclosed) shall constitute the AEK for ECMP and UC. However, Slap scanner and Dual Iris scanner do not form a part of the AEK for UCL.

3. As part of revised specifications, the System Integrator (SIs)/OEMs of Biometric Devices (Slap/Iris Scanner/Single Iris Scanner/Camera) shall provide following to the Technology Centre, Bengaluru:
   a. Standard drivers for the devices compatible with Windows 11 professional or higher;
   b. SDK supporting Java and .Net for Windows drivers at (a);
   c. VDMs with source code based on the publicly available drivers and SDK versions.

4. System Integrators (SIs) and vendors are required to get the Kit tested at UIDAI Regional Offices/Tech Centre for interoperability with the latest UIDAI's enrolment application as per the existing process.

5. Regional Offices shall inform the Registrars to procure devices as per the latest specifications. Registrars can procure devices with higher/upgraded specification based on the local requirement and availability through GeM portal.

6. The enclosed specifications supersede the existing AEK specifications issued vide Circular No. 4(4)/57/122/2012/UIDAI/Pt dated 31.12.2018.

7. This is issued with the approval of competent authority.

Encl.: as above

(Prabhakaran C R)
Dy. Director (E&U-I)

To
1. All UIDAI Regional Offices and Tech Centre
2. All Registrars
3. All System Integrators/OEMs
4. Guard file

INDEX

Aadhaar Enrolment Kit

Aadhaar enrolment kit consists of a set of hardware devices required to carry out successful Aadhaar enrolments & update. This set of devices comprises of following devices.

I. Laptop/Desktop
II. Monitor
III. Multifunction Device
IV. White screen
V. Focus Light
VI. Surge Protector spike
VII. Iris Scanner
VIII. Camera
IX. Slap scanner
X. Global Navigation Satellite System (GNSS) Device
XI. Single Finger Print RD L1 device
XII. Single Iris Scanner RD device

1. All these devices shall be as per UIDAI's specifications.
2. Biometric devices (Slap/Iris Scanner/Single Iris Scanner/Camera) L0 RD device and Single Finger Print RD L1 device shall be STQC certified.
3. Complete kit warranty shall be for 3 years except White screen, Focus light & surge protector.
4. **During warranty, faulty equipment's shall be replaced/repaired within 7 days.**
5. Aadhaar Enrolment Kit comprising of specific make/model of device shall be UIDAI certified for its working with latest UIDAI's enrolment client (ECMP)
6. AEK vendors to provide Manufacturers Authorization Form (MAF) issued by OEM for warranty support.
7. It is the responsibility of the AEK vendor/OEM to provide Standard drivers, java and .net supporting SDK, **digitally signed VDM** with source code based on the publicly available drivers & SDK versions and on demand support for the devices which are part of the AEK.
8. OEMs to support UIDAI for Forensic analysis in case of any requirement or need arises

INDEX

Aadhaar Enrolment Kit

Minimum Specification of Aadhaar Enrolment Equipment

Item S.1.1. – Laptop

Specification	Details
Machine Form Factor	Laptop
CPU	4 Core processor or higher with minimum Frequency 4.0 GHz or higher and 10 MB Cache or higher
Display	Minimum 14" HD Anti-Glare (16:9)
Display type	LED
Connectivity	Wi-Fi (IEEE 802.11b/g/n/ac) and Ethernet (10/1000 Base-T)
MEMORY	Min. 16-GB DDR4RAM or higher expandable up to 32-GB or higher with 1 DIMM SLOT FREE
Solid-State Drive (SSD)	Minimum 512GB SSD
Input/output Ports	One HDMI – minimum
	Two(VGA/ DP Port/Type C/HDMI) port with Display Transfer feature
	Dedicated Minimum 3 USB 2.0 port*
	One Ethernet (RJ-45)
Battery Backup	6hrs backup time in case of laptop
Chipset	System-on-a-Chip
Graphics	Integrated Graphics
Keyboard	Integrated for laptop sized (Minimum 84 Keys) Windows compatible Spill-resistant keyword
Touchpad	Wide Touchpad below keyboard for laptop
Preloaded OS	Windows 11 professional or higher (Standard and Home edition of windows are not allowed)
Certification	BIS,or any other relevant Indian Certificates
ACCESSORIES	*USB Hub with multiple USB connections (enabling 5 devices plug-in through USB port)*, Laptop carrying case
WARRANTY	3 years comprehensive onsite-warranty including Battery and power adapter
ANTI-VIRUS	Reputed Antivirus/EDR software with regular signature updates
TPM	System should support Trusted Platform Module (TPM) version 2.0 or higher version

Aadhaar Enrolment Kit

Item S.1.1.1 – Desktop

Specification	Details
Machine Form Factor	Desktop(Small form Factor)
CPU	4 Core processor or higher with minimum Frequency 4.0 Ghz or higher and 10 MB Cache or higher
MEMORY	Min. 16-GB DDR4RAM or higher expandable up to 32-GB or higher with 1 DIMM SLOT FREE
Connectivity	Ethernet (10/1000 Base-T)
Solid-State Drive (SSD)	Minimum 512GB SSD
Input/output Ports	Min 1 HDMI
	One (VGA/ DP Port/Type C) port with Display Transfer feature supported by Monitor
	Dedicated Minimum 5 USB 2.0 port
	One Ethernet (RJ-45)
Battery Backup	0.5KVA UPS with 30 min backup time For desktop
Chipset	Integrated with CPU or equivalent
Graphics	Integrated Graphics
Keyboard	(Minimum 104 Keys) Windows compatible Spill-resistant keyword
Touchpad	Optical USB mouse
Preloaded OS	Windows 11 professional or higher (Standard and Home edition of windows are not allowed)
Certification	BIS, or any other relevant Indian Certificates
WARRANTY	3 years comprehensive onsite-warranty
ANTI-VIRUS	Reputed Antivirus/EDR software with regular signature updates(Licensed version required)
TPM	System should support Trusted Platform Module (TPM) version 2.0or higher version

Aadhaar Enrolment Kit

Item S.1.2. - Monitor

Specification	Details
Size	15-16 inch or higher
Type	LED
Resolution	1024 x 768 or above
Note: One additional Monitor with Desktop & Laptop - One for Operator view and other for applicant of enrolment and update view	

Item S.1.3. – Multi Functional Device (MFD)

Specification	Details
Function	PRINTCOPY SCAN (COLOR)
DUTY CYCLE IN PAGES	3000 PAGES per month
Print Speed PPM – BLACK(A4)	18 PPM or better
Resolution	600 X 600 DPI
Printing Technology	Ink Tank /laser
Custom media size	A4
Standard operating system supported	Compatible with Windows 11 professional or higher
Scan resolution	600 X 600 DPI OPTICAL
Bit/color depth	24 BITS
Copy speed	18 CPM or better
Copy resolution	600 X 600 DPI
Scan file format	Minimum PDF,JPEG,
BIS Registration under CRS of MeitY	Yes
Onsite OEM Warranty	Minimum 3 years

Aadhaar Enrolment Kit

Item S.1.4. – White Screen

Specification	Details
Size	4 X 5 ft Stand mountable / wall mountable
Accessories	Stand
Non-Reflecting	Yes
Opaque	Yes

Item S.1.5. – Focus Light

Specification	Details
Type	LED, minimum 5 W
Accessories	Stand, 2Mrts Wire and on/off Switch near the operator

Item S.1.6. – Surge Protector Spike

Specification	Details
General	6 nos. of 5A sockets (4 Indian style + 2 International Style), Fuse, on/off Switch and ISO mark

Aadhaar Enrolment Kit

Item S.2.1 – Iris Device Specification

Specification	**Stationary (mounted: wall, tripod or stand)[1]**	**Hand_held[2]**	**Hand-held with alignment aid[3]**
Standard compliance for image capture	ISO/IEC 19497-6 (2005 or preferable2011 version)		
Iris Diameter (In pixel)	> 190		
Spatial Resolution Pixel Resolution	> 60% @ 4.0 Lp/mm > =18 Pixels/mm		
# of simultaneous captured	2		
eyes[4]			
Viewfinder	External	Internal	External or Internal
Capture distance	> 750 mm	> 50mm	> 20 mm
Capture volume (width/height/depth)	>250x500x500mm	> 20x15x12mm	> 20x15x12mm
Exposure time	< 15ms	< 33ms	< 33ms
Imaging wavelength	700-900 nm		
Spectral Spread	Power in any 100nm band > 35% of total power		
Scan type	Progressive		
Image margins	Left & right: 0.50x iris diameter, Top & bottom: 0.25x iris diameter		
Pixel depth	> 8 bits/pixel		
Image evaluation frame rate	>= 7 frames/sec, continuous image capture		
Capture mode	Auto capture with built-in quality check (incorporates NIST quality considerations)		
Sensor signal to noise ration	> 40 DB		
Connectivity[5]	USB 2 or higher, USB-IF certified or Networked (TCP/IP)	USB 2 or higher, USB-IF certified	

INDEX

Aadhaar Enrolment Kit

Power	USB or independent PS		
Weight	NA	< 1 kg	< 1 kg
Dimension	<300 x 100 x 300mm	< 220 x 200 x 100 mm	< 220 x 200 x 100 mm
Operating temperature	0-49C		
Humidity	10 - 90% non-condensing		
Durability/Shock	IP54		
Safety Standard	Exempt Group per IEC 62471:2006-07		
Standards	FCC Class A, RoHS		
Liveness	Liveness detection compliance as per IEEE Std 2790™-2020 & ISO/IEC 30107-3		
Software AP	Compliant with latest UIDAI Device Capture API Specifications. Windows 11 Professional VDM ready certified by UIDAI		
[1]Stationary: Any capture process where the device is stationary and the subject is required to position and rest himself/herself [2]Handheld: Operator operates and holds the camera and the subject is stationary. [3]Alignment aid: Camera has mechanical fixture for alignment. Optical viewfinder is not considered alignment aid. [4]Considered simultaneous if second eye is captured within 2 seconds of first eye done without moving the device. [5]Total of only 1 USB port will be available for connectivity and power			
Security – Digital Signature(Preferably at firmware level)			

Item S.2.2 – Camera

Specification	Details
Standard compliance for image capture	ISO/ IEC 19794-5
Capture Mode	Plain live capture
Image Quality	Full Frontal (0x01) as per ISO/IEC 19794-5
Minimum Resolution	1920x1080
Capture Mode	Manual Capture with Auto Focus and Auto Lighting Adjustment

Aadhaar Enrolment Kit

Sensor	>2 Mega Pixel Native
Connectivity6	High Speed USB 2.0 or higher, USB-IF certified
Lens	Fixed, SLR
Power	Through USB/Independent PS/Lithium Ion
Mount	Tripod/Universal Clip
Operating Temperature	0 to 50 degree Celsius
Humidity	10 – 90%
Safety Standard	UL, IS 616:2017
Software API	Compliant with latest UIDAI Device Capture API Specifications
Durability / Shock	IP 54
[6]Total of only 1 USB port will be available for connectivity and power	
Security – Digital Signature(Preferably at firmware level)	

Item S.2.3 – Finger Print Device Specification (Slap Scanner)

Specification	Details
Standard compliance for image capture	ISO/IEC 19794-4
Capture Mode	Plain live scan capture
Image Acquisition Requirements	Setting level 31 or higher (Section 9.1 of Biometric Design Standards for UID Applications V1.0
Image evaluation frame rate	> 3 frames/sec, continuous image capture

Aadhaar Enrolment Kit

<table>
<tr><td>Capture mode</td><td>Auto capture with built-in quality check (incorporates NIST quality considerations)</td></tr>
<tr><td>Capture area</td><td>>76mm x 80mm</td></tr>
<tr><td>Capture sizes</td><td>
<table>
<tr><th rowspan="2">Finger prints</th><th colspan="2">Preferred width</th><th colspan="2">Preferred height</th></tr>
<tr><th>(in)</th><th>(mm)</th><th>(in)</th><th>(mm)</th></tr>
<tr><td>Roll finger</td><td>1.6</td><td>40.6</td><td>1.5</td><td>38.1</td></tr>
<tr><td>Plain Thumb</td><td>1</td><td>25.4</td><td>2</td><td>50.8</td></tr>
<tr><td>Plain 4 fingers (Sequence check)</td><td>3.2</td><td>81.3</td><td>3</td><td>76.2</td></tr>
<tr><td>Plain 4 fingers (identification flat)</td><td>3.2</td><td>81.3</td><td>3</td><td>76.2</td></tr>
</table>
</td></tr>
<tr><td>Pixel depth</td><td>1 to 16 bits (size 1 byte)</td></tr>
<tr><td>Image resolution (horiz) and (vert)</td><td><=scan resolution (horiz) --2 bytes size and <=scan resolution (vert) --2 bytes size</td></tr>
<tr><td>Resolution of final output image</td><td>500 ppi, plus or minus 5 ppi</td></tr>
<tr><td>Signal - to - noise ratio</td><td>Both the ratio of signal to white noise standard deviation and the ratio of signal to black noise standard deviation of the digital scanner >= 125</td></tr>
<tr><td>Connectivity[7]</td><td>USB 2.0 or higher, USB-IF certified</td></tr>
<tr><td>Power</td><td>Through USB</td></tr>
<tr><td>Dimension (W X H X D)</td><td><180MM x 180mm x 180mm</td></tr>
<tr><td>Weight</td><td>Maximum 2.5Kg.</td></tr>
<tr><td>Operating temperature</td><td>0 – 50 C</td></tr>
<tr><td>Humidity</td><td>10 – 90% non-condensing</td></tr>
<tr><td>Durability / Shock</td><td>IP 54</td></tr>
</table>

Aadhaar Enrolment Kit

Standards	UL certified (if applicable). Meets ISO 19794-4:2005 Section7 and Annex A certification requirements (IAFIS Appendix F certified).
Software API	Compliant with latest UIDAI Device Capture API Specifications Linux/Windows 64 bit VDM ready certified by UIDAI
Platen Area Hardness	Hardness Test: 6H compliant Tested as per ASTM D3363; RCA Test: 175g, 400 cycles Abrasion test compliant as per ASTM F 2357-04
Liveness	Liveness detection compliance as per IEEE Std 2790™-2020 & ISO/IEC 30107-3
Note: [7]Total of only 1 USB port will be available for connectivity and power	
Security – Digital Signature(Preferably at firmware level)	

Item S.2.4 – GNSS Device

Specification	Details
Environmental Specifications	
Operating temperature	-10 ~ 85°C
Storage temperature	-40 ~ 85°C
Humidity	5% toUp to 95% non-condensing
Water proof	IP54 or higher
GNSS+NavIC Specification	
GNSS Chipset	SIRF Star III/SIRF Star IV GSD4e /Mediatek/u-blox/sky traq *Must support NavIC with other constellation
Frequency	L1&L5 Dual band
Position Accuracy	<5m 3drms
Time Accuracy	15 ns
Channels	>=34 channel + GAGAN SBAS(Preferable)
Acquisition Sensitivity (in –dBm)	-142dBm or better
Tracking Sensitivity (in –dBm)	-156dBM or better
Protocol/Standard support	NMEA 0183 V3.0or latest protocol@ 115200/9600 baud rate, and supports messages: GGA, GSA, GSV, RMC, VTG, GLL,ZDA v2.2
Position fix time	
Hot Start	1-2 sec

Aadhaar Enrolment Kit

Warm Start	< 30 sec
Cold Start	< 60 sec
Position Update Rate	>= 1Hz
Electrical characteristics	
Voltage	3.5V ~ 6.5V
Current draw	55-80mA
Other Parameters	
Type of connection and Range	Location and Time/NMEA data transmission to be Wireless with min. 50 m range For Wired min.20 m range
Ensuring Coordinate Accuracy	The coordinate must be captured with over 99% accuracy
Accessories	With all necessary required cables and accessories to connect to the PC/Laptop
Warranty	3 years Comprehensive on-site Warranty
Note: **1.* GNSS receiver should be capable of computing location from NavIC constellation** **2. Total of only 1 USB port shall be available for connectivity and power**	

Item S.2.5 – Single Finger Print Scanner L1 Registered Device (RD)

S. No.	Name/Description	Specifications	Properties
1	Single Finger Print Scanner Registered Device (L1 Compliant)	Yes	Mandatory
2	Single Finger Print Scanner Registered Device for Aadhaar Authentication with STQC UIDAI certified RD Service to the L1 compliant Fingerprint Registered Device	Yes	Mandatory

Aadhaar Enrolment Kit

3	STQC Certified (STQC Certificate for the Registered L1 device must be submitted)	Yes	Mandatory
4	STQC Certificate Number & its validity(L1 compliant)	Yes	Mandatory
5	Connector Cable to connect the Device to Micro USB/Type C Port	Yes	Mandatory
6	Finger Print Device Connectivity	Through Integrated USB 2.0 or higher	Mandatory
7	Finger Print Device Power	Through USB	Mandatory
8	Sample application for Android platform to test sensor/extractor	Yes	Mandatory

Note: (Refer approved **Single Finger Print Scanner Registered Device** devices on UIDAI website)

Item S.2.6 – Single Iris Scanner Registered Device (RD)

Note: (Refer approved **Single Iris Scanner Registered Device** devices on UIDAI website)

SPECIAL TERMS AND & CONDITIONS FOR AADHAAR ENROLMENT KIT

1. Installation & commissioning: Bidder shall provide Remote support Facility for installation of Aadhaar Enrolment Kit
2. Delivery Period: - Bidder shall complete the entire delivery to consignee within 30 days from date of purchase order.
3. Performance bank guarantee – Bidder shall submit the PBG of 10% of the contract value to the purchaser before payment is released
4. Payments: 100 percent of the payment shall be made within 10 days of supply of Aadhaar enrolment kit to consignee after its acceptance & submission of PBG.
5. SLA: Incase failing to replace/repair of faulty equipment's within 7 days (equipment's within warranty), Rs100 penalty per day per equipment till the replacement/repair shall be deducted from PBG.

F. No. HQ-16031/1/2021-EU-I-HQ
Unique Identification Authority of India (UIDAI)
(Enrolment and Update I-Division)
*****

7th floor, UIDAI Head Office
Behind Kali Mandir, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated 13th August 2024

Frequently Asked Questions (FAQs) on revised Aadhaar Enrolment Kit specifications

Frequently asked Questions (FAQ) to clarify doubts/queries received regarding revised Aadhaar Enrolment Kit specifications issued vide UIDAI OM no. 1 of 2024 of even file number dated 01.07.2024.

S.No. 1. CPU Specifications (Item S.1.1. – Laptop and Item S.1.1.1 – Desktop)

Question: Does the required CPU speed of 4.0 GHz refer to the base frequency or the maximum turbo frequency?

Answer: The specified 4.0 GHz refers to the minimum turbo frequency of a 4-core processor with a cache size of at least 10 MB. This configuration is necessary for optimal performance in handling demanding tasks.

S.No. 2. Display Port Requirements (Item S.1.1. – Laptop, Input/output Ports)

Question: New laptops often have one HDMI port/one display transfer port and two USB ports. How can the requirement of multiple ports be met?

Answer: If multiple ports are not available as required, the requirement can be fulfilled by providing additional connector or/and USB Hub as a part of the AEK Kit.

S.No. 3. Desktop Certification (Item S.1.1.1 – Desktop)

Question: Does the required BIS or other Indian certification apply to the entire desktop unit or just the display unit?

Answer: The BIS certification mentioned is applicable for display unit of the desktop.

S.No. 4. TPM Requirement (Item S.1.1. – Laptop and Item S.1.1.1 – Desktop)

Question: Is hardware or software TPM 2.0 required for enhanced security?

Answer: TPM 2.0 or higher is mandatory at hardware level.

S.No. 5. Chipset Compatibility (Item S.1.1.1 – Desktop)

Question: Chipset Integrated with CPU or equivalent, does "equivalent" is acceptable as compatible also?
Answer: Yes, "equivalent" can be interpreted as compatible in this context.

INDEX

S.No. 6. Hardness Testing (Item S.2.3 – Finger Print Device Specification, Slap Scanner)

Question: Which type of report is required for compliance with the 6H hardness test (ASTM D3363), RCA Test (175g, 400 cycles), and Abrasion test (ASTM F 2357-04) for the slap scanner platen area?

Answer: In this regard, Test report from any accredited Lab or in-house test reports from the OEMs shall be acceptable.

S.No. 7. Liveness Detection (Item S.2.3 – Finger Print Device Specification, Slap Scanner)

Question: Is compliance with IEEE Std 2790™-2020 sufficient, or is a certificate for ISO/IEC 30107-3 also required for slap scanner liveness detection?

Answer: A certificate from a NIST/NABL accredited lab for ISO/IEC 30107-3 compliance and a certificate from any accredited Lab or an undertaking from OEM for compliance with IEEE Std 2790™-2020 shall be acceptable.

S.No. 8. Registered Device Level (AEK specification point no. 2)

Question: Does "L0 RD device" mean the biometric devices (slap/iris scanner/single iris scanner/camera) must comply with L0, Registered Device standards and what is the compliance needed for the same?

Answer: Yes, all biometric devices such as slap/iris scanner/single iris scanner/camera must adhere to the L0, Registered Device requirements for enrolment and update processes and an OEM undertaking confirming compliance with L0, Registered Device standards and adherence to Device-Capture API specifications as and when released by UIDAI.

Signed by Prabhakaran C R
Date: 13-08-2024 14:19:30
(Prabhakaran C R)
Dy. Director (E&U-I)

To:

1. All UIDAI Regional Offices and Tech Centre
2. All Registrars /EA.
3. All System Integrators/OEMs
4. Guard file

INDEX

F. no. HQ-16024/2/2020-EU-I-HQ
Unique Identification Authority of India
(Enrolment and Update Division)

UIDAI Head Office
Bangla Sahib Road, Behind Kali Mandir
Gole Market, New Delhi – 110 001
Dated 12.03.2025

Circular no. 1 of 2025

Subject: Policy regarding action in case of default in adherence to or violation of any regulation, process, standard, guideline or order issued by the Unique Identification Authority of India, by registrars, enrolment agencies or other service providers

The policy regarding action in case of default in adherence to or violation of any regulation, process, standard, guideline or order issued by the Unique Identification Authority of India, by Registrars, enrolment agencies or other service providers, version 5.0 (hereinafter referred to as the "instant policy"), annexed hereto, is issued hereby, pursuant to the provisions contained in sub-regulation (3) of regulation 26 of the Aadhaar (Enrolment and Update) Regulations, 2016, made in exercise of the powers conferred by, *inter alia*, sub-section (1) and sub-clause (s) of sub-section (2) of section 54 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, read with, *inter alia*, clause [F] ("Financial Disincentives") of the terms of engagement of registrar, issued *vide* UIDAI's OM F. no. HQ-16024/4/2020-EU-I-HQ Part (1), dated 29.9.2022 and revised *vide* its OM of even number, dated 23.3.2023 and signed and furnished to UIDAI by registrars.

2. The instant policy supersedes the policy issued *vide* the Authority's circular policy issued vide UIDAI's circular F. no. HQ-16024/2/2020-EU-I-HQ, dated 30.11.2022 and modified *vide* its circular bearing the said number, dated 03.10.2023 and shall come into effect from 01.04.2025.

3. This issues with the approval of competent authority.

Signed by Prabhakaran C R
Date: 17-03-2025 13:27:09

(Prabhakaran C. R.)
Deputy Director
Tel.: 011-23478444
Email: dd.eu1-hq@uidai.net.in

To:
1. All UIDAI Regional Offices
2. Deputy Director General, UIDAI Tech Centre
3. Deputy Director General (Finance), UIDAI HO
4. All Enrolment Registrars
5. Guard file

INDEX

HQ-16024/2/2020-EU-I-HQ I/42381/2025

[Issued *vide* Circular no.1 of 2025, dated 12.03.2025]

Policy regarding action in case of default in adherence to or violation of any regulation, process, standard, guidelines or order issued by the Unique Identification Authority of India, by Registrars, enrolment agencies or other service providers (version 5.0)

1. Appointment of Registrars, enrolment agencies and other service providers is governed by Chapter V (Regulations 21 to 26) of the Aadhaar (Enrolment and Update) Regulations 2016. Regulation 26 thereof reads as under:

> "**26. Liability of Registrars, enrolling agencies and other service providers and action in case of default—** (1) The Registrars, enrolling agencies, and other service providers, and the supervisors, operators or any other persons or agencies employed by them shall adhere to all regulations, processes, standards, guidelines, and orders issued by the Authority from time to time, and the code of conduct provided in Schedule V.
>
> (2) The Authority shall monitor the enrolment activities of the Registrars, enrolling agencies and the operators, supervisors and other personnel associated with enrolment.
>
> (3) Without prejudice to any other action which may be taken under the Act, for violation of any regulation, process, standard, guideline or order, by a Registrar or Enrolment Agency or any service provider or any other person, the Authority may immediately suspend the activities of such a Registrar or Enrolment Agency or service provider or concerned person, and after holding due enquiry, it may take steps for imposition of financial disincentives on such a Registrar or Enrolment Agency or service provider or any other person and for cancellation of the credentials, codes and permissions issued to them pursuant to the Act or these regulations, or any other steps as may be specifically provided for in the terms of engagement with the Authority."

2. Further, clause [F] ("Financial Disincentives") of the terms of engagement of Registrar, issued *vide* UIDAI's OM F. no. HQ-16024/4/2020-EU-I-HQ Part (1), dated 29.9.2022, reads as under:

> "**[F] Financial Disincentives**
>
> a. UIDAI without prejudice to any other action which it may take under the Act, for violation of the Act, any regulation, direction issued by the Authority, process, standard, guideline or order, by the Registrar or its Enrolling Agency (through Registrar), may immediately suspend the activities of the Registral or its Enrolling Agency after holding due enquiry, it may take steps for imposition of financial disincentives on the Registrar as per the UIDAI policy or guidelines and for cancellation of the credentials, codes and permissions issued to them pursuant to the Aadhaar Act, 2016 and regulations framed thereunder.
>
> …
>
> g. The financial disincentive shall be levied upon the Registrars against defaults as per the Policy for enforcing of Aadhaar (Enrolment and Update) Regulations 2016, process, standards, guidelines, Data Quality and containing corrupt / fraudulent practices issued by UIDAI, as modified from time to time."

3. This policy is issued pursuant to the provisions contained in sub-regulation (3) of regulation 26 of the Aadhaar (Enrolment and Update) Regulations, 2016, read with the terms

of engagement of Registrar (hereinafter referred to as "instant policy"). The instant policy provides for the policy, process and guidelines for suspension of activities and the steps that may be taken for the imposition of financial disincentives and cancellation of credentials etc., for non-adherence to or violation of any regulation, process, standard, guideline or order issued by UIDAI, by a Registrar, enrolment agency or service provider, and any agency or other person employed by the aforesaid.

4. The provisions of the instant policy are without prejudice to any other action that may be taken as provided for under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereinafter referred to as "the Act") or any other applicable law.

5. **Procedure for establishing non-adherence to or violation of any regulation, process, standard, guideline or order**

5.1 Operator at an Aadhaar enrolment centre is required to follow the procedure as per regulation 11 of the Aadhaar (Enrolment and Update) Regulations, 2016 while providing Aadhaar enrolment or update services to an individual seeking enrolment or update of information in Aadhaar. Further, all equipment used in enrolment, such as computers, printers, biometric devices and other accessories need to be as per the specifications issued by the Authority for this purpose. The Authority while processing the information/data collected at the enrolment centre and uploaded to Central Identities Data Repository (CIDR), pursuant to regulation 13 and 14 of the Aadhaar (Enrolment and Update) Regulations, 2016 read with code of conduct as set out in Schedule V, may reject an enrolment or update request due to quality or any other technical reason, in the course of checking by UIDAI for quality of information/data collected (hereinafter referred as 'QC process'). In case the request is rejected the QC process, it is marked with applicable error category.

5.1.1 The list of error categories, along with the nature of violation of any regulation, process, standard, guideline or order is at Annex I. Based on the type and count of errors marked during QC process, UIDAI generates a Registrar-wise data quality and deficiency report (DQDR) on a monthly basis or otherwise. The DQDR forms the basis for action as specified in Annex II to be taken for violation of any regulation, process, standard, guideline or order.

5.2 Sub-section (l) of section 23 of the Act empowers the Authority to call for information and records, conduct inspections, inquire and audit the operations of the CIDR, Registrars, enrolling agencies and other agencies. Non-adherence to or violation of any regulation, process, standard, guideline or order may also be established through such calling for information and records, inspections, inquiry and audit as follows:

(a) UIDAI has put in place a system of Out Bound Dialling (OBD) survey to collect feedback from the individuals on the Aadhaar enrolment and update services availed by them. Grievances pertaining to overcharging and corrupt practices by a Registrar, enrolment agency, service provider or other person are also investigated by UIDAI through the system of OBD survey.

INDEX

(b) UIDAI also performs various checks at the backend to detect violations relating to bypassing of or tampering with the enrolment software.

(c) Physical audit and inspections of the enrolment centres are conducted through Regional Offices and other means to monitor the activities of the Registrars, enrolling agencies, operators, supervisors and other personnel associated with enrolment and update.

5.2.1 In case any violation of any regulation, process, standard, guideline or order as set out in Schedule V or any other provisions of the Aadhaar (Enrolment and Update) Regulations, 2016 is identified through calling for information and records, inspections, inquiries and audit, action as specified in Annex III shall be initiated against the Registrar, and operator concerned, which can be in addition to the action already taken for violations as mentioned in paragraph 5.1.1.

6. Procedure for imposition of financial disincentives on Registrars

6.1 UIDAI generates — (i) consolidated Registrar-wise Aadhaar generation (AG) report, (ii) detailed EID-wise report of successful and unsuccessful transactions, and (iii) DQDR on monthly basis or otherwise and shares the same with the Registrars.

6.2 All the Registrars are mapped to any one of the UIDAI Regional offices (RO) for administrative purpose. On receipt of the above reports along with calculations, every Registrar concerned shall submit to the RO concerned a tax invoice if registered under GST or an invoice if not registered under GST, for processing of payment for the month or otherwise.

6.3 The total amount of financial disincentives on account of violations specified in paragraph 5.1.1 for each calendar month or otherwise shall be capped at 10% of the amount of financial assistance due from UIDAI (excluding GST) for the corresponding period.

6.4 There shall be no capping on the amount of financial disincentives on account of the violations as mentioned in paragraph 5.2.1. In case the total amount of financial disincentives on account of such violations exceeds the amount of financial assistance due from UIDAI during the relevant month, the excess amount is liable to be recovered from the future payments.

7. Procedure for suspension of activities, cancellation of credentials, codes and permissions, and training and testing of operator

7.1 *Procedure in respect of violations specified in Annex II*

7.1.1 In the event of an operator exceeding any threshold specified in Annex II, UIDAI Technology Centre may suspend the activities of the operator concerned and permissions of the operator under intimation to the Registrar, enrolment agency and RO concerned. Further steps shall be taken by the Registrar as applicable and specified in **Annex II**.

INDEX

7.2 *Procedure in respect of violations specified in Annex III*

7.2.1 In the event of an operator committing any violation as specified in Annex III, the RO concerned shall communicate the same to the UIDAI Technology Centre for the suspension of activities or the cancellation of the credentials, codes and permissions, or both, of such operator, and the Technology Centre shall give effect to the same, under intimation to the Registrar, enrolment agency and RO concerned. Further steps shall be taken by the Registrar as applicable and specified in **Annex III**.

8. Re-training and certification

8.1 Violation of any regulations, process, standards, guidelines or order by an operator in the course of carrying out the enrolment or update process is likely to result in rejection of the request or recording of inaccurate information in CIDR, or both, to the detriment of the individual undergoing such process or a requesting entity that may rely on such information, or both. Therefore, it is necessary that operators exercise due care and caution in the performance of their duties. While operators who commit a violation as is specified at serial number 1 in Annex II, or in Annex III, shall not be permitted to continue in the system, in respect of other violations, the operator concerned shall be provided opportunity for re-training and certification as follows:

(a) Errors with error code DOE-1: On the first and second instances of an operator committing Document Error-1 ("DOE-1") as specified in Annex II, an email alert shall be sent to the Registrar, enrolment agency and operator concerned. In case a third instance of such violation by such operator in the same month, the activities of the operator shall be suspended forthwith. Registrar will have the discretion to consider re-onboarding such operator after one month of such deactivation, on completion of re-training and certification through LMS portal of UIDAI. Upon receipt of request from the Registrar concerned, the RO concerned may re-onboard such operator.

(b) Errors with error code -AL, DOE-2, DE, BE, RSV: On the 10th, 20th and 25th instances of an operator committing any of the errors namely, Abusive Language ("AL"), Document Error-2 ("DOE-2"), Demographic Error ("DE"), Biometric Error ("BE"), Rejection during Source Verification ("RSV") as specified in Annex II, an email alert shall be sent to the Registrar, enrolment agency and operator concerned. In case of 30th instance of such violation by such operator in the same month, the activities of the operator shall be suspended forthwith. Registrar will have the discretion to consider re-onboarding such operator after one month of such deactivation, on completion of re-training and certification through LMS portal of UIDAI. Upon receipt of request from the Registrar concerned, the RO concerned may re-onboard such operator.

8.2 In case an operator is re-onboarded after re-training and certification as described at paragraph 8.1(a) and 8.1(b) above, and the activities of such an operator is suspended again for any violation subsequently, he shall not be given the opportunity for undergoing re-training and re-onboarding within a period of 12 months from the date of such suspension.

INDEX

8.3 The condition mentioned at paragraph 8.2 will not be applicable to regular Government employees working as Aadhaar operators under various State and Central Government Registrars.

9. Mechanism for reconsideration of the action taken against violations of regulations, processes, standards, guidelines, orders and the code of conduct

9.1 A Registrar, enrolment agency, service provider or other person aggrieved by any action taken pursuant to the instant policy may, within a period of 45 days from the date of receipt of communication in this regard, represent to the Deputy Director General (DDG) in charge of the RO concerned, for reconsideration of such action. In the case of an enrolment agency, service provider or other person, the submission of such representation shall be done through the Registrar concerned. Such DDG shall consider and decide the representation and shall cause the substance of such decision to be conveyed in writing to the representing Registrar or, through the Registrar concerned, to the representing enrolment agency, service provider or other person concerned, as the case may be. The decision so conveyed shall be final.

10. The instant policy supersedes the policy issued *vide* UIDAI's circular F. No. HQ-16024/2/2020-EU-I-HQ, dated 30.11.2022 and modified *vide* its circular bearing the said number, dated 03.10.2023 (hereinafter referred to as "superseded policy"). However, such supersession shall not affect—

(a) any suspension of activities, credentials or codes or permissions cancelled, or other steps taken under the superseded policy;
(b) any right, obligation or liability acquired, accrued or incurred under the superseded policy; or
(c) any steps initiated under the superseded policy for the cancellation of credentials, codes or permissions, which may continue to be proceeded with under the superseded policy as if the instant policy has not come into effect:

Provided that where the operator whose activities were suspended for a period of one year under the superseded policy for a deficiency other than the deficiency listed at serial number 2 in the table below clause (xviii) of paragraph 4 of the said policy, such operator may, on successful completion of re-training and certification as referred to in paragraph 8 of the instant policy and if a request is made by the Registrar concerned in this regard, be re-onboarded before expiry of the said period of one year.

Annex I

List of error categories along with nature of violation of regulations / processes / standards / guidelines / orders

S. No.	Nature of violation of regulations / processes / standards / guidelines / orders	Error category
1	**Photo on photo (POP)** of the individual seeking enrolment/ update	POP
2	**Document Error-1 (DOE-1)** (a) Uploading of overwritten/tampered system generated documents issued by Central/State Governments (b) Uploading of photo of object/ screenshot/ picture etc. against document	DOE-1
3	**Use of unparliamentarily language / abusive language in demographic details**	AL
4	**Document Error-2 (DOE-2)** (a) Uploading of poor-quality document/scan (b) Uploading of blank document or document not as per list of supporting documents (c) Uploading of wrong document in the selected document type (d) Uploading of expired or outdated documents like DL, passport, electricity bill, post-paid telephone bill, water bill, etc. (if not otherwise specified) (e) Uploading of only one side of a document whose both sides required for validation (*e.g.* one side of voter id card is not valid for proof of address) or not uploading all the relevant pages of a document (f) Uploading of photoshop document or document generated from unauthorised website (g) Uploading of wrong relationship document (*e.g.*, relationship mentioned in the address part of the document as w/o, h/o, c/o, d/o, s/o etc. shall not be acceptable) (h) Uploading of photocopy of document (i) Uploading of invalid document (j) Uploading of document bearing correction fluid/overwriting/ cutting etc. without attestation by issuer	DOE-2
5	**Demographic Error (DE)** (a) Minor typographical errors or demographic data mismatch (b) Transliteration error (c) Wrong selection of gender type/ relationship type (d) Visible age/photo mismatch (e) Any other document or data entry mistakes not covered under DOE-1	DE
6	**Biometric Error (BE)** (a) Photo not captured as per guidelines (b) Biometric exception photo not captured properly (c) Photo not of the individual seeking Enrolment/Update	BE

7

INDEX

	(d) Biometric exception photo not of individual seeking enrolment/ update	
7	**Rejection during source verification at QC (RSV):** Document found invalid during source verification	RSV
8	**Rejection due to technical issues at UIDAI's end (TR)**	TR

Annex II

Action to be taken for violations of regulations, processes, standards, guidelines, orders and the code of conduct provided in the Aadhaar (Enrolment and Update) Regulations, 2016 as identified in the QC processes*

S. No.	Error category	Nature of violation of regulations / processes / standards / guidelines / orders	Action to be taken	Rate of financial disincentive
1	POP	**Photo on photo (POP)** of the individual seeking enrolment/ update	(1) Suspension of the activities of the operator concerned with email notification to operator/EA /Registrar concerned (2) Consider imposing financial disincentives on the Registrar	₹ 25,000 per packet
2	DOE-1	**Document Error 1 (DOE-1)** (a) Uploading of overwritten/tampered system generated documents issued by Central/ State Governments (b) Uploading of photo of object/ screenshot/ picture etc. against document	(1) Email notification to operator/EA/Registrar concerned on 1st and 2nd violation. (2) Suspension of the activities of the operator concerned on 3rd violation within the month along with email notification to operator/EA/Registrar concerned. (3) Consider imposing financial disincentives on the Registrar	₹10,000 per packet
3	AL	Use of unparliamentarily language / abusive language in demographic details	(1) Email notification to operator/EA/Registrar concerned on 10th, 20th and 25th violation. (2) Suspension of the activities of the	₹50 per packet

			operator concerned on 30th violation within the month along with email notification to operator/EA/Registrar concerned. (3) Consider imposing financial disincentives on the Registrar	
4	DOE-2	**Document Error-2 (DOE-2)** (a) Uploading of poor-quality document/scan (b) Uploading of blank document or document not as per list of supporting documents (c) Uploading of wrong document in the selected document type (d) Uploading of expired or outdated documents like DL, passport, electricity bill, postpaid telephone bill, water bill, etc. (if not otherwise specified) (e) Uploading of only one side of a document whose both sides required for validation (e.g. one side of voter id card is not valid for proof of address) or not uploading all the relevant pages of a document (f) Uploading of photoshop document or document generated from unauthorized website (g) Uploading of wrong relationship document (e.g. relationship	(1) Email notification to operator/EA/Registrar concerned on 10th, 20th and 25th violation. (2) Suspension of the activities of the operator concerned on 30th violation within the month along with email notification to operator/EA/Registrar concerned. (3) Consider imposing financial disincentives on the Registrar	₹ 50 per packet

INDEX

		mentioned in the address part of the document as w/o, h/o, c/o, d/o, s/o etc. shall not be acceptable) (h) Uploading of photocopy of document (i) Uploading of invalid document (j) Uploading of document bearing correction fluid/ overwriting/ cutting etc. without attestation by issuer		
5	DE	**Demographic Error (DE)** (a) Minor typographical errors or demographic data mismatch (b) Transliteration error (c) Wrong selection of gender type/ relationship type (d) Visible age/photo mismatch (e) Any other document or data entry mistakes not covered under DOE-1	(1) Email notification to operator/EA/Registrar concerned on 10th, 20th and 25th violation. (2) Suspension of the activities of the operator concerned on 30th violation within the month along with email notification to operator/EA/Registrar concerned. (3) Consider imposing financial disincentives on the Registrar	₹50 per packet
6	BE	**Biometric Error (BE)** (a) Photo not captured as per guidelines (b) Biometric exception photo not captured properly (c) Photo not of the individual seeking Enrolment/Update (d) Biometric exception photo not of individual seeking enrolment/ update	(1) Email notification to operator/EA/Registrar concerned on 10th, 20th and 25th violation. (2) Suspension of the activities of the operator concerned on 30th violation within the month along with email notification to operator/EA/Registrar concerned. (3) Consider imposing financial disincentives on the Registrar	₹1,000 per packet

INDEX

7	RSV	**Rejection during source verification at QC (RSV):** Document found invalid during source verification	(1) Email notification to operator/EA/Registrar concerned on 10th, 20th and 25th violation. (2) Suspension of the activities of the operator concerned on 30th violation within the month along with email notification to operator/EA/Registrar concerned. (3) Consider imposing financial disincentives on the Registrar	₹ 250 per packet
8	TR	Rejection due to technical issues at UIDAI's end (TR)	—	—

**Without prejudice to any other action which may be taken under the Act.*

Note: In case of multiple errors in a single packet, the error with higher amount of financial disincentive to be marked.

Annex III

Action to be taken for violations of regulations, process, standards, guidelines, orders and the code of conduct provided in the Aadhaar (Enrolment and Update) Regulations, 2016 as identified through other sources or means**

S. No.	Incident / criteria	Action	Rate of financial disincentive
1	Enrolment of adult as a child with age less than five years to avoid collection of biometric	(1) Suspension of the activities of the operator concerned (2) Consider imposing financial disincentives on the Registrar (3) Registrar may file FIR on the operator and shall be reviewed in the SRC meeting	₹ 25,000 per incident
2	Gross violation of the stipulated guidelines such as tampering of UIDAI's software/ Hardware (BYPASS of operator /supervisor Biometrics)	(1) Suspension of the activities of the operator concerned (2) Consider imposing financial disincentives on the Registrar	₹ 25,000 per machine
3	Enrolment of an adult as a child with age less than 18 years to	(1) Suspension of the activities of the operator concerned	₹ 25,000 per incident

	avoid individual's verification	(2) Consider imposing financial disincentives on the Registrar (3) Registrar may file FIR on the operator and shall be reviewed in the SRC meeting	
4	Wrong capturing of biometrics such as capturing reverse biometrics, toes instead of fingerprints, reverse iris etc.	(1) Suspension of the activities of the operator concerned (2) Consider imposing financial disincentives on the Registrar (3) Registrar may file FIR on the operator and shall be reviewed in the SRC meeting	₹ 25,000 per incident
5	Capturing of mixed biometrics	(1) Suspension of the activities of the operator concerned (2) Consider imposing financial disincentives on the Registrar (3) Registrar may file FIR on the operator and shall be reviewed in the SRC meeting	₹ 25,000 per incident
6	Capturing of biometrics using gummy fingers	(1) Suspension of the activities of the operator concerned (2) Consider imposing financial disincentives on the Registrar (3) Registrar may file FIR on the operator and shall be reviewed in the SRC meeting	₹ 25,000 per operator
7	Operating unauthorised enrolment center/ operating from unauthorised location	(1) Suspension of the activities of the operator concerned (2) Consider imposing financial disincentives on the Registrar	₹ 25,000 per operator
8	Overcharging for Aadhaar enrolment and update services/ involvement in corrupt practices	(1) Suspension of the activities of the operator concerned (2) Consider imposing financial disincentives on the Registrar	₹ 25,000 per operator
9	Wrong capturing of biometrics as biometric exception case	(1) Suspension of the activities of the operator concerned (2) Consider imposing financial disincentives on the Registrar (3) Registrar may file FIR on the operator and shall be reviewed in the SRC meeting	₹ 25,000 per packet
10	Identified for non-displaying of rate chart, available services or/and list of documents at	(1) Issue notice to Registrar with details and proof for corrective action within one	₹ 1,000 per incident

INDEX

	enrolment centres during inspection.	week (2) Consider imposing financial disincentives on the Registrar for non-compliance.	

***Without prejudice to any other action which may be taken under the Act.*

***

INDEX

MOST URGENT

File No HQ-16024/4/2021-EU-II-HQ-Part(1)(E-11762)
Unique Identification Authority of India
(Enrolment & Update-II Division)
******

7th Floor, Aadhaar Building,
Bangla Sahib Road, Behind Kali Mandir,
New Delhi-110001
Dated: 23.4.2025

Office Memorandum

Subject: - Online verification of documents presented to evidence identity, address, relationship or date of birth for enrolment and update -reg.

UIDAI endeavors to transition to complete online verification of documents presented to evidence identity, address, relationship or date of birth for enrolment and update from the databases of document issuing authorities.

2. To achieve the same, it is imperative that each document mentioned in the "list of acceptable supporting documents" fulfils the following parameters:

a. Document is digitally issued;
b. Document is digitally verifiable; and
c. Document is available in Digilocker in machine readable form for verification.

3. Accordingly, ROs are requested to coordinate with the concerned State Government / UT Administration and furnish the requisite information against each document mentioned in the attached proforma (Annexure-I). Separate sheets must be added in the Annexure -I for each State/UT under ROs' jurisdiction. List of documents mentioned in the Annexure -I is indicative and ROs may add other State/UT issued documents under the relevant document category.

INDEX

4. In case of manually issued / unverifiable documents, ROs are requested to encourage State Government / UT Administration to issue all the documents in QR coded digitally verifiable format and subsequently take necessary steps to integrate the same in Digilocker in machines readable format for quick verification.

5. Further, it is also pertinent to mention that legacy documents issued before the date of digitization need to be verified from the source. Therefore, ROs may coordinate with the concerned State Government / UT Administration and encourage them to take necessary actions in this regard.

6. ROs are requested to present the duly filled Annexures in the upcoming Management Review Meeting (MRM) to be held on 8th and 9th May, 2025 at Lucknow.

This issues with the approval of the competent authority.

Signed by
Rahul Kumar
Date: 23-04-2025 17:42:12

Rahul Kumar
Director (E&U-II)
UIDAI HO

To,

Deputy Director General of all ROs.

Copy to: Deputy Director General, Technology Centre

HQ-16027/1/2022-EU-I-HQ 1/448827/2025

F. no. HQ-16027/1/2022-EU-I-HQ
Unique Identification Authority of India
Enrolment and Update-I Division

UIDAI Head Office
Near Kali Mata Mandir
Gole Market, New Delhi – 110 001
Dated 11th June 2025

OFFICE MEMORANDUM

Subject: Extension of relaxation in fee charges through myAadhaar portal for document update - reg.

Ref: OM of even number dated 12.12.2024 issued in this regard.

In order to encourage more Aadhaar number holders to update their documents in Aadhaar, it was decided to provide the provision to update their documents in Aadhaar through myAadhaar portal for free of cost up to 14.06.2025.

Based on the positive response from the Aadhaar number holders, it is decided to extend the facility for one more year i.e., from 15.06.2025 to 14.6.2026. Accordingly, the facility for document update shall continue to be free of cost through myAadhaar portal at https://myaadhaar.uidai.gov.in/ up to 14.6.2026.

This is issued with the approval of competent authority.

Signed by Himanshu
Date: 11-06-2025 10:56:44
(Himanshu)
Deputy Director

To
1. All UIDAI Regional Offices
2. UIDAI Tech Centre
3. Director, Media Division HO (*with a request to provide wide publicity*)
4. Director, CRM
5. File.

INDEX

HQ-16034/1/2021-EU-I-HQ I/45348/2025

F. no. HQ-16034/1/2021-EU-I-HQ
Unique Identification Authority of India (UIDAI)
(Enrolment and Update-I Division)

UIDAI Head Office
Near Kali Mata Mandir
Gole Market, New Delhi – 110 001
Dated 25 June 2025

Office Memorandum

Subject: Initiation of Aadhaar enrolment and update Services using the Universal Client application - reg

This is to inform that UIDAI has introduced the Universal Client (UC) as a standard application for carrying out Aadhaar enrolment and update services under a single platform.

2. All existing enrolment and update client application versions would shortly be phased out and all Registrars and Enrolment Agencies (EAs) are required to transition to the UC client application.

3. Accordingly, it is requested to initiate necessary actions to adopt and implement the UC application across the machines operating at all the Aadhaar enrolment centres functioning under the Registrars. The key steps include:

a) Installation of latest version of UC at all enrolment/update stations as per UIDAI guidelines.
b) Training of operators on the new interface and workflows of the UC. Training workshops for master trainers of Registrars are being organized at four locations. Further, the training material on UC is under preparation and will be shared in due course.

4. It is requested to render support and cooperation in ensuring a smooth and timely transition. For further clarifications or technical assistance, UIDAI Regional Offices and Tech Support teams may be contacted.

Yours sincerely,

Himanshu
(Deputy Director)

To:
UIDAI Regional Offices (*for dissemination to all the Registrars*)

Copy to:
UIDAI Tech Centre, Bengaluru.

INDEX

F. No. HQ-16054/1/2024-EU-II-HQ (E-13969)

Unique Identification Authority of India

(Enrolment and Update-II Division)

UIDAI Head Office
Bangla Sahib Road
New Delhi – 110 001
Dated:07.07.2025

Circular

(02/2025)

Subject: Procedure for submitting request for reactivation of Aadhaar number in cases where Aadhaar number holder was reported to be deceased

Unique Identification Authority of India (UIDAI) deactivates the Aadhaar number of the deceased person based on validation and matching of death registration details with the database of death registering authority and Aadhaar database.

2. In case, at a later date, it is found that the Aadhaar number was deactivated based on reported deceased status, but the Aadhaar number holder is alive, he/she may follow the procedure below for reactivation of his/her Aadhaar number:

(a) Aadhaar number holder may submit the request for reactivation of his/her Aadhaar number in the prescribed application format (Annexure) to the nearest Regional Office/State Office through post, email or in person. The details of the Regional Offices/State Offices are provided at the official website of UIDAI i.e., www.uidai.gov.in.

(b) Regional Office/State Office, on receipt of such request, will examine the request and call the Aadhaar number holder at a designated Aadhaar centre for submitting his/her full biometric information (face, iris and fingers) under the supervision of UIDAI official, within two weeks of receipt of such application.

(c) Regional Office/State Office concerned will inform the Aadhaar number holder about the status of disposal of the request within 30 days of submission of the biometric information. The status of disposal of the request will also be intimated to the Aadhaar number holder through SMS. The Aadhaar number holder may also check the same on 'myAadhaar' portal.

INDEX

(d) In case, it is established that Aadhaar number was deactivated based on reported deceased status but the Aadhaar number holder is alive, the Aadhaar number will be reactivated and UIDAI will inform Registrar of Births and Deaths concerned with a copy to Registrar General of India and the Aadhaar number holder.

3. This issues with the approval of competent authority.

Signed by
Tushar Kumar Rakshit
Date: 07-07-2025 18:06:20

(Tushar Kumar Rakshit)
Dy. Director (E&U-II)

Encl: Annexure

HQ-16054/1/2024-EU-II-HQ

I/45707/2025

Annexure

Format for application by Aadhaar number holder for re-activation of Aadhaar number
(In terms of Regulation 31 (2) of the Aadhaar (Enrolment and Update) Regulations, 2016)

1.	Aadhaar Number	
2.	Name	
3.	Gender	
4.	Date of Birth	
5.	Parent's name and Aadhaar number (Only in case Aadhaar number holder is less than 18 years of age)	
6.	Address	
7.	District	
8.	State	
9.	Mobile Number	
10.	Email Address (If available)	
11.	Any other information	
12.	Signature / Thumb Impression	
13.	Place	
14.	Date	

INDEX

F.no. HQ-16024/4/2020-EU-I-HQ-Part(1)
Unique Identification Authority of India (UIDAI)
(Enrolment & Update-I Division)

7th floor, UIDAI Head Office
Bangla Sahib Road, Behind Kali Mandir
Gole Market, New Delhi-110 001
Dated: 18th July 2025

Subject: Standard Operating Procedure (SOP) for appointment of a new Registrar/Enrolment Agency (EA) - reg

Please refer to the SOP on the above subject issued on 27.5.2022.

2. In supersession of the above SOP, a revised process to be followed for appointment of a new Registrar/EA is as follows:

(i) Entities may submit their request for appointment as a UIDAI Registrar/EA to the Regional Office (RO) concerned.

(ii) RO shall verify the request based on the eligibility, requirement and feasibility, and forward to UIDAI HeadOffice (HO) with clear recommendations and tentative plan of the entity for opening Aadhaar enrolment centers and carrying out Aadhaar enrolment and update services. The request should be submitted in e-Office with the approval of DDG, RO along with duly filled checklist (enclosed).

(iii) E&U-I Division, HO shall examine the proposal and allot Registrar/EA code, upon approval of competent authority.

(iv) Upon receipt of Reg/EA code, RO shall submit a signed copy of Terms of Engagement (ToE) to E&U-I Division, for records.

(v) RO shall coordinate with Tech Centre for completing the onboarding process of Registrar/EA.

(vi) RO shall collect requests for creation of Registrar/EA Admin and forward to Tech Support with approval of officials not below the rank of Director, RO.

(vii) In case the Registrar has all-India presence and is mapped to Nodal RO but EAs are mapped with different ROs, the above process of Registrar Admin onboarding shall be completed by Nodal RO, where the Headquarter of Registrar is situated. Regarding EAs, concerned RO shall onboard the EA Admin.

(viii) The L1, L2 registration and operator onboarding shall be performed by the mapped RO where the EA is onboarded.

3. It may be noted that, as per the Terms of Engagement that are required to be signed by the entity upon appointment as a Registrar, the Registrar may onboard any of its subordinate office(s)/unit(s) as an EA to provide Aadhaar related services with the prior approval of UIDAI.
An entity that does not fall under the administrative control of a Registrar cannot be appointed as an EA under it.

4. Further, as per Regulation 21(7) of Aadhaar (Enrolment and Update) Regulations, 2016, ***"Registrars shall not permit sub-contracting of enrolment functions by enrolling***

INDEX

agencies to third parties. Registrars may permit field level manpower to be hired through third parties provided the enrolling agencies furnishes details of the entities from which such manpower is sought to be hired". As such, if required, Registrars (either directly or through their EAs) may hire field level manpower on salary basis.

5. This issues with the approval of competent authority.

Enclosed: Checklist for Appointment of a new Registrar/EA.

Signed by Himanshu
Date: 18-07-2025 13:39:01

(Himanshu)
Deputy Director (E&U-I)

To:

UIDAI Regional Offices
UIDAI Technology Centre, Bengaluru

INDEX

HQ-16024/4/2020-EU-I-HQ-Part(1) I/46039/2025

Checklist for Appointment of a new Registrar/EA

1. Entity Name: _____

2. Request for onboarding as: Registrar ☐ Enrolment Agency ☐ Both ☐

3. Name of existing Registrar:
(in case of appointment for new EA) _____

4. Specify the category of entity as per Regulation 21(1) of Aadhaar (E&U) Regulations, 2016:

State/UT Government	☐	Central Ministry	☐
Department/Agency under Central Ministry	☐	Public Sector company of Central Govt	☐
Public Sector company of State Govt	☐	Scheduled Banks	☐
Regulated entities	☐	SPV created by Central Government	☐
SPV created by State Government	☐		

5. Category as per In-house model OM dated 30.1.2023: Category A ☐ Category B ☐

6. Number of Aadhaar enrolment centres proposed:
along with locations (location list to be enclosed) _____

7. Aadhaar enrolment equipment owned by: Registrar ☐ EA ☐

8. Source of amount for procurement of equipment:

ICT by UIDAI ☐ Central Govt. funds ☐ State Govt. funds ☐ Registrar/EA ☐

9. Ownership of Premises:

Govt. owned ☐ Govt. hired/leased ☐ Registrar/EA owned ☐

10. Mode of employment of:- Operators: Employees on payroll of Registrar/EA ☐
Hired through manpower agency (salaried) ☐

Supervisors: Employees on payroll of Registrar/EA ☐
Hired through manpower agency (salaried) ☐

11. Name of manpower hiring agency (if applicable): _____

12. Additional details of equipment and operators to be enclosed as annexure, if required.

13. Justification (attach additional document, if required):

Date:

Sign & Stamp
(Officer not below the rank of Director, RO)

INDEX

HQ-16011/2/2022-EU-I-HQ I/47511/2025

F.no. HQ-16011/2/2022-EU-I-HQ
Unique Identification Authority of India (UIDAI)
(Enrolment and Update-I Division)

UIDAI Head Office
Bangla Sahib Road, Behind Kali Mandir
Gole Market, New Delhi – 110 001
Dated 11.9.2025

Office Memorandum

Subject: One-time financial assistance to Department of Post & State Government UIDAI registrars for replacement of L0 single fingerprint device scanner in line with requirement of L1 registered devices for the purpose of biometric authentication during Aadhaar enrolment and update - reg.

In order to enhance the security levels of fingerprint based authentication transaction and end-to-end encryption during the authentication process, fingerprint devices used in Aadhaar authentication ecosystem have been upgraded from currently used L0 to the next generation L1 Registered Device (RD). Authentication Division, vide letters in F.no. HQ-13021/1/2021-Auth-I HQ dated 27.01.23, 25.3.25 and 23.5.25, has issued directions to all AUA/KUAs/ASAs to phase out fingerprint L0 Registered Devices from Aadhaar authentication ecosystem.

2. UIDAI has granted financial assistance to Registrars of Central and State Governments/UT Administrations under various phases in order to facilitate procurement of Aadhaar enrolment kits for use in targeted Aadhaar enrolment to cover the unenrolled population. L1 devices have been included in the latest specifications of Enrolment Client Multiple Platform (ECMP) and Child Enrolment Lite Client (CELC) kits released *vide* OM No. F. No. HQ-16031/1/2021-EU-I-HQ dated 01.07.2024 (OM 1 of 2024) and OM No. F. No. HQ-16031/1/2021-EU-I-HQ dated 01.07.2024 (OM 2 of 2024) respectively. To ensure that L1 fingerprint scanner registered devices are used in all ECMP and CELC kits for authentication, UIDAI shall provide financial assistance to the tune of maximum amount of ₹2,500/- (including GST) per L1 fingerprint scanner device to Department of Post and State Government registrars for procurement of such registered devices. This assistance shall be provided subject to fulfilment of following conditions:

i. Assistance shall be provided only for those ECMP/CELC kits which have been procured from Central/State Government funding;
ii. Assistance shall be considered only for kits, the details of which have been provided by Regional Offices (ROs);
iii. This shall be a one-time assistance only.

3. The requirement of number of L1 finger-print scanner devices has been received from all ROs. Keeping an additional 20% of the received number, details of consolidated number of devices for which assistance shall be provided to Registrars are as below:

INDEX

HQ-16011/2/2022-EU-I-HQ I/47511/2025

	Regional Office	Number of L1 devices requested
1	Bengaluru	4875
2	Chandigarh	518
3	Delhi	6412
4	Guwahati	1683
5	Hyderabad	7223
6	Lucknow	1647
7	Mumbai	7577
8	Ranchi	3356
	Total	**33,291**
	Additional 20%	**39,949**

4. The funds for financial assistance shall be disbursed in the following manner:
   i. RO shall submit the consolidated requirements received from Registrars in the form of Detailed Project Report (DPR) along with due recommendations for consideration to UIDAI HO;
   ii. UIDAI HO, upon approval of competent authority, shall provide Budget availability of the eligible amount to the Registrars under intimation to RO concerned;
   iii. The Registrar shall initiate the procurement process and place the Purchase order as per the "Budget availability" informed by UIDAI HO;
   iv. The ICT assistance amount shall be disbursed upon production of copies of the Invoices from Registrar against procurement of L1 fingerprint scanner registered devices; and
   v. Utilisation certificate for the amount utilised shall be furnished to the HO within a period of one month of the release of funds. Any unspent amount of the funds shall be refunded to UIDAI along with accrued interest earned at the prevailing savings bank rate during the period.

5. This issues with the approval of competent authority.

Signed by Himanshu
Date: 11-09-2025 12:39:55

(Himanshu)
Deputy Director
Tel.: 011-23478444
Email: dd.eu1-hq@uidai.net.in

To:

1. DDG, UIDAI Regional Offices (*with a request to disseminate to Registrars*)
2. DDG, Technology Centre
3. DDG, Authentication Division, UIDAI HO
4. Guard file

INDEX

HQ-16033/1/2020-EU-I-HQ-Part(2) I/47838/2025

F. no. HQ-16033/1/2020-EU-I-HQ-Part (2)
Unique Identification Authority of India (UIDAI)
(Enrolment and Update-I Division)

7th floor, UIDAI Head Office
Behind Kali Mandir, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated: 19 September 2025

Office Memorandum

Subject: Rates of financial assistance provided by UIDAI to registrars against Aadhaar generation and Mandatory Biometric Update (MBU) services, and fees to be collected by registrars for other Aadhaar services – regarding

In supersession of the OM of even number dated 20.4.2023, and pursuant to the approval accorded by the Authority, the rates of financial assistance provided by UIDAI to registrars against Aadhaar generation and MBU services, and fees to be collected by registrars for other Aadhaar services stand revised as follows:

Table-1
Effective for the period from 1.10.2025 to 30.9.2028:

S. no.	Service	Rate of assistance to registrar* (₹, incl. GST)	Fee to be collected from resident by registrar/service provider (₹, incl. GST)
1	Aadhaar Generation of residents in 0-5 age group (ECMP/ UC or CEL Client enrolment)	75	Free of cost
2	Aadhaar Generation of residents more than 5 years age	125	Free of cost
3	Mandatory Biometric Update (5 to 7 years and 15 to 17 years)	125	Free of cost
4	Mandatory Biometric Update (7 to 15 years & more than 17 years)	-	125
5	Other Biometric Update (with or without Demographic Update)	-	125
6	Demographic update (update of one or more fields) in online mode or at Aadhaar Enrolment Centre using ECMP/ UCL/ UC/ CELC	-	75
7	PoA/PoI Document Update at Aadhaar Enrolment Centre	-	75

INDEX

8	PoA/PoI Document Update through SSUP (myAadhaar) Portal	-	75
9	Aadhaar Search using eKYC/ Find Aadhaar/any other tool & colour printout on A4 Sheet	-	40

**Financial assistance is applicable only to the successful transactions*

Table-2

Effective for the period from 1.10.2028 to 30.9.2031:

S. no.	Service	Rate of assistance to registrar* (₹, incl. GST)	Fee to be collected from resident by registrar/service provider (₹, incl. GST)
1	Aadhaar Generation of residents in 0-5 age group (ECMP/ UC or CEL Client enrolment)	90	Free of cost
2	Aadhaar Generation of residents more than 5 years age	150	Free of cost
3	Mandatory Biometric Update (5 to 7 years and 15 to 17 years)	150	Free of cost
4	Mandatory Biometric Update (7 to 15 years & more than 17 years)	-	150
5	Other Biometric Update (with or without Demographic Update)	-	150
6	Demographic update (update of one or more fields) in online mode or at Aadhaar Enrolment Centre using ECMP/ UCL/ UC/ CELC	-	90
7	PoA/PoI Document Update at Aadhaar Enrolment Centre	-	90
8	PoA/PoI Document Update through SSUP (myAadhaar) Portal	-	90
9	Aadhaar Search using eKYC/ Find Aadhaar/any other tool & colour printout on A4 Sheet	-	50

**Financial assistance is applicable only to the successful transactions*

2. The charges for Home enrolment services shall be ₹700 (including GST) and will be charged in addition to the normal fee applicable for demographic/biometric update in Aadhaar. If the service is availed by more than one resident at the same address (as per Aadhaar), ₹700 service charge (including GST) will be charged for first resident and ₹350 (including GST) for each additional resident.

INDEX

HQ-16033/1/2020-EU-I-HQ-Part(2) I/47838/2025

3. For Registrars which are not functioning under in-house model as per OM No. 16024/4/2022-EU-I-HQ-Part(1) dated 30.01.2023, the applicable rates for assistance remain unchanged, as tabulated below:

Table-3

S. no.	Service	Rate of assistance to registrar* (₹, incl. GST)	Fee to be collected from resident by registrar/service provider (₹, incl. GST)
1	Aadhaar Generation	50	Free of cost
2	Mandatory Biometric Update (with or without Demographic Update)	50	Free of cost

**Financial assistance is applicable only to the successful transactions*

4. This issues with the approval of competent authority.

Yours faithfully,

Digitally signed by Himanshu
Date: 21-09-2025 10:12:01

(Himanshu)
Deputy Director (E&U-I)

To:

All Registrars/EAs (through notification)
Regional Offices of UIDAI

Copy to:

UIDAI Technology Centre, Bengaluru
Media/CRM Division
File.

INDEX

F. no. HQ-16034/1/2021-EU-I-HQ-Part(1)
Unique Identification Authority of India (UIDAI)
(Enrolment and Update-I Division)

7th floor, UIDAI Head Office
Near Kali Mata Mandir
Gole Market, New Delhi – 110 001
Dated: 29th September 2025

OFFICE MEMORANDUM

Subject: Waiver of charges for Mandatory Biometric Update - 1 (MBU-1) of children aged 7 to 15 years - reg.

An Aadhaar number holder is required to update his/her Aadhaar with the biometric information upon attaining the age of 5 and 15 years. The Mandatory Biometric Update (MBU) service is free of cost to the children in the age groups of 5 - 7 years and 15 - 17 years.

2 In order to reduce the MBU pendency in mission mode, the Authority has decided to waive off the charges to be collected from the Aadhaar number holders for carrying out MBU-1 in the age group of 7 - 15 years for a period of one year, *w.e.f.* 1.10.2025.

3. This is issued with the approval of competent authority.

(Himanshu)
Deputy Director

To
1. UIDAI Tech Centre
2. All UIDAI Regional Offices
3. Director, Media Division HO (*with a request to provide wide publicity*)
4. Director, CRM
5. File.

INDEX

File No- HQ-16022/2/2020-EU-II-HQ-Part(1) (E-1133)
Unique Identification Authority of India
(Enrolment & Update Division-II)
*****

UIDAI Head Office, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated: 24.12.2025

Standard Operating Procedure for Date of Birth update in Aadhaar

This Standard Operating Procedure (SOP) is being issued in supersession of all previous communications issued by UIDAI regarding update of date of birth in Aadhaar database including Standard Operating Procedure (SOP) to update Date of Birth (DoB) under exception handling process vide letter No. HQ 16022/2/2020-EU-II-HQ-Part (1) dated 19.07.2021.

The basic tenets for the purpose of update of date of birth in Aadhaar are being highlighted below: -

1. **An individual can have only one Date of Birth (DoB).** Therefore, under the normal circumstances, there should be **No Need** to change the date of birth in Aadhaar database. From the experience, it has been seen that the following three circumstances may necessitate an updation or correction or change in the date of birth:
    a. Currently the DoB is declared or approximate and needs to be updated to a verified DoB.
    b. An error or mistake on part of the operator or the Aadhaar number holder (ANH) leads to incorrect DoB getting recorded inadvertently.
    c. Where the ANH (or the parent or guardian of the ANH, if the ANH is a child) had reported a wrong DoB with false or fraudulently obtained supporting documents in the past and now wants to mend the past wrongdoing and correct the DoB with a verifiable document.
2. A Birth Certificate is the legal proof of DoB. Therefore, once a Birth Certificate has been submitted as Proof of Date of Birth (PDB) document, no further DoB updates should be considered under normal circumstances.
3. For enrolment of children below 5 years of age, Birth Certificate is the mandatory document. Nowadays, the CRS and other State Registrars of Births issue digital

INDEX

versions of the older Birth Certificates. Children in the age group of 5-18 years can easily procure the online-verifiable Birth Certificates.

4. UIDAI cannot turn a blind eye to the cases where false or fraudulently obtained documents have been submitted by ANH (or the parent or guardian of the ANH, if the ANH is a child) to get a wrong date of birth recorded in Aadhaar database. At the same time, UIDAI would not like to prevent them forever from correcting their past mistake. This is also essential to ensure the integrity and continued accuracy of the Aadhaar database and maintain the trust of the user entities. Therefore, such ANH will be provided one last opportunity to correct the DoB in his/her Aadhaar. **The Aadhaar of such ANH would be deactivated whenever such a case comes to light either during DoB update request or otherwise. The deactivated Aadhaar will be considered for reactivation when a DoB update request is mandatorily accompanied by a genuine online-verifiable PDB document along with an affidavit by the ANH (or the parent or guardian of the ANH, if the ANH is a child). In such cases, depending on the circumstances, an FIR may also be lodged against the ANH or the parent or the guardian, as the case may be.**

5. Rules defined in the "important note" section of the "*List IV – Documents that may be presented to evidence Proof of Identity, Address, Relationship or Date of Birth for update of information in respect of Aadhaar Number Holder of any age*" of Schedule II of the Aadhaar (Enrolment and Update), Regulations 2016 (hereafter mentioned as "*List-IV*"), also serve as basic guiding principles. The same are being reproduced as follows:

   a. *Request for update of date of birth in Aadhaar shall be accepted, in the following manner:*

      (i) If date of birth is recorded as declared or approximate:

         a. *For resident Indians below 18 years of age: - Aadhaar number holder shall mandatorily submit birth certificate as proof of date of birth.*

         b. *For Non-Resident Indian (NRI) below 18 years of age: - Aadhaar number holder shall submit birth certificate or Indian Passport as proof of date of birth.*

         c. *For resident Indians and Non-Resident Indian (NRI) of 18 years and above of age: - Aadhaar number holder shall submit any of the*

acceptable proof of date of birth documents as specified in the above list.

(ii) If the Aadhaar number holder had earlier submitted birth certificate as proof of date of birth, the Aadhaar number holder shall submit corrected birth certificate bearing same Birth Registration Number (BRN).

(iii) If the Aadhaar number holder had earlier submitted any proof of date of birth document except birth certificate (for e.g. Marksheet, Passport etc.), the Aadhaar number holder shall submit corrected version of the same document or submit a birth certificate.

(iv) In case of date of birth update of woman who has changed her name post-marriage, proof of date of birth documents issued pre-marriage will be accepted along with evidence of name change (Aadhaar with old name or marriage certificate with both names).

6. Based on the guiding principles mentioned above, this SOP is being issued. It covers an exhaustive list of scenarios, which are detailed below:

Case 1: Indian Resident applies for DoB update for the first time

a) ***If the existing DoB in Aadhaar is 'declared' or 'approximate'***:

UIDAI may enable the Aadhaar Number Holder (ANH) to view his DoB in Aadhaar as ***'declared' or 'approximate' or 'verified'*** during the process of DoB updation in the enrolment-client. DoB update in all such cases can be carried out based on any of the permitted PDB document as mentioned in "*List-IV*". For the age group 0-5 years and 5-18 years, Birth Certificate is the only document permitted for DoB update.

There may be cases wherein the DoB in Aadhaar is 'declared' or 'approximate', but Aadhaar Number Holder (ANH) has submitted Birth Certificate during enrolment or update as one of the supporting documents (PDB or PoR document), such cases shall be handled as cases of DoB in Aadhaar as 'verified' based on birth certificate as given below in Para (b) (i).

b) ***If the existing DoB in Aadhaar is 'verified'***:

Following scenarios may arise in this category:

i) Even though the DoB may be recorded as 'verified' but the PDB document does not exist in the Aadhaar database. Such a case shall be treated as a

case of ***'declared' or 'approximate'*** DoB outlined at para (a) above. For the age group 0-5 years and 5-18 years, Birth Certificate is the only document permitted for DoB update.

ii) **DoB was recorded as 'verified' in Aadhaar database based on Birth Certificate:** If the document submitted at the time of enrolment was a Birth Certificate, there should be no need for DoB update under normal circumstances. Some exceptional circumstances may arise where the Birth Certificate itself may require correction. **In such cases, the only document acceptable for DoB update would be the corrected Birth Certificate with the same BRN and issued by the same registrar as earlier, along with an affidavit (Annex-I).** If a document, other than Birth Certificate, is submitted or a Birth Certificate with a different BRN or from a different registrar is submitted, the update request shall be rejected.

This shall apply irrespective of the age group for all Indian residents.

iii) **DoB was recorded as 'verified' in Aadhaar database based on PDB document other than Birth Certificate:** In such a case also, there should be no need for DoB update under normal circumstances. But under exceptional circumstances, the document submitted earlier may itself require correction. In such an exceptional scenario, the Aadhaar number holder shall submit either a **corrected version of the same document (document must be a part of the existing list of valid PDB documents) or a Birth Certificate along with an affidavit (Annex-I).** If the document submitted earlier is not a part of the current list of valid PDB documents, then the only document admissible would be a Birth Certificate.

Corrected version of the same document means the document issued by the same authority, same description, same year and same details except the corrected date of birth. For example: a mark sheet issued for the same qualification but by appearing in the exam again in a different year would **NOT** mean the same document.

This will apply to all Indian residents 18 years of age or above and will NOT apply to children below 18 years of age.

c) **Cases where operator error is alleged:** If the DoB in Aadhaar differs from that mentioned in the PDB document earlier submitted by the ANH, and the current update request is for change to the same DoB mentioned in that earlier

document, it is a case of 'operator error'. If the earlier submitted document by the ANH is still a valid PDB document as per the existing list, ANH may submit DoB update request with the same document as the earlier submitted document. However, if the earlier submitted document by the ANH is no longer a valid PDB document as per the existing list or ANH is not in possession of the same document, the DoB update request may be permitted based on self-declaration (Annex-II) submitted by ANH stating that his/her DoB was incorrectly entered by operator. The PDB document submitted by ANH at the time of enrolment will be checked to establish the alleged operator error.

All the scenarios mentioned above under "Case 1", shall also be applicable to Non-Resident Indians (NRIs) with one exception that in case of ANH below 18 years of age, NRIs may submit Birth Certificate or Indian Passport as defined in the list of acceptable documents.

Case 2: Indian Residents / NRIs – Subsequent DoB updates

In an exceptional scenario, Aadhaar number holder may request for subsequent update of his/her DoB as below:

a) A subsequent DoB update after the first update done since enrolment, **shall be processed only on submission of Birth Certificate (in cases where the earlier PDB document during enrolment or DoB update was not a Birth Certificate), or corrected Birth Certificate with same BRN and registrar (in cases where the earlier PDB document during enrolment or DoB update was a Birth Certificate) along with an affidavit (Annex-I), as the case may be.**

This will apply irrespective of the age group to all Indian residents/NRIs.

b) **Cases where operator error is alleged:** If the current DoB in Aadhaar differs from that mentioned in the last PDB document submitted by the ANH, and the current update request is for change to the same DoB mentioned in that last document, it is a case of 'operator error'. If the submitted document by the ANH is still a valid PDB document as per the existing list, ANH may submit DoB update request with the same document as the earlier submitted document. However, if the earlier submitted document by the ANH is no longer a valid PDB document as per the existing list or ANH is not in possession of the same document, the DoB update request may be permitted based on self-declaration (Annex-II) submitted by ANH stating that his/her DoB was incorrectly entered. The PDB

document submitted by ANH at the time of enrolment/update will be checked to establish the alleged operator error.

Case 3: Enrolment in 0-5 years of age and first or subsequent DoB update

a) If an individual had enrolled in the 0-5 years age category and is trying to update the age in such a way that the age of the ANH on the date of enrolment was actually more than 5 years, **it is clearly a case of fraud** because it means that the individual had enrolled without giving biometrics even though s/he was more than 5 years old at the time of enrolment. All such update request would be rejected and Aadhaar may be deactivated / omitted as per provisions of The Aadhaar (Enrolment and Update) Regulations, 2016.

   Legal action may be initiated against the ANH (the parent or guardian, if the ANH is a child) as well as the Aadhaar centre operator, if s/he is found to have colluded in such process of fraudulent enrolment.

Case 4: Enrolment in 5-18 years of age and first or subsequent DoB update

a) If an individual had enrolled in the 5-18 years age category and is trying to update the age in such a way that the age of the ANH on the date of enrolment was actually more than 18 years, **it is clearly a case of fraud** because it means that the individual had enrolled as a minor. If the enrolment was done on or after the date of operation of State Portal for that State, the individual had also bypassed the verification by the State authorities even though s/he was more than 18 years old at the time of enrolment. All such update request would be rejected and Aadhaar may be deactivated as per provisions of The Aadhaar (Enrolment and Update) Regulations, 2016.

   Depending on the findings, legal action may be initiated against the Aadhaar number holder along with the individual posing as the Head of Family of the ANH (if applicable) as well as the Aadhaar centre operator who colluded in the process of enrolment.

An Aadhaar deactivated due to scenarios mentioned at cases 3 & 4 above or due to submission of a fraudulent PDB document, may be reactivated through the concerned Regional Office with correct date of birth by performing a full biometric update (face, iris and fingers) along with an **online verifiable Birth Certificate (except for the States/ Districts/ Cantonment Boards/ Embassies or any other**

registrar of births and deaths which are not issuing online verifiable Birth Certificate) and affidavit (Annex-III), at any Aadhaar Seva Kendras / any Government centre designated for this purpose by the Regional Offices. For scenario in case 4, the case would also be sent to the State portal for verification before taking any further action in the process of reactivation.

Case 5: Resident Foreigners – DoB Updates

a) The PDB document is also the Proof of Identity (PoI) document for foreign residents. Hence the need for DoB update should arise only due to operator errors. If the DoB in Aadhaar differs from that mentioned in PoI cum PDB document(s), and the update request is for change to the same DoB mentioned in those document(s), it is a case of operator error. DoB in such cases should be updated as per the document submitted at the time of enrolment, by submitting a self-declaration (Annex-II) stating that his/her DoB was incorrectly entered by operator.
DoB update request will not be entertained on any other grounds for the resident foreigners.

7. This issues with the approval of Competent Authority.

Rahul Kumar
24.12.2025
(Rahul Kumar)
Director, E&U-II

Annexure-I- For Adults

Affidavit for date of birth updation

(Applicable for cases where the DoB is verified in Aadhaar. To be printed on non-judicial stamp paper of minimum value of ₹ 10)

1. I, _____ S/D/W/o _____, resident of _____ holding Aadhaar number _____, do hereby solemnly affirm and declare as under:-
   i) That I am the resident of the above said address.
   ii) That my correct date of birth is _____.
   iii) That the earlier recorded date of birth in Aadhaar is _____ based on _____ document submitted by me.
   iv) That I have _____ (never/ once/ more than once) updated my date of birth in Aadhaar.
   v) That currently a corrected version of the same document as mentioned in (iii) above / birth certificate (choose as applicable) is being provided in support of DoB update request.
   vi) That I wish to get my date of birth updated in the Aadhaar as _____, for which I am submitting _____ as proof of date of birth.
   vii) That I further undertake that I shall not be eligible for any further updation of my date of birth in Aadhaar.
2. I undertake that if the document submitted as proof of date of birth is found to be fraudulent/false/forged/non-genuine or I was not entitled for the said document, my Aadhaar number may be deactivated as per Regulation 28 of the Aadhaar (Enrolment and Update) Regulations, 2016 and I shall be liable to be prosecuted under provisions of the applicable law.
3. I hereby declare that all the information mentioned above is true to the best of my knowledge. In case of any discrepancies, the undersigned will be held responsible.

Date **Name & Signature of Resident (Deponent)**

(This affidavit may be signed and attested in presence of a Judicial Magistrate or Executive Magistrate/Notary Public)

INDEX

Annexure IA- For children

Affidavit for date of birth updation

(Applicable for cases where the DoB is verified in Aadhaar. To be printed on non-judicial stamp paper of minimum value of ₹ 10)

1. I, _____ S/D/W/o _____, resident of _____holding Aadhaar number_____, do hereby solemnly affirm and declare as under:-
2. That I am the resident of the above said address.
   i) That I am the resident of the above said address.
   ii) That I am parent/legal guardian of the _____*<<name of child>>*_____ holding Aadhaar number_____.
   iii) That correct date of birth of my child/ ward is _____.
   iv) That the earlier recorded date of birth in Aadhaar of my child/ward is _____ based on _____ document submitted by me.
   v) That I have _____ (never/ once/ more than once) updated my child/ward date of birth in Aadhaar.
   vi) That birth certificate of my child/ward is being provided in support of DoB update request.
   vii) That I wish to get my child/ward date of birth updated in the Aadhaar as _____, for which I am submitting his/her birth certificate as proof of date of birth.
   viii) That I further undertake that my child/ward shall not be eligible for any further updation of date of birth in Aadhaar.
3. I undertake that if the document submitted as proof of date of birth is found to be fraudulent/false/forged/non-genuine or my child/ward was not entitled for the said document, the Aadhaar number of my child/ward may be deactivated as per Regulation 28 of the Aadhaar (Enrolment and Update) Regulations, 2016 and I shall be liable to be prosecuted under provisions of the applicable law.
4. I hereby declare that all the information mentioned above is true to the best of my knowledge. In case of any discrepancies, the undersigned will be held responsible.

Date **Name & Signature of Parent /Guardian of Minor (Deponent)**

(This affidavit may be signed and attested in presence of a Judicial Magistrate or Executive Magistrate/Notary Public)

INDEX

Annexure II- For adults

Self-Declaration requesting DoB update for correcting operator error / typographical mistake

1. I, _____ S/D/W/o _____, resident of _____ holding Aadhaar number_____, do hereby solemnly affirm and declare as under: -
   i) That I am the resident of the above said address.
   ii) That I had earlier submitted a valid document-_____, bearing number_____, dated_____ while enrolment / update through EID number_____, as proof of date of birth for updating my date of birth in Aadhaar.
   iii) That the date of birth was incorrectly mentioned as _____ in Aadhaar, while the date of birth mentioned in the submitted valid document was _____, which is indeed my correct date of birth.
   iv) That I do not have possession of earlier submitted proof of date of birth document/ the document then submitted is no longer a valid proof of date of birth. (choose applicable)
2. I request UIDAI to update my date of birth based on previously submitted and then valid proof of date of birth document.
3. I undertake that if the earlier document submitted as proof of date of birth is found to be fraudulent/false/forged/non-genuine or I was not entitled for the said document, my Aadhaar number may be deactivated as per Regulation 28 of the Aadhaar (Enrolment and Update) Regulations, 2016.
4. I hereby declare that all the information mentioned above is true to the best of my knowledge. In case of any discrepancies if arises, the undersigned will be held responsible.

Date **Name & Signature of Resident**

INDEX

Annexure IIA- For children

Self-Declaration requesting DoB update for correcting operator error / typographical mistake

1. I, _____ S/D/W/o _____, resident of _____ holding Aadhaar No_____, do hereby solemnly affirm and declare as under: -
   i) That I am the resident of the above said address.
   ii) That I am parent/legal guardian of the _____<<name of child>>_____ holding Aadhaar No_____.
   iii) That I had earlier submitted a valid document-_____, bearing number_____, dated_____ while enrolment / update through EID number_____, as proof of date of birth for updating date of birth of my child/ward in Aadhaar.
   iv) That the date of birth of my child/ward was wrongly mentioned as _____ in Aadhaar, while the date of birth mentioned in the submitted valid document was _____ , which is indeed the correct date of birth of my child/ward.
   v) That I do not have possession of earlier submitted proof of date of birth document/ the document then submitted is no longer a valid proof of date of birth. (choose applicable)
2. I request UIDAI to update date of birth of my child / ward based on previously submitted and then valid proof of date of birth document.
3. I undertake that if the earlier document submitted as proof of date of birth is found to be fraudulent/false/forged/non-genuine or my child/ward was not entitled for the said document, Aadhaar number of my child/ward may be deactivated as per Regulation 28 of the Aadhaar (Enrolment and Update) Regulations, 2016.
4. I hereby declare that all the information mentioned above is true to the best of my knowledge. In case of any discrepancies if arises, the undersigned will be held responsible.

Date **Name & Signature of Parent /Guardian of Minor**

INDEX

Annexure III-For adults

Affidavit for reactivation of Aadhaar

(To be printed on non-judicial stamp paper of minimum value of ₹ 10)

1. I, _____S/D/W/o _____, resident of_____ holding Aadhaar number _____, do hereby solemnly affirm and declare as under: -
   i) That I am resident of the above said address.
   ii) That I had earlier submitted an invalid document -_____, bearing number_____, dated_____ and provided false information, while enrolment/update through EID number _____, as proof of date of birth.
   iii) That I understand and accept that submission of such invalid document and false information is a violation of law and legal action may be taken against me for the same under Aadhaar Act and/or any other applicable laws.
   iv) That I sincerely regret this act and tenders an unconditional apology and ensures that such mistake shall not be repeated.
   v) That I humbly seek pardon and request UIDAI to kindly reactivate my Aadhaar number _____to enable its continued usage.
   vi) That I undertake to submit only genuine, correct and verifiable proof of date of birth document _____ in support of my request to reactivate my Aadhaar.
   vii) The I further undertake that I shall not be eligible for any further updation of my date of birth in Aadhaar.
2. I undertake that if the document submitted as proof of date of birth is found to be fraudulent/false/forged/non-genuine or I was not entitled for the said document, my Aadhaar number may again be deactivated as per Regulation 28 of the Aadhaar (Enrolment and Update) Regulations, 2016 and I shall be liable to be prosecuted under provisions of the applicable laws.
3. I hereby declare that all the information mentioned above is true to the best of my knowledge. In case of any discrepancies if arises, the undersigned will be held responsible.

Date **Name & Signature of Resident (Deponent)**

(This affidavit may be signed and attested in presence of a Judicial Magistrate or Executive Magistrate/Notary Public)

INDEX

Annexure IIIA-For children

Affidavit for reactivation of Aadhaar

(To be printed on non-judicial stamp paper of minimum value of ₹ 10)

1. I, _____S/D/W/o _____, resident of_____ holding Aadhaar number _____, do hereby solemnly affirm and declare as under: -
   i) That I am resident of the above said address.
   ii) That I am parent/legal guardian of the _____<<name of child>>_____ holding Aadhaar No_____.
   iii) That I had earlier submitted an invalid document-_____, bearing number_____, dated_____ or provided false information, while enrolment/update through EID number _____, as proof of date of birth of my child/ward.
   iv) That I understand and accepts that submission of such invalid document and false information is a violation of law and legal action may be taken against me for the same under Aadhaar Act and/or any other applicable laws.
   v) That I sincerely regret this act and tenders an unconditional apology and ensures that such mistake shall not be repeated.
   vi) That I humbly seek pardon and request UIDAI to kindly reactivate my child/ward Aadhaar number _____ to enable its continued usage.
   vii) That I undertake to submit only genuine, correct and verifiable proof of date of birth document _____ in support of my request to reactivate my child/ward Aadhaar.
   viii) The I further undertake that my child/ward shall not be eligible for any further updation of date of birth in Aadhaar.
2. I undertake that if the document submitted as proof of date of birth is found to be fraudulent/false/forged/non-genuine or my child/ward was not entitled for the same, Aadhaar number of my child/ward may again be deactivated as per Regulation 28 of the Aadhaar (Enrolment and Update) Regulations, 2016 and I shall be liable to be prosecuted under provisions of the applicable laws.
3. I hereby declare that all the information mentioned above is true to the best of my knowledge. In case of any discrepancies if arises, the undersigned will be held responsible.

Date **Name & Signature of Parent /Guardian of Minor (Deponent)**

(This affidavit may be signed and attested in presence of a Judicial Magistrate or Executive Magistrate/Notary Public)

INDEX

B
LOGISTICS

F.No. 14014/8/2011-Logistics Vol.II
Government of India
Ministry of Electronics & IT
Unique Identification Authority of India
(Logistics Division)
*****

9th Floor, Tower-I, Jeevan Bharti Building,
Connaught Circus, New Delhi-110001
Dated the 28th April, 2017

CIRCULAR

Subject: Validity of downloaded Aadhaar (e-Aadhaar) as Proof of identity – regarding.

The Unique Identification Authority of India (UIDAI) is a statutory body under Section 11 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits & Services) Act, 2016 (Aadhaar Act, 2016) which came into force on 12.09.2016. The UIDAI is mandated to issue 12 digit Unique Identification number called Aadhaar to the residents based on demographic and biometric information submitted by them to the UIDAI during enrollment. Aadhaar number is communicated to the residents in physical form (Aadhaar letter) by post. UIDAI also provides facility to download Aadhaar in electronic form (Downloaded Aadhaar or e-Aadhaar) on its website (https://uidai.gov.in/).

2. UIDAI is receiving requests from various organisations/individual residents seeking clarification on validity of downloaded Aadhaar (e-Aadhaar) as various authorities are not accepting downloaded Aadhaar. This circular is being issued to clarify the validity of downloaded Aadhaar (e-Aadhaar).

3. As per Section 4(3) of Aadhaar Act, 2016:

> *" An Aadhaar number, in physical or electronic form subject to authentication and other conditions, as may be specified by regulations, may be accepted as proof of identity of the Aadhaar number holder for any purpose ".*
>
> [Explanation- For the purposes of this sub-section, the expression "electronic form" shall have the same meaning as assigned to it in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000].

4. Further, as per Regulation 15 (1) of the Aadhaar (Enrolment and Update) Regulations, 2016:

> The Aadhaar number may be communicated to residents in physical form (including letters or cards) and/or electronic form.

5. It is informed that downloaded Aadhaar (e-Aadhaar) carries Name, Address, Gender, Photo and Date of Birth details of the Aadhaar holder in similar form as in Printed Aadhaar letter. The downloaded Aadhaar also contains date of Aadhaar generation and date of Aadhaar download. The downloaded Aadhaar (e-Aadhaar) is a digitally signed document by UIDAI as per IT Act, 2000 which provides for legal recognition of electronic records with digital signatures.

INDEX

6. Downloaded Aadhaar (e-Aadhaar) is, therefore, as legally valid proof of identity under Section 4(3) of the Aadhaar Act, 2016 read together with Regulation 15 (1) of the Aadhaar (Enrolment and Update) Regulations, 2016, as printed version of Aadhaar Letter.

7. It is, therefore, clarified that, **Downloaded Aadhaar (e-Aadhaar) is a valid and secure electronic document which should be treated at par with printed Aadhaar letter.** Ministries/Departments/State Governments/agencies accepting printed Aadhaar as proof of identity are hereby required to accept downloaded Aadhaar (e-Aadhaar) also as a proof of identity and not to discriminate it vis-a-vis printed Aadhaar.

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

(B.M. Patnaik)
Deputy Director (Logistics)

Copy to:

1. Secretaries to the Government of India, All Ministries/ Departments of Government of India.
2. All Chief Secretaries to the State Government/Union Territories.
3. All DDGs of UIDAI HQ and ROs.
4. UIDAI Webmaster, Website.

INDEX

F.No.11014/07/2020-Logistics
Government of India
Ministry of Electronics & IT
Unique Identification Authority of India
(Logistics Division)
*****

6th Floor, UIDAI HQ,
Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi-110001

Dated: 29.09.2020

CIRCULAR

Subject: Introduction of Aadhaar Card for use at par with other forms of Aadhaar like Aadhaar letter, e-Aadhaar, masked e-Aadhaar and m-Aadhaar.

UIDAI has introduced a new service known as "Order Aadhaar Card (OAC)" for facilitating Indian residents to get their Aadhaar number and demographic details on a PVC card by paying a nominal charge @ Rs.50/-. The Aadhaar card is delivered at the registered address of the resident through speed post service of India Post. It is pocket sized verifiable identity of residents which is easy to carry and durable. Similar to other forms of Aadhaar, it has a digitally signed secure QR code with photograph and demographic details verifiable by using STQC certified scanner devices with Windows application and Android/iOS mobile scanner App available on Google play store/Apple store.

2. Aadhaar card can be ordered online by visiting UIDAI's official website (http://www.uidai.gov.in or https://resident.uidai.gov.in) and using Aadhaar number (UID), VID or enrollment ID. A sample Aadhaar card issued by UIDAI is annexed for reference.

3. Aadhaar card is a valid proof of identity like other forms of Aadhaar such as Aadhaar letter, e-Aadhaar, masked e-Aadhaar and m-Aadhaar under section 4(3) of the Aadhaar Act, 2016 read with Regulation 15(1) of the Aadhaar (Enrolment and Update) Regulations, 2016. It is a valid and secure document which should be treated at par with Aadhaar letter, e-Aadhaar, masked e-Aadhaar and m-Aadhaar. Ministries/Departments/State Governments/Autonomous bodies/other agencies accepting Aadhaar as proof of identity are requested to accept Aadhaar Card also as a proof of identity.

4. It is emphasized that Aadhaar card, Aadhaar letter, e-Aadhaar, masked e-Aadhaar and m-Aadhaar are all equally valid forms of Aadhaar to be used by the resident as per their choice and all of them should be accepted as proof of identity with due validation without giving any preference to one form of Aadhaar over the other.

(Pooran Chand)
Assistant Director General (Logistics & CRM)

To

1. Secretaries to the Government of India, All Ministries/ Departments of Government of India.
2. All Chief Secretaries to the State Government/Union Territories.
3. Autonomous bodies/other agencies.

Copy to:
All DDGs of UIDAI HQ and ROs for information

INDEX

Annexure

Pictorial Representation of Aadhaar PVC Card:

INDEX

F.No.HQ-22017/3/2022-LOG-HQ
Ministry of Electronics & IT
Unique Identification Authority of India
(Logistics and Channel Interface Division)

6th floor, Aadhaar HQ, Bangla Sahib Road,
Behind Kali Mandir, Gole Market,
New Delhi – 110001
Dated: 22.03.2023

CIRCULAR

Subject: Usage of Aadhaar-Do's and Don'ts of the Tamper Proof QR Code scanning by residents

Aadhaar's Tamper Proof QR code is used for Offline Verification of identity without connecting to the CIDR (Central Identities Data Repository) of UIDAI. The Tamper Proof QR code is unique, encrypted and tamper-proof. It contains the photograph and demographics of the resident which cannot be duplicated as it is digitally signed. This is an essential security component that establishes the authenticity of the document, as presented by the resident seeking service from an Offline Verification Seeking Entity (OVSE). Aadhaar digitally signed Tamper Proof QR code can be read by using UIDAI's windows, android and iOS based scanners and validated with UIDAI's digital signature. These scanner applications are freely available for both Android and iOS based mobile phones as well as Windows based applications. The scanner is also available as part of UIDAI's m-Aadhaar mobile application, for both Android and iOS phones.

2. Residents may voluntarily use the Aadhaar number for a lawful purpose, to establish their identity by way of offline verification by an OVSE. For the purpose of offline verification by an OVSE, the Aadhaar number holder may use his/her Aadhaar either in (i) the physical form like Aadhaar letter (or copy thereof) or printed e- Aadhaar or Aadhaar PVC Card.

Following are the Do's and Don'ts to be followed by residents while using the Tamper Proof QR code:

Do's

1. QR Code scanner works best for PVC card, in case PVC card is not available then Do ensure to have good quality print in case of E-Aadhaar or photocopy of Aadhaar letter/PVC card.
2. Do use only STQC certified scanners available on UIDAI website while using Windows app for Tamper Proof QR code scanning.
3. Do ensure to use only UIDAI mobile applications namely **mAadhaar** and **Aadhaar QR Code scanner** for Android and iOS to read Aadhaar Tamper Proof QR code available on eAadhaar, Aadhaar letter & PVC card.
4. Do download the authorised Aadhaar QR Code scanner from the Google Play Store or the Apple store (or wherever else it is available).
5. Do note, that the Aadhaar QR Code scanner – standalone app and Windows app works without any requirement of internet connectivity.
6. Do use torch given in the app in low light conditions.
7. Do ensure to lay the Tamper Proof QR code within the rectangular box in mAadhaar for scanning.
8. Do use mAadhaar app to generate and share your Tamper Proof QR code in file format/soft copy.

Don'ts

1. Don't move the device while scanning the Tamper Proof QR code
2. Don't use the inferior/faded print or photocopy for scanning the Tamper Proof QR code.
3. Don't allow any entity to scan your Tamper Proof QR code for offline verification without your consent.

(Mayank Jhingan)
Deputy Director, Logistics & CI

INDEX

File No.: HQ-22017(11)/1/2025-LOG-HQ (Computer No. 17831)
भारतीय विशिष्ट पहचान प्राधिकरण
(लोजिस्टिक्स प्रभाग)

छठा तल, आधार, बंगला साहिब रोड
काली मंदिर के पीछे, गोल मार्केट
नई दिल्ली – 110001
दिनांक : 17.10.2025

CIRCULAR

Subject: **Discontinuation of Aadhaar Hologram on Aadhaar PVC Card- reg.**

UIDAI provides a facility to Aadhaar holders for ordering Aadhaar PVC Card through Order Aadhaar PVC Card Service. Till recently, Aadhaar PVC Card was being issued with Aadhaar Hologram.

2. However, it has now been decided to discontinue the use of Aadhaar Hologram on Aadhaar PVC Card. Henceforth, Aadhaar PVC Card will be issued without Hologram.

3. This issues with the approval of the Competent Authority.

(Mayank Jhingan)
Deputy Director, Logistics Division

Copy for information to:
1. OSD to CEO UIDAI
2. All DDGs/Directors, UIDAI Head office
3. All DDGs/Directors, UIDAI ROs/TC

INDEX

File No.: HQ-22017(12)/4/2021-LOG-HQ (Computer No. 6434)
Unique Identification Authority of India
(Logistics Division)

6th Floor, UIDAI HQ, Bangla Sahib Road
Behind Kali Mandir, Gole Market
New Delhi – 110001
Dated : 12.12.2025

Office Memorandum

Sub.: Revision of rate of Aadhaar PVC card service from ₹ 50/- to ₹ 75/- (including taxes).

The Unique Identification Authority of India (UIDAI) has been providing Aadhaar Number Holders the facility to order Aadhaar PVC Cards through the myAadhaar portal and the mAadhaar mobile application. This service was introduced in the year **2020**, and since its inception, a nominal charge of **₹50/- per PVC card** (inclusive of all taxes and delivery charges) has been levied.

2. Over the years, the cost of materials, printing, secure delivery, and related logistics for Aadhaar PVC Card production and distribution has increased. In view of the rising operational expenditure and with the objective of ensuring continued high-quality service delivery, the Authority has reviewed the existing fee structure.

3. Accordingly, it has now been decided to revise the rate for the Aadhaar PVC Card service from ₹50/- to ₹75/- (including taxes). The revised rate shall be applicable with effect from 1st January 2026 for all Aadhaar PVC Card orders placed through the myAadhaar portal or the mAadhaar mobile app.

4. This issues with the approval of the Competent Authority.

(Mayank Jhingan)
Deputy Director, Logistics Division

INDEX

C
HUMAN RESOURCE

Unique Identification Authority of India

Policy on engagement of Young Professionals with the Authority

1. Object and purpose

1.1 UIDAI has a unique mandate, which includes shaping the technology vision and developing the technology strategy and deep tech for Aadhaar as the foundational layer of the India stack. UIDAI's Technology Centre at Bengaluru is responsible for meeting all technological, data engineering and information security needs of UIDAI, developing the Aadhaar technology stack, undertaking research and development and supporting innovation and partnerships. Details in this regard are at Annex.

1.2 UIDAI recognises that in the development and realisation of this technology vision, strategy and deep tech, young technologists capable of finding unconventional solutions to unique problems and build solutions that can solve population scale problems can be a key resource. The Young Professionals (YP) Programme offers a platform for fresh technology graduates to create world-class innovative solutions and contribute to India's digital transformation by enriching the India stack.

1.3 The programme envisions YPs as constituting a key stream contributing to UIDAI's in-house talent pool for developing a continuous pipeline for technology solutions and innovations.

2. Programme overview

2.1 The YP Programme is a structured programme of engagement of YPs selected from premier technology institutions across India, with high degree of flexibility and systematic opportunities for the YPs—

(a) to familiarise themselves with the working of and the challenges and opportunities associated with the Aadhaar ecosystem;
(b) to have one-on-one mentorship of UIDAI technology team leaders and architects;
(c) to get guidance from internal technology team and access external experts in a wide range of technology domains;
(d) to identify problems and potential solutions and innovations that may represent value for the ecosystem;
(e) to pitch project proposals, individually or jointly with other YPs, to a select group of technology champions and domain experts who shall assess the same based on technological suitability and the value proposition;

INDEX

(f) to explore potential partnership with startups, industry, academia and accomplished professionals, consistent with UIDAI's policies and programmes in this regard;
(g) to explore and move from one business division or technology domain in UIDAI to another, on the basis of interest and mutual fit;
(h) to lead technology teams after gaining requisite experience and displaying leadership attributes; and
(i) for professional enrichment and skill development through participation in relevant training programmes, conferences and technology events in India and abroad.

2.2 The programme is for an initial period of three years with option of extension by further periods of two years at a time.

3. Programme structure

3.1 In the first two years of engagement, UIDAI will assign the YP either to existing technology teams or assign them independent projects under the guidance of a senior architect or Development Lead, aimed at giving them practical experience of implementing technology solutions, gaining an understanding of the Aadhaar stack and learning the back- and front-end technologies used by UIDAI.

3.2 From the third year, a YP may be designated as Development Lead and may identify problems and potential solutions and innovations that represent value for the ecosystem and pitch project proposals, individually or jointly with other YPs. Projects approved on the basis of the YP's proposal may be in addition to their work on existing teams or continuation of previously assigned projects. In case of the approved projects, the YP may either be the project lead or a key member of the project team.

3.3 From the fifth year, a YP may be designated as Architect and may also explore potential project partnership with startups, industry, academia and accomplished professionals, consistent with UIDAI's policies and programmes in this regard. Projects approved on the basis of the YP's proposal may be in addition to their work on existing teams or continuation of previously assigned projects. In case of the approved projects, the YP may either be the project lead or a key member of the project team.

3.4 Approved projects from the third year onwards may include commitment of fresh resources, including financial and technological, for operationalising the same, subject to UIDAI's normal project approval processes.

3.5 In case of exceptional performance, a YP may be given the next level designation in advance of the years referred to above. Further, in respect of a project

INDEX

proposal of significant value, a YP may be permitted to pursue the same in advance of the years referred to above.

3.6 YPs will be given quarterly goals in a consultative manner, appraised on their performance and given feedback. They will be given opportunity to showcase their work on a half-yearly basis before the YP Programme Steering Group and to interact with it, with a view to identify the direction and pathways for future professional development. The Group shall include both the internal technology team and external experts.

***

INDEX

Annex

Regarding UIDAI's technological mandate

1. The Unique Identification Authority of India (UIDAI) has the mandate to develop and manage Aadhaar as the foundational public infrastructure of the India stack. This includes developing the technology vision to meet future ecosystem needs, drive innovation and forge partnerships for adopting and contributing to cutting-edge technology and innovation.

2. The all-encompassing mandate and canvas of UIDAI offers a unique opportunity to shape the technology vision and develop the technology strategy and deep tech for enabling India's digital transformation at population scale. UIDAI's functions and activities include:

(a) Meeting the digital identity needs of over 1.3 billion Aadhaar holders;
(b) Developing the policy, procedure and systems for Aadhaar issuance and authentication;
(c) Establishing, operating and maintaining the Central Identities Data Repository of UIDAI;
(d) Enabling over 2,300 use cases spanning the government, financial and ICT sectors and allowing new use cases;
(e) Regulating, laying down standards and specifications and supervising the Aadhaar ecosystem, consisting of about 700 Aadhaar-enrolling and over 500 Aadhaar-authenticating entities;
(f) Laying down the standards and specifications for registered biometric authentication devices;
(g) Specifying the processes for Aadhaar data management, security protocols and other technology safeguards;
(h) Developing new modalities and improved models for biometrically establishing identity; and
(i) Promoting research and development for advancement in biometrics and related areas, including usage of Aadhaar numbers through appropriate mechanisms.

***

INDEX

Unique Identification Authority of India (UIDAI)

Guidelines for recruitment of Personnel as Volunteers

1. Short Title and Commencement

(1) These Guidelines may be called UIDAI Volunteers Guidelines, 2022.
(2) They shall come into force at once.

2. Object and Purpose

The Government of India has constituted Unique Identification Authority of India with the mandate to issue Unique IDs to the Residents of the country. Considering that the UID project is a unique venture in its design, scope, size and implementation and will be chartering unknown territories in the areas of technology, logistics and computing, it is necessary that it has access to the world-class professionals in the areas of ICT (database, cryptology, data-mining, biometric, AI/ML, Machine Learning simulation, etc.), management, contract, procurement and public administration.

Further, expertise would also be required to formulate long term technology roadmap, including enterprise architecture and innovation management, redesign/re-architect existing UIDAI solution, transformation of UIDAI's business model, products etc.

To venture out and excel in these areas, talents may not be necessarily available with the Government, hence UIDAI is willing to take people from industry and academia to work with the UIDAI on Volunteer basis from their parent organization so that these experts play a key role in improving Aadhaar eco-system.

3. Definition: Unless the Context requires otherwise, following words shall have the meaning attributed to them in these Guidelines for the purpose of these Guidelines.

(1) "Authority" means The Unique Identification Authority of India

(2) A "Volunteer" is a person who wants to give services to the Authority, either on a part-time basis or on a full-time basis, without any remuneration from the Authority.

(3) "Area of Expertise" means the subject or area in which the Volunteer possesses expertise.

4. Identification of Volunteers: The Authority may follow any of the processes given below to identify volunteers.

INDEX

(1) The Authority may, whenever it has the requirement of volunteers for any specific area or job(s), post an advertisement on its website prescribing the procedure to be followed for application from potential volunteers or may write to industry bodies/associations or academic institutions calling for willing candidates to apply for volunteers in UIDAI.

(2) Any person who wishes to provide his services on a voluntary basis to the Authority may apply to the Authority as per the application form attached to these Guidelines.

5. Criteria and Methodology for selection: The Authority will follow the following methodology for deciding if an applicant can be accepted as a Volunteer of the Authority:

(1) Based on the application for becoming a Volunteer, the Authority shall assess if the Volunteer's services are required in his/her area of expertise. The Authority will then conduct an interview (personal or telephonic).

(2) If the Authority is satisfied that the Applicant possesses requisite specialized skill, experience and qualification, has relevant professional/volunteer experience, has satisfactory background and reference and that there is no conflict of interest between the Applicant working as a Volunteer for the Authority and any other work the Volunteer may be engaging in either for gain or a Volunteer, then the Authority will issue an offer letter along with the specific role for the Volunteer and the reporting structure. The Volunteer will convey acceptance by signing the offer letter and the non-disclosure and confidentially agreement of the Authority.

(3) In case of applications received under Guideline 3(2) of these Guidelines, the Authority shall first determine if the services of the Volunteer are needed in the Area of Expertise of the person. If there are Volunteers in the Authority working in the Area of Expertise indicated by the applicant, then the determination will include whether or not more Volunteers are required in that area.

(4) The Authority may, from time to time and on a case by case basis issue job titles to certain volunteers who have roles that carry responsibility and have a high component of interaction with third parties. The titles must reflect the work that the Volunteer does in the Authority and should enable these specific Volunteers to represent themselves to third parties on behalf of the Authority as required in order to fulfill their responsibilities to the Authority.

INDEX

6(a). Code of Conduct: The Volunteers appointed by the Authority shall observe the following Code of Conduct, which shall include, but not be limited to, the following:

(1) The Volunteers shall follow the policies of the Authority that are in general applicable to employees of the Authority.

(2) The Volunteer shall follow the confidentiality protocol of the Authority and shall not reveal to any person or organization confidential information of the Authority, its work and its polices. Some Volunteers may specifically be authorized to interact with third parties on behalf of the policies as well as the Volunteer's work in the Authority.

(3) In general a Volunteer may not represent the Authority vis a vis third parties. Some Volunteers may specifically be authorised to interact with third parties on behalf of the Authority depending on the nature of their roles and responsibilities.

(4) Volunteer interaction with third parties should be need based; in particular no Volunteer shall interact with or represent the Authority to the media (print and electronic).

(5) Volunteer may, with the prior permission of the Authority, present their work to academic bodies and at seminars and conferences. However, even for this purpose information that is confidential to the Authority cannot be revealed under any circumstances.

(6) Volunteers will follow the advice given to them by the Authority regarding representation to third parties.

(7) Any paper and documents written and /or published by the Volunteer should carry the caveat that the views are the personal views of the Volunteer and do not represent or reflect the views of the Authority.

(8) Volunteers shall develop work plans and work schedules in consultation with their supervisor and will adhere to the same.

(9) Volunteers will conduct themselves professionally in their relationship with the Authority and the public in general.

(10) Volunteers will be required to submit a report of their work prior to leaving the Authority.

INDEX

6(b). Conflict of interest from private sector members moving from one category of employment to another

Current designation in the UIDAI	Volunteer	Sabbatical member	PMU/TSU member	Employee of any other organisation
New designation in the UIDAI/Role Volunteer	NA	Need NoC from parent sabbatical organisation &subject to Volunteer selection guidelines	Acceptable –subject to Volunteer guidelines	Acceptable –subject to Volunteer guidelines
Sabbatical member	NA	NA	NA	NoC from parent organisation as per sabbatical guidelines & specific approval of UIDAI & parent organization in case joining another organisation during the tenure
PMU/TSU member	Acceptable-subject to **PMU/TSU** selection guidelines	Need NoC from parent Sabbatical organisation & subject to **PMU/TSU** selection guidelines	NA	Acceptable-subject to **PMU/TSU** Selection guidelines
Joining any other organisation	Require approval to safeguard UIDAI's interest	Require approval to safeguard UIDAI-interest	Require approval to safeguard UIDAI's interest	NA

7. Termination: Either the Volunteer or the Authority may terminate the relationship under any one of the following situations:

(1) The Authority may disengage the Volunteer if the Authority is of the view that the services of the volunteer are no more required.

(2) In general the Authority may terminate the services of the Volunteer at any time without assigning any reasons and with immediate effect.

(3) In general, if the Volunteer decides to disengage from the Authority, he should provide 2 weeks' prior notice. However, the Authority may, in certain cases, particularly long term Volunteers, prescribe a notice period of upto one month. Notice period may be waived from time to time by the supervisor depending on the role of the Volunteer.

(4) Upon termination, the Volunteer must hand over to the Authority, any papers, equipments or other tangible assets which might have been given to the Volunteer by the Authority in course of his work with the Authority. This

INDEX

will include any badges or ID Cards which may have been issued to the Volunteer.

(5) If it comes to the notice of the Authority that the person whose services have been terminated by the Authority continues to act in a manner which gives an impression that he is still working as a volunteer for the Authority, the Authority shall be free to take appropriate legal action against such person.

8. Power to Remove Difficulties: The Authority shall have the power to remove any difficulty which comes in the way of the implementation of these Guidelines.

INDEX

Annexure

Volunteer Application Form
(see Guideline3(2))

1. Covering Letter with the following information (not more than 500 words)
    a. Area of Expertise of the person.
    b. Why they would like to work as a Volunteer with the Authority.
    c. How the Authority would benefit from the Volunteer working with the Authority.
2. Curriculum Vitae
3. Two references

INDEX

[To be published in the Gazette of India, Extraordinary, Part I, Section 2]
Ministry of Electronics and Information Technology
Unique Identification Authority of India

4th Floor, Bangla Sahib Road
Behind Kali Mandir
Gole Market, New Delhi – 110 001
Dated 19th June 2023

NOTIFICATION

F. No. A-19011/306/2023-UIDAI.—In pursuance of the Secretariat of the Appointments Committee of the Cabinet (ACC) communication no. 36/02/2023-EO(SM-I), dated 11.6.2023 conveying that ACC has approved appointment of Shri Amit Agrawal, IAS (CG:93) as Chief Executive Officer (CEO), Unique Identification Authority of India (UIDAI) in the rank and pay of Additional Secretary to the Government of India, and consequent upon his relieving from the Ministry of Electronics and Information Technology *vide* the Ministry's Office Order (G.No. 62/2023) dated 19.6.2023, it is hereby notified that Shri Amit Agrawal, IAS (CG:93) has assumed the office of CEO, UIDAI in the forenoon of 19th June 2023.

(Alok Shukla)
Deputy Director General
Tel: 23478331

To

The Manager
Government of India Press
Minto Road, Delhi

Copy to:

1. Shri Amit Agrawal, Chief Executive Officer, Unique Identification Authority of India
2. PS to Hon'ble Minister, Electronics and Information Technology
3. PS to Hon'ble Minister of State, Electronics and Information Technology
4. PS to Secretary, Ministry of Electronics and Information Technology
5. Secretary (ACC & EO), ACC Secretariat, Department of Personnel & Training, Room No. 115, North Block, New Delhi
6. Secretary, General Administration Department, Govt. of Chhattisgarh, Mantralay, Mahanadi Bhawan, Atal Nagar, Nawa Raipur, Chhattisgarh – 492101.
7. CVO, Ministry of Electronics and Information Technology
8. Director (SM), Department of Personnel & Training, Room No. 20, North Block, New Delhi
9. Sh. Devender Pal, Deputy Director, GC Section, Ministry of Electronics and Information Technology, Electronics Niketan, 6 - CGO Complex, New Delhi –110003- For updation in AVMS portal
10. All DDGs/Directors & ADGs of UIDAI
11. OSD to CEO, UIDAI
12. PS to CEO, UIDAI
13. DDO, UIDAI
14. PAO, UIDAI
15. DD(Admin.), UIDAI, Headquarters
16. Admn Division/HR-II Section/RTI Cell/Co-ordination Division/Enforcement Cell/ Legal Division/Enrolment & Updation Division/ Media Division/Cashier
17. Service Book of Shri Amit Agrawal, CEO, UIDAI
18. Assistant Manager (HR), UIDAI

INDEX

[भारत के राजपत्र, असाधारण, भाग I, खंड 2 में प्रकाशनार्थ]

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

भारतीय विशिष्ट पहचान प्राधिकरण

चतुर्थ तल, बंगला साहिब रोड,
काली मंदिर के पीछे,
गोल मार्किट, नई दिल्ली-110001
दिनांक 19 जून, 2023

अधिसूचना

फा.सं.ए-19011/306/2023-यूआईडीएआई — श्री अमित अग्रवाल, आईएएस (सीजी:93) के अपर सचिव, भारत सरकार के वेतन एवं रैंक में मुख्य कार्यकारी अधिकारी, भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई) के रूप में नियुक्ति के विषय में मंत्रिमंडल की नियुक्ति संबंधी समिति के अनुमोदन के अनुसार मंत्रिमंडल की नियुक्ति संबंधी समिति (एसीसी) सचिवालय की दिनांक 11.6.2023 की संसूचना संख्या 36/02/2023-ईओ(एसएम-I) और तत्पश्चात उन्हें इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय से दिनांक 19.6.2023 के कार्यालय आदेश (जी.सं. 62/2023) के तहत कार्यभार मुक्त किए जाने के अनुसरण में, यह एतद्द्वारा अधिसूचित किया जाता है कि श्री अमित अग्रवाल, आईएएस (सीजी:93) ने 19 जून, 2023 की पूर्वाह्न से मुख्य कार्यकारी अधिकारी, भारतीय विशिष्ट पहचान प्राधिकरण का पदभार ग्रहण कर लिया है।

आलोक शुक्ला

(आलोक शुक्ला)
उपमहानिदेशक
दूरभाष: 23478331

सेवा में,

प्रबंधक
भारत सरकार मुद्रणालय
मिंटो रोड, दिल्ली

प्रतिः

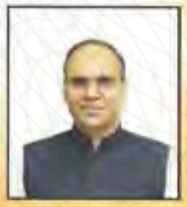
1. श्री अमित अग्रवाल, मुख्य कार्यकारी अधिकारी, भारतीय विशिष्ट पहचान प्राधिकरण
2. माननीय इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री के निजी सचिव
3. माननीय इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री के निजी सचिव
4. सचिव, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री के निजी सचिव
5. सचिव(एसीसी एवं ईओ),एसीसी सचिवालय, कार्मिक एवं प्रशिक्षण विभाग, कमरा सं. 115, नार्थ ब्लॉक, नई दिल्ली
6. सचिव, सामान्य प्रशासन विभाग, छत्तीसगढ़ सरकार, मंत्रालय, महानदी भवन, अटल नगर, नवा रायपुर, छत्तीसगढ़ -492101
7. सीवीओ, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
8. निदेशक(एसएम), कार्मिक एवं प्रशिक्षण विभाग, कमरा सं. 20, नार्थ ब्लॉक, नई दिल्ली
9. श्री देवेन्दर पाल, उप निदेशक, जीसी अनुभाग, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय, इलेक्ट्रॉनिक्स निकेतन, 6-सीजीओ कांप्लेक्स, नई दिल्ली-110003 – एचीएमएस पोर्टल पर अपलोड हेतु
10. सभी उपमहानिदेशक/निदेशक एवं सहायक महानिदेशक, भारतीय विशिष्ट पहचान प्राधिकरण

जारी.....2/-

INDEX

11. मुख्य कार्यकारी अधिकारी के विशेष कार्य अधिकारी, यूआईडीएआई
12. मुख्य कार्यकारी अधिकारी, यूआईडीएआई के निजी सचिव
13. आहरण और संवितरण अधिकारी, यूआईडीएआई
14. वेतन एवं लेखा अधिकारी, यूआईडीएआई
15. उप निदेशक (प्रशासन), भा.वि.प.प्राधिकरण मुख्यालय
16. प्रशासन प्रभाग/मानव संसाधन-II अनुभाग/आरटीआई प्रकोष्ठ/समन्वय प्रभाग/प्रवर्तन अनुभाग/ विधि प्रभाग/नामांकन एवं अद्यतन प्रभाग/मीडिया प्रभाग/कैशियर
17. श्री अमित अग्रवाल, मुख्य कार्यकारी अधिकारी, यूआईडीएआई की सेवा-पुस्तिका
18. सहायक प्रबंधक (मानव संसाधन), यूआईडीएआई

INDEX



सत्यमेव जयते

आधार
मेरा आधार, मेरी पहचान

अमित अग्रवाल भा.प्र.से.
मुख्य कार्यकारी अधिकारी, भा.वि.प.प्रा

संदेश

हिंदी दिवस के अवसर पर भारतीय विशिष्ट पहचान प्राधिकरण के सभी अधिकारियों एवं कर्मचारियों को मेरी हार्दिक शुभकामनाएं।

भारत प्रारंभ से ही संस्कृति, कला और विज्ञान के क्षेत्र में एक संपन्न राष्ट्र है। भारत एक बहुभाषी देश है और यहां कई भाषाएं एवं बोलियां बोली जाती हैं। ये सभी भाषाएं अपने-अपने क्षेत्र में बहुत ही समृद्ध और सशक्त हैं। प्रत्येक भाषा की अपनी एक अलग सांस्कृतिक और साहित्यिक पहचान है। हिंदी अपने अलग-अलग स्वरूपों में, सदियों से एक संपर्क भाषा के रूप में सभी संस्कृतियों को जोड़ने का कार्य कर रही है। भाषा की इसी महत्ता को ध्यान में रखते हुए 14 सितंबर, 1949 के दिन हिंदी को संवैधानिक रूप से भारत संघ की राजभाषा का दर्जा प्रदान किया गया और तभी से प्रत्येक वर्ष 14 सितंबर को 'हिंदी दिवस' के रूप में मनाया जाता है।

भारतीय विशिष्ट पहचान प्राधिकरण, भारत के निवासियों को आधार नंबर के जरिए एक विशिष्ट पहचान उपलब्ध कराने, आधार से जुड़ी हुई नामांकन एवं अद्यतन, अधिप्रमाणन आदि सेवा प्रदान करने और भारत सरकार की विभिन्न योजनाओं में बायोमेट्रिक सत्यापन द्वारा पहचान सुनिश्चित करने में महत्वपूर्ण भूमिका निभा रहा है। भारत सरकार द्वारा अधिदेशित कार्यों के साथ-साथ प्राधिकरण के प्रधान कार्यालय और क्षेत्रीय कार्यालयों में संघ की राजभाषा नीतियों, आदेशों, दिशानिर्देशों और योजनाओं का भी सहर्ष पालन किया जा रहा है और उनके कार्यान्वयन को प्रभावी रूप से लागू किया जा रहा है। भारतीय विशिष्ट पहचान प्राधिकरण अपने कार्यालयों में संघ की राजभाषा के कार्यान्वयन को भलीभांति सुनिश्चित करने के अन्यत्र विभिन्न बोलियों एवं भाषाओं से संबद्ध देश के निवासियों को हिंदी सहित कुल 13 भाषाओं में आधार से जुड़ी विविध उल्लेखनीय सेवाएं प्रदान कर रहा है।

भारत सरकार की राजभाषा नीति प्रेरणा और प्रोत्साहन पर आधारित है और हमारा संवैधानिक कर्तव्य है कि हम राजभाषा संबंधित नीतियों एवं दिशानिर्देशों का अनुपालन सुनिश्चित करें। हिंदी दिवस के अवसर पर मैं प्राधिकरण के सभी अधिकारियों और कर्मचारियों से अपील करता हूं कि वे स्वयं भी अपना सरकारी काम-काज हिंदी में करें और अपने सहकर्मियों को भी इसके लिए प्रेरित और प्रोत्साहित करें। हिंदी दिवस के अवसर पर हिंदी पखवाड़े के दौरान आयोजित विभिन्न प्रतियोगिताओं और कार्यक्रमों में अपनी भागीदारी सुनिश्चित करें और आयोजन को सफल बनायें।

हिंदी दिवस के शुभ अवसर पर आप सभी को पुनः मेरी हार्दिक शुभकामनाएं।

नई दिल्ली
14 सितंबर, 2024

अमित अग्रवाल
मुख्य कार्यकारी अधिकारी

INDEX

रजिस्ट्री सं. डी.एल.- 33004/99 REGD. No. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-19052025-263226
CG-DL-E-19052025-263226

असाधारण
EXTRAORDINARY
भाग I—खण्ड 2
PART I—Section 2
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 22] नई दिल्ली, सोमवार, मई 19, 2025/वैशाख 29, 1947
No. 22] NEW DELHI, MONDAY, MAY 19, 2025/VAISAKHA 29, 1947

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

(भारतीय विशिष्ट पहचान प्राधिकरण)

अधिसूचना

नई दिल्ली, 9 मई, 2025

फा. सं. ए-19011/339/2024-यूआईडीएआई.—श्री भुवनेश कुमार, आईएएस (यूपी:1995), अपर सचिव को भारत सरकार के अपर सचिव के पद और वेतन में मुख्य कार्यकारी अधिकारी (सीईओ), भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई) के रूप में नियुक्ति के विषय में मंत्रिमंडल की नियुक्ति संबंधी समिति के अनुमोदन के अनुसार मंत्रिमंडल की नियुक्ति संबंधी समिति (एसीसी) सचिवालय की संसूचना संख्या 36/02/2025-ईओ (एसएम-I) दिनांक 18.04.2025 तथा इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय से दिनांक 30.04.2025 के मंत्रालय के कार्यालय आदेश संख्या 4(1183)/2021-Pers.I के तहत कार्यभार मुक्त किए जाने के अनुसरण में, यह एतद्वारा अधिसूचित किया जाता है कि श्री भुवनेश कुमार, आईएएस (यूपी:1995) ने 1 मई 2025 को पूर्वाह्न में मुख्य कार्यकारी अधिकारी (सीईओ), भारतीय विशिष्ट पहचान प्राधिकरण का पदभार ग्रहण कर लिया है।

विवेक चंद्र वर्मा, उपमहानिदेशक

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

(Unique Identification Authority of India)

NOTIFICATION

New Delhi, the 9th May, 2025

F. No. A-19011/339/2024-UIDAI.—In pursuance of the Secretariat of the Appointments Committee of the Cabinet (ACC) communication no. 36/02/2025-EO (SM-I), dated 18.4.2025 conveying that ACC has approved appointment of Shri Bhuvnesh Kumar, IAS (UP:1995), Additional Secretary, Ministry of Electronics & Information Technology as Chief Executive Officer (CEO), Unique Identification Authority of India (UIDAI) in the rank and pay of Additional Secretary to the Government of India, and consequent upon his relieving from the Ministry of Electronics and Information Technology *vide* the Ministry's Office Order No. 4(1183)/2021-Pers.I, dated 30.4.2025, it is hereby notified that Shri Bhuvnesh Kumar, IAS (UP:1995) has assumed the office of Chief Executive Officer (CEO), UIDAI in the forenoon of 1st May, 2025.

VIVEK CHANDRA VERMA, Dy. Director General

INDEX

A-12025/I/2010-UIDAI
Unique Identification Authority of India
(Human Resource Division)
***

Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi – 110001
Dated: May 2025

Circular

Sub: Internship Policy, 2025

I am directed to forward the amended Internship Policy, 2025 as attached herewith for information and necessary action at your end.

This issues with the approval of the Competent Authority.

Encl: As Above

Signed by
Piyush Chand Gupta
Date: 15-05-2025 10:04:20

(Piyush Chand Gupta)
Director
Tel.: 011-23478554
e-Mail : dir.hr-hq@uidai.net.in

To:

1. All Deputy Director Generals, UIDAI.
2. All Director/Director (Tech), UIDAI.
3. UIDAI Website.
4. KM portal of e-office

INDEX

UNIQUE IDENTIFICATION AUTHORITY OF INDIA

Internship Scheme -2025

1. Purpose:

An internship is an opportunity for a student to secure first hand and practical work experience under the guidance of a qualified and experienced Mentor. It also aims at active participation in the learning process through experimentation and putting into practice the knowledge acquired in the classrooms. These "Interns" shall be given adequate exposure to various Technology tracks and other units within UIDAI Head Office, Technology Centre and Regional Offices and would be expected to work in the field of application development, legal domains (like cyber laws/IT act) & general management. For the "Interns" the exposure to the functioning of the UIDAI & the technologies applied shall be an add-on furthering their future career prospects in niche technology, legal domains, management and many other areas as the case may be.

2. About UIDAI:

2.1. The Unique Identification Authority of India (UIDAI) is a statutory authority established under the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act 2016") on 12 July 2016 by the Government of India, under the Ministry of Electronics and Information Technology (MeitY).

2.2. Under the Aadhaar Act 2016, UIDAI is responsible for Aadhaar enrolment and authentication, including operation and management of all stages of Aadhaar life cycle, developing the policy, procedure, and system for issuing Aadhaar numbers to individuals and perform authentication and the security of identity information and authentication records of individuals.

3. Objective:

3.1. To allow young academic talent to be associated with the UIDAI's work for mutual benefit.

3.2. The "Interns" shall have an opportunity to know about the UIDAI functioning. It will enable UIDAI to interact with young scholars and to get fresh ideas and study/research support from the field of academics. At the same time, it will provide an opportunity to young scholars to contribute in the UIDAI work and have an insight into the related technical domains, management fields or related legal aspects.

INDEX

3.3. Indian Citizens are eligible to apply under this policy. Bonafide students at any recognized University/ Institution within India or abroad, fulfilling prescribed conditions are eligible to apply for the internship.

4. Eligibility:

4.1. Students who have secured minimum 60% marks (GPA avg of 6.0/10) in all prior semester examinations; and

a. Graduate in Technical fields like B.Tech/ BE/ B.Design/ B.Graphic and other similar Technical Fields as considered appropriate by ROs/ Technology Centre/ FWs of UIDAI Head Office:
   i. Students studying in Final or Pre-final (3rd / 4th year) or
   ii. Students who have just completed graduation within last six months*;

or

b. Post Graduate in Technical Fields like M.Tech/ ME/ Master in Design/ Master in Information Design, Master in Computer Application and other similar Technical Fields as considered appropriate by ROs/ Technology Centre/ FWs of UIDAI Head Office:
   i. Students studying in Final or pre-final (1st year/ 2nd year) or
   ii. Students who have just completed post graduation within last six months*;

or

c. Graduate in Other Fields like Legal, Commerce, Accounts, Business Administration, Finance, Mass Communication, Mathematics, Statistics or any other field as considered appropriate by concerned RO, FW of HQ or TC:
   i. Students who have appeared in the final exam or
   ii. Students who have completed Graduation within last six months*;

or

d. Post Graduate in Other Fields like Legal, Commerce, Accounts, Business Administration, Finance, Mass Communication or any other field as considered appropriate by concerned RO, FW of HQ or TC:
   i. Students who have appeared in the final exam or who have completed Post Graduation within last six months* or
   ii. Appeared in the term-end exams of first year/ 2nd semester of their post graduate programme or

or

INDEX

e. Students pursuing PhD/ Research in Fields like Computer Science, IT Act and cyber laws related to Data Privacy, Cyber Security, Digital Economy, Block Chain, Quantum Computing, Computer Vision, Artificial Intelligence, Machine Learning, Big Data Analytic & Design, Cloud, Public Policy & Management or any other field as considered appropriate by concerned RO, FW of HQ or TC:

i. The student must be registered for PhD/ Research at a recognised Indian institution and

ii. Recommendation letter must be from the PhD/Research supervisor.

*The period between the month of declaration of result of final exam and the desired month of internship should not exceed six months e.g. if the result is declared in the month of June then he/she can apply for the internship beginning till the month of December only.

4.2. Period : The period of Internship shall be at least six weeks but not exceeding 12 months. Interns not completing the requisite period will not be issued any certificate.

5. Place Of Internship:

All the interns shall work either at the Technology Centre, Bengaluru or Regional Offices/ State Offices of UIDAI or UIDAI Head office.

6. Stipend:

The interns shall be paid monthly stipend subject to submission of satisfactory report from the supervisor (not below the rank of Director) only. The monthly stipend (In Rs.) to be paid to interns is as under:

Sl. No.	Subject	Technical	Other field
1	Graduate in Technical fields like B.Tech/ BE/ B.Design/ B.Graphic and other similar Technical Fields as considered appropriate by ROs/ Technology Centre/ FWs of UIDAI Head Office	30000	NA
	Post Graduate in Technical Fields like M.Tech/ ME/ Master in Design/ Master in Information Design, Master in Computer Application and other similar Technical Fields as considered appropriate by ROs/ Technology Centre/ FWs of UIDAI Head Office	40000	
2	MBA/PGDM	NA	40000

INDEX

3	Graduate in Other Fields like legal, commerce, accounts, business administration, finance, mass communication, mathematics, statistics or any other field as considered appropriate by concerned RO, FW of HQ or TC	NA	20000
4	Post Graduate in Other Fields like legal, commerce, accounts, business administration, finance, mass communication, mathematics, statistics or any other field as considered appropriate by concerned RO, FW of HQ or TC	NA	30000
4	PhD/ Research*	50000	40000

**Note:- PhD/ Research candidates, who may already be drawing a fellowship / financial benefit/ stipend, will be eligible for gap amount only.*

7. How To Apply:

i. Interested and eligible students need to apply online when it is notified or send CV along with supporting document through email for internship at the locations mentioned in Annexure-E.

ii. For applicant who is currently enrolled in a institute, the application needs to be sponsored/ forwarded by the Institution in the prescribed format.

iii. The selected candidates may be asked by the Regional Office/ HO Division/ TC to submit the soft copy of their NOC from their Head of the Department/ Principal by giving sufficient time before issuance of the offer letter by the vertical head. It also must be indicated in the NOC that the student would not be registered for any course requiring his/her attendance in the class during the period of internship. Tech Centre/ Regional office/ division must obtain the original NOC issued by the college/ institution at the time of joining of the candidate and also verify his/her eligibility from the original documents. If any discrepancy is found, the candidature will be cancelled by the UIDAI.

Note: Requirement of NOC/Sponsorship of the Institution shall not be required in case of pass out applicants.

8. Selection:

INDEX

The selection of the interns will be made by the concerned DDG of RO/ Tech Centre/ Division of Head Office. The concerned DDG may form a Selection Committee for the purpose of screening, selection and/or conduct personal or virtual interview, if considered necessary. No TA/DA shall be paid to applicants for attending the personal interview. The decision of the concerned DDG heading respective office (Tech Centre/ Regional office/ Division of Head Office) regarding the suitability of a candidate as intern shall be final and binding.

9. Number Of Interns:

The maximum number of interns that can be on-boarded for internship per calendar year shall be as under:

Each Division of Head Office	4
Each Regional office	5
Technology Centre	30
Each State office	2

10. Logistic Support:

10.1. The Intern has to make his/ her own accommodation arrangement during the internship in case of working from UIDAI premises. They shall arrange their own transport to and from office. However, basic lodging facilities can be made available on payment basis in UIDAI Technology Centre, only.

10.2. The Intern will not be given any Computer System/ Laptop etc for carrying out his/her assignments during the internship. The intern shall be required to bring his/her own Laptop for carrying out the works assigned to him/her. However, in certain cases considering the technical nature of task assigned to the intern, concerned DDG may provide desktop to work within UIDAI premises.

10.3. The intern may be given access to the office internet, which shall be at the sole discretion of the supervising officer and subject to compliance of Information Security policy of UIDAI.

11. Submission Of Report/ Paper:

11.1. The interns will be required to submit a project report on the work undertaken at the end of the internship to the UIDAI.

11.2. The interns must furnish a "No Demand Certificate" to UIDAI in the prescribed format after completion of project work along with soft copy and hard copy of the project report.

INDEX

12. **Experience Certificate:** The UIDAI will issue certificate for the period of internship in UIDAI at the end of the internship subject to completion of assigned work, duly recommended by the concerned reporting officer.

13. **Key Performance Indicators (KPIs)** : Performance of each intern pursuing internship for period more than four months in technical field, shall be evaluated on bi-monthly basis based on KPIs. KPIs shall be decided at the beginning of the tenure of internship wherein reporting/ supervising officer shall award ratings out of a score of 100.

14. **Code Of Conduct:**
    - 14.1. The interns shall be required to maintain confidentiality of all the documents/reports and or any information received by him/her during his/her internship period. The interns shall not reveal to any person or organisation any information relating to the Department, its work and policies.
    - 14.2. The interns may also be required to sign an undertaking as per the Annexure-I, prior to the commencement of the internship.
    - 14.3. The interns and the Sponsoring Institution concerned shall have no claim whatsoever on the results of the project work. The UIDAI retains all intellectual property rights, patents, designs, software copyright (source code) and publications, if any, that may be generated during the course of project work.
    - 14.4. However, interns may with the prior approval of UIDAI present their work to academic bodies and at seminars/ conferences. Even for this purpose, information that is confidential to the UIDAI cannot be revealed under any circumstances.
    - 14.5. The interns shall not engage with third parties such as potential vendors, experts, professionals, civil society groups and others without prior consent from project supervisor.
    - 14.6. Interns are not authorized to represent the UIDAI in public forums, conferences and meetings or to interact with the media (print or visual).

15. **Other Modalities & Termination of Internship:**
    - 15.1. All the interns will be given clearly outlined work so that they can complete it within the engagement period and contribute to UIDAI in a meaningful manner.
    - 15.2. The work of interns would be reviewed by their respective project supervisor in an institutional manner and due feedback/guidance will be provided.
    - 15.3. Any student who is found to be lacking or disinterested after on boarding, she/ he will be de-boarded with 15 days of notice.
    - 15.4. Interns will be explained about the UIDAI's security policy and has to sign a non-disclosure agreement.

16. **Scheme Review:**
    UIDAI reserves the right to review the Scheme at any time. The Scheme so reviewed will be placed on the website of UIDAI.

INDEX

17. Relaxation:

Notwithstanding anything contained above, the CEO, UIDAI have the power to relax any of the conditions in respect of any deserving candidate.

INDEX

Annexure-I

UNDERTAKING

a) I will follow the rules and regulations of the Authority that are in general applicable to employees of the authority.

b) I will follow the strict confidentiality protocol of the Authority and shall not reveal to any person or organization confidential information on the Authority, its work and its policies.

c) Any papers and documents written (if any) and / or published by me will carry the caveat that the view are the personal views of the intern and do not represent or reflect the view of the authority.

d) I will conduct myself professionally in my relationship with the Authority and the Public in general. I will enter into the "Non-Disclosure Agreement" with UIDAI on joining.

Place:

Date: Name & Signature of the Candidate:

INDEX

Annexure "A"

Proforma of Application for Internship in UIDAI

1. Registration No :
2. Name :
3. Father's Name :
4. Address for correspondence :
5. Contact Number :
6. E-mail :
7. Date of Birth :
8. Educational Qualification (Starting from 12th onward)

Sl No	Name of Board/University/Institute	Course details	Discipline	Year of Joining (month/year)	Pursuing/ Completed	Consolidated/ cumulative Percentage/ Grade/CGPA as on final/Last Semester/year attended
1						
2						
3						
4						

9. Place of Internship :
10. In case of Head Office, preferred functional wing (Kindly refer annexure-F)
11. Area of interest (please indicate courses taken/certification done which qualify you for the role)

12. Remarks (In brief not exceeding 50 words):

INDEX

I declare that the information given by me is true, correct and to the best of my knowledge and nothing has been concealed

Date: Name & Signature:

INDEX

Annexure "B"

FORMAT OF INTERNSHIP COMPLETION CERTIFICATE

(To be given on Letter Head)

Dated:

TO WHOMSOEVER IT MAY CONCERN

This is to certify that Mr/Ms._____a student of University/Institution_____ has successfully completed his/her Internship with _____(Name of office) Unique Identification Authority of India from_____to_____. During the period of Internship he/she worked under_____in the following areas.

(i)

(ii)

2. He/She has shown special flair for _____and his/her performance in preparation of the report has been rated as _____.

3. During the period of his/her internship programme he/she was punctual and hardworking.

4. I wish him/her every success in his/her life and career.

(Signature)

INDEX

'Annexure C'

(Applicable to students who are still pursuing their studies)

FORMAT FOR NOC TO BE OBTAINED FROM COLLEGE/INSTITUTION

(To be given on Letter Head)/ To be signed by HOD/Principal)

Dated:-

Subject: No Objection Certificate for UIDAI Internship Programme.

It is certified that Mr./Ms _____is a bonafide student College ID No._____ of Semester/Year of _____of this Institution/College.

The Institution/College has no objection for doing the Internship programme at UIDAI for the period from _____ to_____. It is also certified that he/she is not registered for any course requiring his/her attendance in the class during the said period.

The conduct of the student as recorded by the college/institution has been found good/satisfactory/unsatisfactory.

(Signature and Seal)

INDEX

Annexure-D

MUTUAL NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement ("**Agreement**") is entered on <.....> by and between

Name of RO/Tech Center /Division of Head office Address **of RO/Tech Center /Division of Head Office** Province/State/Country/Postal Code - Place of Incorporation – Referred as the Contractor/ Disclosing party	_____ "Intern of " Address _____ Province/State/Country/Postal Code _____ Place of Incorporation -_____ Referred as Receipt Party _____

WITNESSETH

(A) UIDAI, Tech Centre, Bengaluru shall undertake executing the said assignment with Shri_____. In connection with the abovesaid the Disclosing Party may disclose to the other certain confidential, technical and business information which the Disclosing Party desires the Recipient Party to treat as confidential.

(B) Shri _____ has been employed as an Intern by (Name and Address **of RO/Tech Centre /Division of Head Office.**)

NOW THEREFORE, in consideration of the mutual agreements and covenants hereinafter set forth, (**Name of office**) and Shri_____ hereby agree as follows.

INDEX

1. As used herein, "Confidential Information" shall mean any and all technical and non-technical information to be provided by either party ("the Disclosing Party") to the other ("the Recipient"), including but not limited to (a) intellectual property (b) trade secrets; (c) proprietary information related to the current, future, and proposed products and services of the Disclosing Party including, without limitation, mask works, ideas, samples, media, techniques, sketches, drawings, works of authorship, models, inventions, know-how, processes, apparatuses, equipment, algorithms, software programs, software source documents, and formulae, its information concerning research, experimental work, development, design details and specifications, engineering, financial information, procurement requirements, purchasing, manufacturing, customer lists, investors, employees, business and contractual relationships, business forecasts, sales and merchandising, marketing plans, information the Disclosing Party provides regarding third parties; and (d) such other information which by its nature or the circumstances of its disclosure is confidential. All Confidential Information provided by the Disclosing Party to the Recipient shall remain the sole and exclusive property of the Disclosing Party.

2. The Recipient agrees that at all times it shall: (a) only disclose the Confidential Information to Shri_____ who have written and binding non-disclosure obligations with disclosing party that are as restrictive as those herein and then only for the Purpose; (b) will hold in strict confidence and not disclose to any third party the Confidential Information, except as approved in writing by the Disclosing Party, and (c) will use the Confidential Information for no purpose other than evaluating or pursuing a business relationship with the Disclosing Party; (d) not reproduce Confidential Information in any form except for the Purpose; (e) not use the Confidential Information to make, have made or sell any products or services that compete with any of Disclosing Party's products or services and (f) not reverse engineer, decompile, or disassemble any Discloser Confidential Information.

3. The Recipient shall immediately notify the Disclosing Party, in writing, upon discovery of any threatened breach, actual loss, or unauthorised disclosure of the Confidential Information.

4. The Recipient's obligations under this Agreement with respect to any portion of the Confidential Information shall terminate when the Recipient can document that: (a) it was in the public domain at the time it was communicated to the Recipient by the Disclosing Party; (b) it entered the public domain subsequent to the time it was communicated to the Recipient by the Disclosing Party through no fault of the Recipient; (c) it was in the Recipient's possession free of any obligation of confidence at the time it was communicated to the Recipient by the Disclosing Party; (d) it was rightfully

INDEX

communicated to the Recipient free of any obligation of confidence by a third party subsequent to the time it was communicated to the Recipient by the Disclosing Party; (e) it was developed by employees or agents of the Recipient independently of and without reference to any Confidential Information communicated to the Recipient by the Disclosing Party; or (f) it is required to disclose pursuant to an order of a duly empowered government agency or a court of competent jurisdiction ,provided due notice and an adequate opportunity to intervene is given to the Disclosing Party ,unless such notice is prohibited by such order.

5. Upon written request of the Disclosing Party, the Recipient shall promptly return to the Disclosing Party all documents and other tangible materials representing the Confidential Information and all copies thereof, or certify the destruction thereof.

6. The Parties recognise and agree that nothing contained in this Agreement shall be construed as granting any property rights to the Recipient, by license or otherwise, to any Confidential Information of the Disclosing Party disclosed pursuant to this Agreement, or to any invention or any patent, copyright, trademark, or other intellectual property right in connection therewith. The Recipient shall not derive any profit from the use of the Confidential Information in an unauthorised manner to the exclusion of the Disclosing Party.

7. The Disclosing Party reserves all other rights in and to its Confidential Information. All confidential information is provided "As-Is" without any kind of warranty. Each party disclaims all warranties, whether express or implied, including any warranties of title, non-infringement, merchantability and fitness for a particular purpose.

8. The Confidential Information shall not be reproduced in any form except in accordance with the provisions of this Agreement. Any reproduction of any Confidential Information by the Recipient shall remain the property of the Disclosing Party and shall contain any and all confidential or proprietary notices or legends, which appear on the original, unless otherwise authorised in writing by the Disclosing Party.

9. The Recipient acknowledges that its breach of the Agreement may cause irreparable damage to the Disclosing Party and agrees that the Disclosing Party shall be entitled to seek injunctive relief under this Agreement, as well as such further relief as may be granted by a court of competent jurisdiction.

10. Notwithstanding anything to the contrary elsewhere herein and except with respect to claims based upon wilful, malicious or grossly negligent conduct of the liable party, neither party shall be liable for any incidental, indirect, special, exemplary, punitive or

INDEX

consequential damages, including but not limited to loss of revenue, income or profits, howsoever caused.

11. The Confidential Information may be subject to Disclosing Party's home country export control laws and regulations, and may be subject to export and import regulations in other countries, too. Recipient agrees that it will not export, re-export or transfer the Confidential Information, or any products developed with or utilizing the Confidential Information or any other product from a Party hereto, in violation of any such applicable laws or regulations of from where the Confidential Information was obtained.

12. The Agreement contains the final, complete and exclusive agreement of the Parties relative to the subject matter hereof and supersedes all prior and contemporaneous understandings and agreements relating to this subject matter and may not be changed, modified, amended or supplemented except by written instrument signed by both Parties. If any provision of this Agreement is found by a proper authority to be unenforceable or invalid, such provision shall be severed and the remainder of the Agreement will continue in full force and effect. The Recipient hereby acknowledges that no remedy at law will afford Discloser adequate protection against or appropriate compensation for breach of Recipient's obligations under this Agreement. The Recipient agrees that Discloser shall be entitled to seek specific performance of Recipient's obligations.

13. Neither Party will assign or transfer any rights or obligations under this Agreement without the prior written consent of the other Party.

14. This Agreement shall be governed by and construed in accordance with the laws of the India and the Parties hereby submit to the jurisdiction of the courts of _____.

15. This Agreement may not be amended except in writing by the Parties hereto.

16. Term: This Agreement shall continue in full force and effect for a term till completion of the contract from the Effective Date. The termination of this Agreement shall not relieve either Party of its obligations with respect to Confidential Information disclosed under this Agreement for a period of 4 (four) years from the Effective Date.

IN WITNESS WHEREOF, the Parties hereto have caused this Non Disclosure Agreement to be executed by their duly authorized officers or agents on the date first set out above.

INDEX

HQ-12058/1/2020-HR-HQ

I/44121/2025

By: UIDAI	By : Shri
Authorized Signature	Authorized Signature
Name and Title	Name and Title

INDEX

Annexure E

SL. No.	Location	Name and Address of Concerned Person
1.	UIDAI Regional Office, Bengaluru	Deputy Director (HR), UIDAI Regional Office, Bengaluru, Khanija Bhavan, No. 49, 3rd Floor, South Wing Race Course Road, Bengaluru - 560001
2.	UIDAI Regional Office, Chandigarh	Deputy Director (HR), UIDAI Regional Office, Chandigarh, SCO 95-98, Ground and Second Floor, Sector 17- B. Chandigarh 160017
3.	UIDAI Regional Office. Delhi	Deputy Director (HR), UIDAI Regional Office, Delhi, Ground Floor, Supreme Court Metro Station, Pragati Maidan, New Delhi-110001
4.	UIDAI Regional Office, Guwahati	Deputy Director (HR), UIDAI Regional Office, Guwahati, Block-V, First Floor, HOUSEFED Complex, Beltola-Basistha Road, Dispur, Guwahati-781 006
5.	UIDAI Regional Office, Hyderabad	Deputy Director (HR), UIDAI Regional Office, Hyderabad, 6th Floor, East Block, Swarna Jayanthi Complex, Beside Maitrivanam, Ameerpet Hyderabad-500 038, Telangana State
6.	UIDAI Regional Office, Lucknow	Deputy Director (HR), UIDAI Regional Office, Lucknow, 3rd Floor, Uttar Pradesh Samaj Kalyan Nirman Nigam Building, TC-46/ V, Vibhuti Khand, Gomti Nagar, Lucknow-226 010
7.	UIDAI Regional Office, Ranchi	Deputy Director (HR), UIDAI Regional Office, Ranchi, 1st Floor, JIADA Central Office Building, Namkum Industrial Area, Near STPI Lowadih, Ranchi-834010
8.	UIDAI Regional Office, Mumbai	Deputy Director (HR), UIDAI Regional Office, Mumbai, 7th Floor, MTNL Exchange, GD Somani Marg, Cuff Parade, Colaba, Mumbai-400 005
9.	State office, Patna (Bihar)	4th Floor, Lalit Bhawan Bailey Road, Jawaharlal Nehru Marg, Patna, Bihar-800001
10.	State Office (West Bengal)	Ground Floor, Telephone Bhawan, 34, BBD Bag (South), Dalhousie, Kolkata. Pin:700001
11.	State Office Bhopal (Madhya Pradesh)	UIDAI State Bhopal, Ground Floor, BSNL Bhawan, Near Paryawas Bhawan, Arera Hills, Bhopal- 462026, Madhya Pradesh
12.	UIDAI State Office	UIDAI State Office Bhubaneswar, 3rd Floor, OCAC

INDEX

HQ-12058/1/2020-HR-HQ I/44121/2025

SL. No.	Location	Name and Address of Concerned Person
	(Odisha)	Tower, Acharya Vihar, RRL Post Office, Bhubaneswar, Khordha, Odisha, PIN: 751013
13.	State office Ahmedabad (Gujarat)	UIDAI Gujarat State Office, 4th Floor, Telephone Bhawan, 23, Chimanlal Girdharlal Rd, Sardar Patel Nagar, Ellisbridge, Ahmedabad, Gujarat 382435
14.	State Office Thiruvananthapuram (Kerala)	UIDAI State Office Doorsanchar Bhavan PMG Junction Thiruvananthapuram - 695033, Kerala.
15.	UIDAI Technology Centre.	Deputy Director (HR), UIDAI Technology Centre, Benagalu Aadhaar Complex, NTI Layout, Tata Nagar, Kodigeha Bengaluru-560092
16.	UIDAI Head Office	Deputy Director [Division Name (any one of the Functional Wing of UIDAI HQ as given in Annexure F] , Unique Identification Authority Of India, Bangla Sahib Road, Behind Kali Mandir, Gole Market, New Delhi-110001

INDEX

Annexure F

i. Enrolment & Update Division
ii. Aadhaar Usage Division
iii. Authentication and Verification Division
iv. Media Division
v. Information Security Division
vi. Technology Management Division
vii. Finance & Accounts Division
viii. Customer Relationship Management & Logistics and Channel Interface Division
ix. Training, Testing and Certification Division
x. Human Resource Division.
xi. Administration Division
xii. Legal Division.
xiii. Co-ordination Division.

INDEX

सत्यमेव जयते

आधार
मेरा आधार, मेरी पहचान

भुवनेश कुमार, भा.प्र.से.
मुख्य कार्यकारी अधिकारी, भा.वि.प.प्रा.

संदेश

'हिंदी दिवस' के अवसर पर भारतीय विशिष्ट पहचान प्राधिकरण के सभी अधिकारियों और कर्मचारियों को मेरी हार्दिक शुभकामनाएं।

भाषा किसी भी राष्ट्र की सामाजिक और सांस्कृतिक धरोहर की संवाहक होती है। हिंदी भारत के जन-मन की अभिव्यक्ति के संप्रेषण की और देश में सबसे ज्यादा बोली एवं समझी जाने वाली भाषा है। संपर्क भाषा के रूप में स्वाधीनता के पूर्व ही अपनी विशेष पहचान बना चुकी हिंदी के महत्व को ध्यान में रखते हुए, संविधान सभा ने 14 सितंबर, 1949 को, हिंदी को भारत संघ की राजभाषा के रूप में अंगीकार किया था। तभी से प्रतिवर्ष 14 सितंबर को 'हिंदी दिवस' के रूप में मनाने की परंपरा है।

भारत में विभिन्न स्थानों पर स्थित प्राधिकरण के प्रधान कार्यालय सहित सभी कार्यालयों एवं केंद्रों आदि में अलग-अलग प्रांतों, धर्मों, बोलियों और समुदायों से संबंध रखने वाले लोग कार्यरत हैं। ऐसे में हिंदी इन सबके बीच में संपर्क भाषा के तौर पर मुख्य कड़ी का काम करती है। आज हिंदी भारत में ही नहीं अपितु पूरे विश्व में अपना परचम लहरा रही है। विश्व के लगभग 150 से अधिक देशों में किसी न किसी रूप में हिंदी का प्रयोग होता है और 200 से अधिक विश्वविद्यालयों में इसका अध्ययन और अध्यापन भी हो रहा है।

हिंदी की भांति ही आज 'आधार' भी विभिन्न सरकारी तंत्रों और भारत के जनमानस से जुड़ा है। भारत जैसे बड़े एवं बहुभाषा वाले राष्ट्र में 'आधार' को सफलतापूर्वक लागू किए जाने के फलस्वरूप अब अन्य देश भी इस परियोजना का अनुकरण करने को आतुर हैं। यह हमारे लिए गौरव का विषय है। चहुमुंखी उत्तरदायित्वों के साथ-साथ प्राधिकरण में भारत संघ की राजभाषा नीतियों, आदेशों और दिशानिर्देशों को लागू किया जा रहा है। वेबसाइट सहित प्राधिकरण द्वारा विकसित ऐप एम-आधार, रेज़िडेंट पोर्टल, चैटबोट-आधार मित्र, क्यूआर स्कैनर, वेबमेल, ई-आफिस और सोशल मीडिया पर भी हिंदी का प्रयोग किया जा रहा है।

हिंदी दिवस के अवसर पर भारतीय विशिष्ट पहचान प्राधिकरण के सभी कार्यालय हिंदी पखवाड़े एवं विभिन्न कार्यक्रमों का आयोजन कर रहे हैं। मुझे विश्वास है कि प्राधिकरण के अधिकारी और कार्मिक न केवल इस दौरान आयोजित गतिविधियों में भागीदारी करके कार्यक्रमों को सफल बनाएंगे बल्कि हिंदी में कामकाज करने के लिए अपने साथियों को भी प्रोत्साहित एवं प्रेरित करते रहेंगे।

हिंदी दिवस के अवसर पर आप सभी को पुन: मेरी हार्दिक शुभकामनाएं।

भुवनेश

(भुवनेश कुमार)
मुख्य कार्यकारी अधिकारी

नई दिल्ली
14 सितंबर, 2025

INDEX

रजिस्ट्री सं. डी.एल.-33004/99 REGD. No. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-18102025-267023
CG-DL-E-18102025-267023

असाधारण
EXTRAORDINARY
भाग III—खण्ड 4
PART III—Section 4
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 684] नई दिल्ली, शुक्रवार, अक्तूबर 17, 2025/आश्विन 25, 1947
No. 684] NEW DELHI, FRIDAY, OCTOBER 17, 2025/ASVINA 25, 1947

भारतीय विशिष्ट पहचान प्राधिकरण

अधिसूचना

नई दिल्ली, 17 अक्तूबर, 2025

फा. सं. ए-12013/13/आरआर/2016-यूआईडीएआई (ई).—आधार (वित्तीय एवं अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्ष्यित परिदान) अधिनियम, 2016 (2016 का 18) की धारा 54 की उप-धारा (1) में प्रदत्त शक्तियों का प्रयोग करते हुए, भारतीय विशिष्ट पहचान प्राधिकरण एतद्द्वारा भारतीय विशिष्ट पहचान प्राधिकरण (अधिकारियों और कर्मचारियों की नियुक्ति) विनियम, 2020 को और संशोधित करने के लिए निम्नलिखित विनियम बनाता है, नामतः —

1. **संक्षिप्त नाम और प्रारंभ.**—(1) इन विनियमों को भारतीय विशिष्ट पहचान प्राधिकरण (अधिकारियों और कर्मचारियों की नियुक्ति) तृतीय संशोधन विनियम, 2025 कहा जाएगा।

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

2. भारतीय विशिष्ट पहचान प्राधिकरण (अधिकारियों और कर्मचारियों की नियुक्ति) विनियम, 2020, अनुसूची में,—

(1) "वरिष्ठ लेखा अधिकारी" पद के लिए, 'श्रेणी जिससे प्रोन्नति/प्रतिनियुक्ति की जानी है,' के कॉलम में, प्रतिनियुक्ति के अंतर्गत, "चार्टर्ड लेखाकार/लागत लेखाकार/व्यवसाय प्रशासन स्नातकोत्तर (वित्त) की व्यावसायिक अर्हताएं" की अंतर्वस्तु को "अर्हताएं: चार्टर्ड लेखाकार/लागत लेखाकार/ व्यवसाय प्रशासन स्नातकोत्तर (वित्त) /वाणिज्य स्नातकोत्तर से प्रतिस्थापित किया जाएगा।

INDEX

(2) "वरिष्ठ लेखा अधिकारी" पद के लिए, 'श्रेणी जिससे प्रोन्नति/प्रतिनियुक्ति की जानी है,' के कॉलम में, प्रतिनियुक्ति के अंतर्गत, अंतर्वस्तु में निम्नलिखित "आईएसटीएम द्वारा आयोजित रोकड़ एवं लेखा कार्य प्रशिक्षण सफलतापूर्वक पूरा किया हो या **लेखा संबंधी कार्य को संभालने में 'सात साल के अनुभव के साथ वाणिज्य में स्नातक"** को शामिल किया जाएगा।

(3) "निजी सचिव" पद के लिए, 'पदों की संख्या' कॉलम में, **"25"** अंकों के लिए, **"22"** अंकों को प्रतिस्थापित किया जाएगा।

(4) "अनुभाग अधिकारी" पद के लिए, 'पदों की संख्या' कॉलम में, **"74"** अंकों के लिए, **"75"** अंकों को प्रतिस्थापित किया जाएगा।

(5) "सहायक लेखा अधिकारी" पद के लिए, 'पदों की संख्या' कॉलम में, **"10"** अंकों के लिए, **"12"** अंकों को प्रतिस्थापित किया जाएगा।

पीयूष चंद गुप्ता, उपमहानिदेशक

[विज्ञापन-III/4/असा./418/2025-26]

नोट : मूल विनियमों को भारत का राजपत्र, असाधारण, भाग-III, खंड 4 में अधिसूचना संख्या ए-12013/13/आरआर/2016-यूआईडीएआई (2020 की संख्या 1) दिनांक 21 जनवरी, 2020 के द्वारा प्रकाशित किया गया था और उसे अंतिम बार अधिसूचना संख्या ए-12013/13/आरआर/2016-यूआईडीएआई (ई), दिनांक 24 मार्च, 2025 के द्वारा संशोधित किया गया था।

UNIQUE IDENTIFICATION AUTHORITY OF INDIA

NOTIFICATION

New Delhi, the 17th October, 2025

F. No. A-12013/13/RR/2016-UIDAI (E).— In exercise of the powers conferred by sub-section (1) of section 54 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), the Unique Identification Authority of India hereby makes the following regulations to further amend the Unique Identification Authority of India (Appointment of Officers and Employees) Regulations, 2020, namely:—

1. Short title and commencement. —(1) These regulations may be called the Unique Identification Authority of India (Appointment of Officers and Employees) Third Amendment Regulations, 2025.

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

2. In the Unique Identification Authority of India (Appointment of Officers and Employees) Regulations, 2020, in the Schedule—

(a) For the post "Senior Accounts Officer", under deputation, in column 'Grade from which promotion/ deputation is to be made', the contents "Professional qualifications of Chartered Accountant/ Cost Accountant/MBA (Finance)" shall be substituted with "Qualification: Chartered Accountant/Cost Accountant/ MBA (Finance)/ **M. Com**".

(b) For the post "Senior Accounts Officer", under deputation, in column 'Grade from which promotion/ deputation is to be made', following shall be added below the contents "Having successfully completed Cash & Accounts Training organized by ISTM"

***"Or,* Graduation in Commerce with Seven years' experience in handling accounts related work."**

(c) For the post "Private Secretary", in column 'Number of post', for the figures "**25**", the figures, **"22"** shall be substituted.

(d) For the post "Section Officer", in column 'Number of post', for the figures "**74**", the figures, **"75"** shall be substituted.

INDEX

(c) For the post "Assistant Account Officer", in column 'Number of post', for the figures "10", the figures, "12" shall be substituted.

PIYUSH CHAND GUPTA, Dy. Director General

[ADVT.-III/4/Exty./418/2025-26]

Note: The principal regulations were published in the Gazette of India, Extraordinary, Part III, Section 4, vide notification number A-12013/13/RR/2016-UIDAI (No. 1 of 2020), dated the 21st January 2020 and last amended vide notification number A-12013/ 13/RR/2016-UIDAI (E), dated 24th March, 2025.

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.

INDEX

D
AADHAAR USAGE

रजिस्ट्री सं. डी.एल.- 33004/99 REGD. No. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-09122025-268361
CG-DL-E-09122025-268361

असाधारण
EXTRAORDINARY

भाग III—खण्ड 4
PART III—Section 4

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 798] नई दिल्ली, मंगलवार, दिसम्बर 9, 2025/अग्रहायण 18, 1947
No. 798] NEW DELHI, TUESDAY, DECEMBER 9, 2025/AGRAHAYANA 18, 1947

भारतीय विशिष्ट पहचान प्राधिकरण

अधिसूचना

नई दिल्ली, 9 दिसम्बर, 2025

फा. सं. एचक्यू-30011/5/2025-एयू-एचक्यो.— आधार (वित्तीय और अन्य सहायिकियों, प्रसुविधाओं और सेवाओं का लक्षित परिदान) अधिनियम, 2016 (2016 का 18) की धारा 54 की उप-धारा (1) और (2) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, भारतीय विशिष्ट पहचान प्राधिकरण एतद्वारा आधार (अधिप्रमाणन और ऑफलाइन सत्यापन) विनियम, 2021 को और संशोधित करने के लिए निम्नलिखित विनियम बनाता है, नामतः—

1. **संक्षिप्त नाम और प्रारंभ.**—(1) इन विनियमों को आधार (अधिप्रमाणन और ऑफलाइन सत्यापन) संशोधन विनियम, 2025 कहा जाएगा।

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

2. आधार (अधिप्रमाणन और ऑफलाइन सत्यापन) विनियम, 2021 (जिन्हें इसमें इसके पश्चात मूल विनियम कहा गया है) में, विनियम 2 में, उप-विनियम (1) में,—

(क) निम्नलिखित खंड (कग) को अंतःस्थापित किया जाएगा, नामतः :—

INDEX

(कग) "आधार एप्लिकेशन" से तात्पर्य प्राधिकरण द्वारा विकसित और प्रबंधित किसी भी आधिकारिक मोबाइल एप्लिकेशन या वेब एप्लिकेशन से है, जो आधार नंबर धारकों को ऑफ़लाइन सत्यापन करने सहित आधार से संबंधित सेवाओं के लिए एक इंटरफेस प्रदान करती है और इसमें 'एमआधार ऐप', 'आधार ऐप', 'आधार क्यूआर स्कैनर ऐप', 'माईआधार पोर्टल' और ऐसे अन्य एप्लिकेशन शामिल हैं, जिन्हें समय-समय पर प्राधिकरण द्वारा अधिसूचित किया जाता है;'

(ख) निम्नलिखित खंड (खङ) को अंतःस्थापित किया जाएगा, नामतः :—

'(खङ) "आधार सत्यापन योग्य क्रेडेंशियल" से तात्पर्य प्राधिकरण द्वारा आधार नंबर धारक को जारी डिजिटल रूप से हस्ताक्षरित एक दस्तावेज से है जिसमें आधार नंबर के अंतिम 4 अंक, जनसांख्यिकीय डेटा, जैसे, नाम, पता, लिंग, जन्मतिथि और आधार नंबर धारक की फोटो, तथा प्राधिकरण द्वारा यथा विनिर्दिष्ट ऐसी अन्य जानकारी जिसे जनसांख्यिकीय जानकारी या फोटो सत्यापन के लिए प्राधिकरण द्वारा विनिर्दिष्ट तरीके से आधार नंबर धारक द्वारा ऑफलाइन सत्यापन मांगकर्ता संस्था (ओवीएसई) को पूर्ण रूप से या आंशिक रूप से साझा किया जा सकता है;'

(ग) खंड (ढक) का लोप किया जाएगा।

(घ) निम्नलिखित खंड (णघ) को अंतःस्थापित किया जाएगा, नामतः :—

'(णघ)' "ऑफ़लाइन चेहरा सत्यापन" से तात्पर्य ऑफ़लाइन सत्यापन की ऐसी विधि से है जिसमें आधार नंबर धारक के सजीव चेहरे की छवि को कैप्चर किया जाता है और उसकी शुद्धता या त्रुटि कोआधार नंबर धारक के आधार ऐप्लिकेशन के साथ संग्रहीत आधार नंबर धारक की छवि से सत्यापित किया जाता है;'

3. मूल विनियमों में, विनियम 3क के लिए, निम्नलिखित विनियम प्रतिस्थापित किया जाएगा, नामतः :—

"3क. ऑफलाइन सत्यापन के प्रकार.—(1) प्राधिकरण द्वारा निम्नलिखित प्रकार की ऑफलाइन सत्यापन सेवाएं प्रदान की जाएंगी, नामतः :—

(i) क्यूआर कोड सत्यापन,

(ii) आधार कागज रहित ऑफलाइन ई-केवाईसी सत्यापन,

(ii)(क) आधार सत्यापन योग्य क्रेडेंशियल का सत्यापन,

(iii) ई-आधार सत्यापन,

(iv) ऑफलाइन कागज आधारित सत्यापन, और

(v) प्राधिकरण द्वारा समय-समय पर लागू किसी भी अन्य प्रकार का ऑफलाइन सत्यापन।

उपर्युक्त ऑफलाइन सत्यापन किसी संस्था द्वारा समय-समय पर प्राधिकरण द्वारा दिए गए विनिर्देशों के अनुसार ऑफलाइन सत्यापन चेहरे के साथ या चेहरे के बिना किया जा सकता है।

(2) प्राधिकरण क्यूआर कोड को स्कैन करने और क्यूआर कोड या ई-आधार या आधार कागजरहित ऑफ़लाइन ई-केवाईसी या आधार सत्यापन योग्य क्रेडेंशियल को आधार एप्लिकेशन या अन्य माध्यमों से डाउनलोड करने के लिए विभिन्न साधन उपलब्ध कराएगा।"

4. मूल विनियमों में, अध्याय-III के शीर्षक को प्रतिस्थापित किया जाएगा, नामतः :—

INDEX

"अनुरोधकर्ता संस्थाओं तथा अधिप्रमाणन सेवा एजेंसियों की नियुक्ति एवं ऑफलाइन सत्यापन चाहने वाली संस्थाओं का पंजीकरण"

5. मूल विनियमों में, निम्नलिखित खंड 13क को अंत:स्थापित किया जाएगा, नामत: :—

"13क. ओवीएसई का पंजीकरण.- (1) आधार कागजरहित ऑफलाइन ई-केवाईसी सत्यापन या आधार ऐप्लिकेशन के जरिए आधार सत्यापन योग्य क्रेडेंशियल सत्यापन कराने की इच्छुक संस्था को पंजीकरण के लिए प्राधिकरण को ऐसे प्रपत्र में आवेदन करना होगा जिसे प्राधिकरण ऐसी संस्था के अनुरोध पर और ऐसे नियमों एवं शर्तों पर उपलब्ध करा सकता है जिन्हें प्राधिकरण द्वारा समय-समय पर निर्दिष्ट किया जा सकता है:

बशर्ते कि ऐसी संस्था ओवीएसई के रूप में पंजीकृत होने पर केवल वैध प्रयोजनों के लिए ऑफलाइन सत्यापन करेगी।

(2) प्राधिकरण, आवेदक से ऐसी कोई और जानकारी या स्पष्टीकरण मांग सकता है, जिसे प्राधिकरण आवेदन पर विचार करने और उसका निपटान करने के लिए आवश्यक समझे।

(3) प्राधिकरण आवेदन पर निर्णय लेने से पूर्व आवेदक द्वारा प्रस्तुत सूचना का सत्यापन कर सकता है।

(4) प्राधिकरण को, यदि यह विश्वास हो जाता है कि संस्था, प्राधिकरण द्वारा विनिर्दिष्ट नियमों और शर्तों के अनुसार पात्र है, तो वह आवेदन को अनुमोदित कर सकता है और संस्था को ओवीएसई के रूप में पंजीकृत कर सकता है।

(5) ओवीएसई के रूप में पंजीकरण हेतु किसी आवेदन के प्राधिकरण द्वारा विनिर्दिष्ट नियम व शर्तें पूर्ण न करने की स्थिति में, प्राधिकरण आवेदन को अस्वीकृत कर सकता है।

(6) आवेदन को प्राधिकरण द्वारा अस्वीकृत करने के निर्णय की सूचना, आवेदक को ऐसे निर्णय की तिथि से पंद्रह दिन के भीतर दी जाएगी, जिसमें उसके आवेदन को निरस्त करने के कारणों का उल्लेख किया जाएगा।

(7) प्राधिकरण के निर्णय से असंतुष्ट कोई भी आवेदक ऐसी सूचना प्राप्त होने की तिथि से तीस दिन की अवधि के अंदर निर्णय पर पुनर्विचार के लिए प्राधिकरण को आवेदन कर सकता है।

(8) आवेदक द्वारा किए गए ऐसे आवेदन पर प्राधिकरण पुनर्विचार करेगा और उस पर अपने निर्णय से आवेदक को यथाशीघ्र सूचित करेगा।

(9) प्राधिकरण समय-समय पर पंजीकरण और ऑफ़लाइन सत्यापन संव्यवहार के लिए ओवीएसई द्वारा देय शुल्क और प्रभार को निर्धारित कर सकता है।"

6. मूल विनियमों में, विनियम 16ख में, उप-विनियम (2) में, शब्द **"(एक्सएमएल) या एम-आधार"** का लोप किया जाएगा।

7. मूल विनियमों में, विनियम 16ग में, उप-विनियम (1) में, **"एम-आधार या"** और **"(एक्सएमएल)"** का लोप किया जाएगा।

8. मूल विनियमों में, निम्नलिखित खंड 23क को अंत:स्थापित किया जाएगा, नामत: :—

"23क. ऑफलाइन सत्यापन चाहने वाली संस्था (ओवीएसई) द्वारा ऑफलाइन सत्यापन सुविधा का ऐक्सेस सरेंडर करना. – (1) इन विनियमों के तहत पंजीकृत कोई ओवीएसई, जो प्राधिकरण द्वारा प्रदत्त ऑफलाइन सत्यापन सुविधा के ऐक्सेस को सरेंडर करने की इच्छुक है, प्राधिकरण को ऐसे सरेंडर के लिए अनुरोध कर सकती है।

(2) इन विनियमों के अंतर्गत ऐसे सरेंडर अनुरोध का निपटान करने के दौरान, प्राधिकरण ओवीएसई से यह अपेक्षा करता है कि वह सेवाओं को सुचारू रूप से बंद करने या समाप्त करने के लिए आवश्यक किसी भी मामले के बारे में प्राधिकरण को संतुष्ट करे, जिसमें निम्नलिखित शामिल हैं–

(क) इन विनियमों और प्रक्रियाओं के अनुसार सत्यापन लॉग और अन्य दस्तावेजों के रखरखाव और परिरक्षण के लिए ओवीएसई द्वारा की गई व्यवस्थाएं, जो इस प्रयोजनार्थ प्राधिकरण द्वारा विनिर्दिष्ट की जाएं;

INDEX

(ख) ऐसे अनुरोध पर संबंधित आधार नंबर धारक को सत्यापन रिकार्ड उपलब्ध कराने के लिए ओवीएसई द्वारा की गई व्यवस्था;

(ग) शिकायत निवारण अभिलेख, यदि कोई हो; और

(घ) प्राधिकरण के साथ खातों का निपटान, यदि कोई हो।"

9. मूल विनियमों में, विनियम 24 में, उप-विनियम (1), शब्द **"या ई-केवाईसी सेवा एजेंसी (केएसए)"** का लोप किया जाएगा।

10. मूल विनियमों में, विनियम 25(1क) के लिए, निम्नलिखित विनियम को प्रतिस्थापित किया जाएगा, नामतः :—

"(1क). जहां कोई ऑफलाइन सत्यापन चाहने वाली संस्था,

(क) प्राधिकरण द्वारा समय-समय पर जारी प्रक्रिया, क्रियाविधि, मानकों, विनिर्देशनों या निर्देशों के अनुपालन में असफल होती है; अधिनियम और इन विनियमों के अधीन दायित्वों के उल्लंघन में पायी जाती है;

(ख) विधिपूर्ण प्रयोजनों के अन्यत्र आधार ऑफलाइन सत्यापन सुविधा का उपयोग करती है;

(ग) इन विनियमों के अंतर्गत प्राधिकरण द्वारा अपेक्षित सूचना को उपलब्ध कराने में असफल रहती है, या

(घ) प्राधिकरण द्वारा कराए गए किसी निरीक्षण या जांच या पूछताछ या लेखापरीक्षा में सहयोग देने में असफल रहती है, प्राधिकरण, अधिनियम के अंतर्गत की जाने वाली अन्य कार्रवाई पर प्रभाव डाले बिना और आपराधिक कार्रवाई सहित, अधिनियम, नियमों और विनियमों के उपबंधों का उल्लंघन करने के लिए ऑफलाइन सत्यापन चाहने वाली संस्था पर दंड अधिरोपित करने के लिए ऐसी कार्रवाई कर सकता है, जिसे प्राधिकरण उचित समझे:

बशर्ते कि कार्रवाई करने से पूर्व संस्था या एजेंसी को सुनवाई का अवसर प्रदान किया जाएगा।"

11. मूल विनियमों में, विनियम 25(2) के लिए, निम्नलिखित उप-विनियम को प्रतिस्थापित किया जाएगा, नामतः :—

"(2) उप-विनियम (1) और (1क) में संदर्भित ऐसी कोई भी कार्रवाई किसी भी संस्था या सब-एयूए या सब-केयूए या ओवीएसई के विरुद्ध भी की जा सकती है।"

12. मूल विनियमों में, विनियम 25(3) के लिए, निम्नलिखित उप-विनियम को प्रतिस्थापित किया जाएगा, नामतः :—

"(3) प्राधिकरण द्वारा नियुक्ति या पंजीकरण की समाप्ति पर, अनुरोधकर्ता संस्था या एएसए या ओवीएसई तुरंत किसी भी उद्देश्य के लिए और किसी भी रूप में आधार के नाम और लोगो का उपयोग करना बंद कर देगी और उसे बंद करने के आवश्यक पहलुओं, जिनमें विनियमन 23(2) और 23ए(2) में वर्णित पहलू भी शामिल हैं, के बारे में प्राधिकरण को भरोसा दिलाना होगा।"

चिराग पंवार, निदेशक

[विज्ञापन-III/4/असा./534/2025-26]

टिप्पणीः मूल विनियम को दिनांक 8 नवंबर, 2021 की अधिसूचना फा. सं. के-11020/240/2021/अधि./ यूआईडीएआई (2021 की संख्या 2) के तहत भारत के राजपत्र, असाधारण, भाग III, खंड 4, में दिनांक 9 नवंबर, 2021 को प्रकाशित किया गया था और उसे तत्पश्चात निम्नलिखित अधिसूचनाओं के तहत संशोधित किया गया—

(i) फा.सं. के-11020/240/2021/अधि./यूआईडीएआई (2022 का सं. 01) दिनांक 04 फरवरी, 2022;

(ii) फा.सं. एचक्यू-13011/2/2021-अधि-II (2023 का सं. 01) दिनांक 24 फरवरी, 2023 (27 फरवरी, 2023 को प्रकाशित)

INDEX

(iii) फा.सं. एचक्यू-13073/1/2020-अधि.II(ई) दिनांक 29 सितंबर, 2023 (03 अक्तूबर, 2023 को प्रकाशित); और

(iv) फा.सं. एचक्यू-13073/1/2020-अधि.II(ई) दिनांक 31 जनवरी, 2024

UNIQUE IDENTIFICATION AUTHORITY OF INDIA

NOTIFICATION

New Delhi, the 9th December, 2025

F. No. HQ-30011/5/2025-AU-HO.—In exercise of the powers conferred by sub-sections (1) and (2) of section 54, of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), the Unique Identification Authority of India hereby makes the following regulations to further amend the Aadhaar (Authentication and Offline Verification) Regulations, 2021 namely: —

1. Short title and commencement. — (1) These regulations may be called the Aadhaar (Authentication and Offline Verification) Amendment Regulations, 2025.

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

2. In the Aadhaar (Authentication and Offline Verification) Regulations, 2021 (hereinafter referred to as the principal regulations), in regulation 2, in sub-regulation (1), —

(a) the following clause (ac) shall be inserted, namely:—

'(ac) "Aadhaar Application" means any official mobile application or web application developed and managed by the Authority to provide an interface to Aadhaar number holders for services related to Aadhaar, including performing offline verification, and includes 'mAadhaar App', 'Aadhaar App', 'Aadhaar QR Scanner App', 'myAadhaar Portal', and such other applications as may be notified by the Authority from time to time;'

(b) the following clause (be) shall be inserted, namely:—

'(be) "Aadhaar Verifiable Credential" means a digitally signed document issued by the Authority to the Aadhaar number holder which may contain last 4 digits of Aadhaar number, demographic data, like, name, address, gender, date of birth, and photograph of Aadhaar number holder, and such other information as may be specified by the Authority, which may be shared by Aadhaar number holder in full or part with an OVSE in the manner specified by the Authority, for verifying the demographic information or photograph of the Aadhaar number holder;'

(c) clause (la) shall be deleted.

(d) the following clause (md) shall be inserted, namely:—

'(md) "Offline Face Verification" means a mode of offline verification in which the live facial image of an Aadhaar number holder is captured and is verified against the photograph of the Aadhaar number holder stored within the Aadhaar application of the Aadhaar number holder for the correctness, or lack thereof;'

3. In the principal regulations, for regulation 3A, the following regulation shall be substituted, namely:—

"**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,

(ii)(a) Aadhaar Verifiable Credential 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 with or without offline face verification as per the specifications given by the Authority from time to time.

INDEX

(2) The Authority shall provide various means to scan QR code and download QR Code or e-Aadhaar or Aadhaar Paperless Offline e-KYC or Aadhaar Verifiable Credential through Aadhaar application or other means."

4. In the principal regulations, the title of the Chapter III shall be substituted, namely:—

"**APPOINTMENT OF REQUESTING ENTITIES AND AUTHENTICATION SERVICE AGENCIES AND REGISTRATION OF OFFLINE VERIFICATION SEEKING ENTITY**"

5. In the principal regulations, the following clause 13A shall be inserted, namely:—

"**13A. Registration of OVSE.**- (1) An entity desirous of undertaking Aadhaar Paperless Offline e-KYC verification or Aadhaar Verifiable Credential verification through Aadhaar Application shall apply to the Authority for registration, in such form as the Authority may provide upon request made to it by such entity and on such terms and conditions as may be specified by the Authority from time to time:

Provided that such entity on being registered as OVSE shall perform offline verification only for lawful purposes.

(2) The Authority may require the applicant to furnish further information or clarification which may be considered necessary by the Authority, to consider and dispose of the application.

(3) The Authority may verify the information submitted by the applicant before deciding the application.

(4) The Authority may, if it is satisfied that the entity is eligible as per the terms and conditions specified by the Authority, may approve the application and register the entity as OVSE.

(5) In the event an application for registration as OVSE does not satisfy the terms and conditions specified by the Authority, the Authority may reject the application.

(6) The decision of the Authority to reject the application shall be communicated to applicant within fifteen days of such decision, stating therein the grounds on which the application has been rejected.

(7) 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 information for reconsideration of the decision.

(8) The Authority shall reconsider such application made by the applicant and communicate its decision thereon, as soon as possible.

(9) The Authority, may from time to time, determine the fee and charges payable by an OVSE for registration and offline verification transactions."

6. In the principal regulations, in regulation 16B, sub-regulation (2), the words "**(XML) or m-Aadhaar**" shall be deleted.

7. In the principal regulations, in regulation 16C, sub-regulation (1), the words "**m-Aadhaar or**" and "**(XML)**" shall be deleted.

8. In the principal regulations, the following clause 23A shall be inserted, namely :—

"**23A. Surrender of the access to offline verification facility by OVSE.** – (1) An OVSE registered under these regulations, desirous of surrendering the access to the offline verification 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 OVSE to satisfy the Authority about any matter necessary for smooth discontinuance or termination of services, including -

(a) the arrangements made by the OVSE for maintenance and preservation of verification 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 OVSE for making verification record available to the respective Aadhaar number holder on such request;

(c) records of redressal of grievances, if any; and

(d) settlement of accounts with the Authority, if any."

9. In the principal regulations, in regulation 24, sub-regulation (1), the words "**or e-KYC Service Agency (KSA)**" shall be deleted.

INDEX

10. In the principal regulations, for regulation 25(1A), the following regulation shall be substituted, namely:—

"(1A). Where any Offline Verification Seeking Entity,

(a) fails to comply with any of the processes, procedures, standards, specifications or directions issued by the Authority, from time to time; is in breach of its obligations under the Act and these regulations;

(b) uses the Aadhaar Offline Verification facilities for other than lawful purposes;

(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, the Authority may, without prejudice to any other action which may be taken under the Act, including such criminal action as it may deem fit, take such steps to impose penalty on the Offline Verification Seeking 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 is taken."

11. In the principal regulations, for regulation 25(2), the following sub-regulation shall be substituted, namely:—

"(2) Any such action referred to in sub-regulation (1) and (1A) may also be taken against any entity or Sub-AUA or sub- KUA or OVSE."

12. In the principal regulations, for regulation 25(3), the following sub-regulation shall be substituted, namely:—

"(3) Upon termination of appointment or registration by the Authority, the requesting entity or the ASA or the OVSE 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) and 23A(2)."

CHIRAG PANWAR, Director

[ADVT.-III/4/Exty./534/2025-26]

Note: The principal regulations were published in the Gazette of India, Extraordinary, Part III, Section 4, dated the 9th November, 2021, vide Notification F. No. K-11020/ 240/ 2021/ Auth/UIDAI (No. 2 of 2021), dated the 8th November 2021, and were subsequently amended vide Notifications—

(i) F. No. K-11020/240/2021/Auth/UIDAI (No. 01 of 2022), dated the 4th February, 2022;

(ii) F. No. HQ-13011/2/2021-AUTH-II (No. 01 of 2023), dated the 24th February, 2023 (published on the 27th February, 2023);

(iii) F. No. HQ-13073/1/2020-AUTH.II(E), dated the 29th September, 2023 (published on the 3rd October, 2023); and

(iv) F. No. HQ-13073/1/2020-AUTH.II(E), dated the 31st January, 2024.

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.

E
AUTHENTICATION & VERIFICATION

Annexure II

डा० अजय भूषण पांडे, भा.प्र.से.
मुख्य कार्यकारी अधिकारी
Dr. Ajay Bhushan Pandey, IAS
Chief Executive Officer

भारत सरकार
Government of India
भारतीय विशिष्ट पहचान प्राधिकरण
Unique Identification Authority of India (UIDAI)
तीसरी मंजिल, टॉवर II, जीवन भारती भवन,
कनॉट सर्कस, नई दिल्ली-110001
3rd Floor, Tower II, Jeevan Bharati Building,
Connaught Circus, New Delhi-110001

No 23011/Gen/2014/Legal-UIDAI

Circular

15th September, 2016

Subject: -Notification for use of Aadhaar under Section 7 of **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016**("Aadhaar Act") for targeted delivery of financial and other subsidies, benefits and services funded from Consolidated Fund of India.

The use of Aadhaar as identifier for delivery of services/benefits/subsidies simplifies the Government delivery processes, brings in good governance, transparency and efficiency, and enables beneficiaries to get their entitlements directly to them in a convenient and hassle free manner. Aadhaar obviates the need for producing multiple documents to prove identity, etc.

2. The provisions of the **Aadhaar Act** have come into effect from 12th September 2016 and a notification to this effect has been published in the Official Gazette. To give effect to the provisions of the Act, UIDAI has approved Regulations under the Aadhaar Act which too have been notified in the official Gazette. The copy of the Act, rules and regulations made there under are available at UIDAI web site www.uidai.gov.in.

3. Section 7 of the Act provides:

"The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt there from forms part of, the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment:

Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service".

4. Further, regulation 12 of the **Aadhaar (Enrolment and Update) Regulations, 2016** provides:

"Any Central or State department or agency which requires an individual to undergo authentication or furnish proof of possession of Aadhaar number as a condition for receipt of any subsidy, benefit or service pursuant to Section 7 of the Act, shall ensure enrolment of its beneficiaries who are yet to be enrolled, through appropriate measures, including co-ordination with Registrars and setting up enrolment centres at convenient locations or providing enrolment facilities by becoming a Registrar itself"

Tel.: 23752675 Fax : 23752679
Website: www.uidai.gov.in email: ceo@uidai.gov.in

AADHAAR
मेरा आधार, मेरी पहचान

5. Therefore, Central Ministries / State Governments which plan to use Aadhaar for delivery of services, benefits and subsidies funded from the Consolidated Fund of India are required to issue a notification under Section 7 of the Act. Section 7 of the Act read with Regulation 12 of the **Aadhaar (Enrolment and Update) Regulations, 2016** require that the notification must include all of the following three points:

5.1. The notification shall mention the service, benefits or subsides funded from the Consolidated Fund of India, which will require, as a condition precedent, a beneficiary applicant to undergo Aadhaar Authentication or furnish proof of possession of Aadhaar number.

5.2. The notification shall mention that in case the applicant does not have Aadhaar number, he will be required to make an application for Aadhaar enrolment, if he is entitled to obtain one under the Section 3 of the Act and the arrangement made by the concerned Central Ministries/State Governments as the case may be to provide Aadhaar enrolment facilities to him. Regulation 12 of the said Regulations casts responsibility on the Ministries /State Governments or agencies under their control to facilitate/ provide Aadhaar enrolment facilities at convenient locations. In case, there are no existing enrolment facilities nearby, they are required to become UIDAI registrars so that they can setup enrolment facilities themselves.

UIDAI has already empowered several Central Ministries / State Departments or agencies under their jurisdictions to become its registrar and undertake enrolment of their beneficiaries who are not enrolled for Aadhaar. UIDAI will continue to provide all technical as well as financial assistance for Aadhaar generation @Rs. 40 per Aadhaar and @Rs 27 per Aadhaar generated for children of age less than 5 years through Tablets Computers. In case any Ministry, State Government Department or agencies under its control wants to become Registrar, it may do so immediately by applying under Regulation 21 of the said Regulations and contact Regional Offices of UIDAI for this purpose.

5.3. The notification shall list the alternate identity documents and verification methodologies to confirm the identity of the beneficiary applicant to whom Aadhaar number has not been assigned for delivery of benefits, subsidies or services, till such time Aadhaar number is assigned.

6. This circular has been placed on UIDAI website www.uidai.gov.in

(Ajay Bhushan Pandey) 15/9/2012
Chief Executive Officer

To
All Ministries/Departments
All State Governments

INDEX

डा० अजय भूषण पांडे, भा.प्र.से.
मुख्य कार्यकारी अधिकारी
Dr. Ajay Bhushan Pandey, IAS
Chief Executive Officer

सत्यमेव जयते

भारत सरकार
Government of India
भारतीय विशिष्ट पहचान प्राधिकरण
Unique Identification Authority of India (UIDAI)
तीसरी मंजिल, टॉवर II, जीवन भारती भवन,
कनॉट सर्कस, नई दिल्ली-110001
3rd Floor, Tower II, Jeevan Bharati Building,
Connaught Circus, New Delhi-110001

No. 23011/Gen/2014/Legal-UIDAI

24th October, 2017

Circular

Subject: Exception handling in Public Distribution Services and other welfare Schemes

Section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 provides that:

"The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment:

Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service."

2. Various Ministries/Departments have issued notification under Section 7 of Aadhaar Act to require Aadhaar / Aadhaar authentication for delivery of various benefits, subsidies or service for which the expenditure is incurred from, or the receipt therefrom forms part of the Consolidated Fund of India.

3. It has come to notice that some beneficiaries are being denied the benefit, subsidy or service for various reasons such as not having Aadhaar; failure of authentication; and other extraneous circumstances like electricity outage, internet connectivity issues etc despite above provisions of Aadhaar Act and other adequate mechanisms to handle such exceptions already provided in the Regulations and notifications issued under Section 7.

4. Therefore, the following exception handling mechanism and back-up identity authentication mechanisms may be followed for implementation to ensure seamless delivery of subsidy, benefit or service to beneficiary:

a. Till the time Aadhaar is assigned to a beneficiary, he/she shall be provided subsidy, benefit or service based on alternate identification document as notified by the Ministry/Department in the relevant notification issued under the provision of Section 7 of the Aadhaar Act, 2016. The notifications also give powers to both Central Ministry and State Governments (as the case may be) to add more alternate documents depending on local conditions.

Tel.: 23752675 Fax : 23752679
Website: email:

AADHAAR
मेरा आधार, मेरी पहचान

b. In case of failure of Biometric authentication due to network/connectivity issue or due to poor biometric of resident etc, he/she shall be provided subsidy, benefit or service based on possession of Aadhaar by him/her as provided in Section 7 of the Aadhaar Act, 2016 and the notification.

c. In case of a family based scheme, such as PDS, an option shall be provided that any member of the family can authenticate and receive the benefit, as notified by the Ministry/Department in the relevant notification issued under the provision of Section 7 of the Aadhaar Act, 2016. This flexibility should be used for ensuring delivery of benefit in case biometric authentication for a member (senior) fails.

d. The State Governments/Implementing agency should also make special arrangements for bed ridden senior residents to get them verified/ authenticated including but not limited to sending a village level worker to their home for this purpose.

e. All such exception handling shall be recorded in the system and steps be taken to avoid any misuse of the exception. The front end service provider shall also maintain record of exception such as copy of Aadhaar letter, signature/thumbprint of the beneficiary and other supporting documents as notified by the Ministry/Department.

f. The Ministry/Department shall devise and implement mechanism for audit and inspection of such exceptions.

5. The Ministries/Department are requested to issue appropriate directions to the State Governments/Implementing agencies for the above exception handling mechanism and also monitor the same on periodical basis.

(Dr. Ajay Bhushan Pandey)
Chief Executive Officer

To
All Ministries/Departments
All State Governments

INDEX

No. D-26011/04/2017-DBT
Government of India
Cabinet Secretariat
(DBT Mission)

Dated: 19th December 2017

Office Memorandum

Subject: Use of Aadhaar in Benefit Schemes of Government - Exception Handling - Regarding.

Aadhaar based DBT is a significant governance reform to ensure greater transparency and accountability in public service delivery through effective use of technology. Aadhaar as an identity proof obviates the need for producing multiple documents for proving one's identity, thereby simplifying procedures and eliminating fake/ ghost beneficiaries through de-duplication.

2. However, Government is sensitive to the fact that the Aadhaar enrolment process has not been completed and infrastructure constraints may pose difficulty in online authentication. To ensure that bona fide beneficiaries are not deprived of their due benefits, sufficient provisions have been made in the Aadhaar Act, 2016. UIDAI has also issued regulations to handle exceptions, ensuring that no beneficiary is denied benefits for want of Aadhaar, vide circular dated 24th October, 2017 (*copy enclosed for ready reference*). In accordance with the guidelines issued by UIDAI from time to time, the following may be considered:

A. For extending benefits to beneficiaries who do not possess Aadhaar, the following mechanism may be adopted:

i. The beneficiary shall be provided subsidy, benefit or service based on alternate identification document as notified in the relevant notifications issued under the provisions of Section 7 of the Aadhaar Act, 2016.

ii. Efforts should be made to ensure that all such beneficiaries are facilitated for enrolment under Aadhaar. The concerned Department through its Implementing Agencies may offer Aadhaar enrolment facilities for such beneficiaries at convenient locations through centres in the respective Block/ Taluka/ Tehsil (including through Post Offices, Banks, ICDS Centres etc).

iii. As per regulation 12 of Aadhaar (Enrolment and Update) Regulations, 2016, the State Government/ Implementing Agencies should also make special arrangements for bed ridden, differently-abled, or senior citizens, who are unable to visit the registration centre(s), to get them enrolled for Aadhaar.

iv. Till such time Aadhaar is assigned to a beneficiary, a separate register, preferably electronic, shall be maintained for recording such transactions, whenever the beneficiary is provided benefits/ services on the basis of alternative identification documents. This register may be periodically reviewed and audited.

B. In all such cases where Aadhaar authentication fails, the following mechanism may be adopted:

INDEX

i. Departments and Bank Branches may make provisions for IRIS scanners along with fingerprint scanners, wherever feasible.

ii. In cases of failure due to lack of connectivity, offline authentication system such as QR code based coupons, Mobile based OTP or TOTP may be explored.

iii. In all cases where online authentication is not feasible, the benefit/ service may be provided on the basis of possession of Aadhaar, after duly recording the transaction in register, to be reviewed and audited periodically.

3. In view of above, DBT implementing Ministries/ Departments and State Governments are requested to implement proper exception handling mechanism in conformity with the Aadhaar Act 2016 and subsequent regulations and guidelines issued from time to time. A robust mechanism for ensuring their compliance and its periodic monitoring may also be put in place.

Enclosure: As above

(Arun Sharma)
Director (DBT)
Tel – (011) 23343860 Ext: 318

To:

1. Secretaries to all Ministries/ Departments of Government of India
2. Chief Secretaries of all States/ Administrators of all UTs
3. CEO, UIDAI

Copy to:

1. Coordinators, DBT Cells in all Ministries / Departments
2. Coordinators, DBT Cells in all States / UTs.

NOO:

1. AS (TB), PMO
2. SO to CS / Sr. PPS to Addl. Secretary (Coordination) / JS (AG) / JS (DBT)

F.No. No. 4(4)/57/186/2016/E&U-pt-II
Government of India
Ministry of Electronics & IT
Unique Identification Authority of India

UIDAI Hqrs. Building,
Bangla Sahib Road, New Delhi-01
Dated : 20/12/2018

OFFICE MEMORANDUM

Sub:- **Clarification regarding usage of Aadhaar.**

This authority has received references seeking clarification on whether Aadhaar can be used as proof of Date of Birth. Furthermore, it has been observed that usage of Aadhaar (as proof of Date of birth) is being interpreted in a differing manner by various Government Department/ Ministry / Court. In this regard, following clarification is issued :-

(1) Aadhaar is an identification number issued to a resident after he /she undergoes the process of Aadhaar enrolment by submitting his/her demographic / Biometric information. Once a resident is assigned an Aadhaar number it can be used to authenticate the resident through various modes as prescribed under Aadhaar Act,2016 and Regulations framed thereunder.

(2) At the time of enrolment/ Updation, UIDAI records date of birth as claimed by the resident, on the basis of the documents submitted by them such as Birth Certificate, SSLC Book/Certificate, Passport and Certificate of Date of Birth issued by Group A Gazetted Officer on letterhead etc. If a resident does not have any valid supporting date of birth document, date of birth is recorded on the basis of Declared and Approximate date of birth. In case of approximate date of birth the age is verbally communicated by resident to the enrolment operator and the enrolment / updation software calculates the year of Birth and by default, the date of birth is recorded as 1st January of that calendar year. Section 4(3) of the Aadhaar Act,2016 mentions that an Aadhaar number, in physical or electronic form subject to authentication and other conditions, as may be specified by regulations, accepted as proof of identity of Aadhaar number holder but, it doesn't mention that Aadhaar can be accepted as proof of date of birth. The date of birth is recorded on the basis of the self declaration given by the resident. Therefore, in case of dispute regarding correctness of the date of birth, the burden of proof lies with the resident.

3. That in other words, Aadhaar is only a proof of the fact the person who is trying to obtain a subsidy/service by identifying himself on the basis of Aadhaar number is the same person who had enrolled for Aadhaar after providing his biometrics and other documents at the time of his Enrolment. Aadhaar is only the method of identification of the identity that the Aadhaar holder presented at the time of Enrolment.

4. That in light of the above, the issue with regard to the correctness of the date of birth etc., has been gone into threadbare by the Hon'ble Supreme Court and it has been found that the purpose of Aadhar is to ensure that the person who seeks to receive the subsidy etc. is the person who had enrolled, is ensured by way of a positive authentication.

INDEX

5. It is also clarified that role of UIDAI is limited to issue of Aadhaar numbers and provide authentication services for establishing identity of the individual/ residents. 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 of thereof, on the basis of information available with it. The usage of Aadhaar for delivery of welfare services benefits etc or for any other purpose and the extent to which Aadhaar is to be used is to be determined by the implementing agencies such as state Governments/ Central Ministries and other agencies.

6. In view of the above, it is suggested that all Central Ministries/ Departments/ State Governments and other implementing agencies may keep in consideration the following :-

(a) An Aadhaar number can be used for establishing identity of an individual subject to authentication and thereby, per se its not a proof of date of birth.

(b) the usage of Aadhaar for delivery of welfare services, benefits or subsidies pursuant to Section 7 of the Aadhaar Act, 2016 or for any other purpose as may be required under any applicable law and the extent to which Aadhaar is to be used is to be determined by the implementing agencies such as State Government/ Central Ministries and other agencies.

(c) Aadhaar which includes Aadhaar card, physical copy of e-aadhaar, masked Aadhaar, offline Aadhaar XML, and QR code embedded on the Aadhaar card, may be used as a proof of identity / proof of address along with other acceptable documents (subject to such terms and conditions as may be imposed by the Authority from time to time), **however, same may not be used as a proof of date of birth.**

(Ashok Kumar)
Assistant Director General

To,

(i) Secretaries, All Ministries/ Departments, Government of India.

(ii) Chief Secretaries, All State Governments/ UT Administrations

INDEX

Annexure III

भारत सरकार
Government of India
भारतीय विशिष्ट पहचान प्राधिकरण
Unique Identification Authority of India (UIDAI)
आधार मुख्यालय, बंगला साहिब रोड, काली मंदिर के पीछे
गोल मार्किट, नई दिल्ली–110001
Aadhaar H.Q., Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi-110001

No. 1-1/2019-UIDAI (DBT) *Dated:* 25th November, 2019

CIRCULAR

Subject: Guidelines on use of Aadhaar under section 7 of the Aadhaar Act 2016 (as amended by the Aadhaar and Other Laws (Amendment) Act, 2019) by the State Governments for the schemes funded out of Consolidated Fund of State.

The use of Aadhaar as identity document for delivery of services or benefits or subsidies simplifies the Government delivery processes, brings in transparency and efficiency, and enables beneficiaries to get their entitlements directly in a convenient and seamless manner by obviating the need to produce multiple documents to prove one's identity.

2 The provisions of the Aadhaar Act, 2016 had come into effect from 12th September 2016 through a Gazette notification. Subsequently, to give effect to the provisions of the Act, various Regulations under the Aadhaar Act have been notified by UIDAI in the official Gazette. Further, the Aadhaar and Other Laws (Amendment) Act, 2019 has been notified on 24th July 2019 after its passing by the Parliament, which *inter-alia*, includes an amendment of section 7 of the Aadhaar Act, as under:

> *"In section 7 of the principal Act, after the words 'the Consolidated Fund of India', the words "or the Consolidated Fund of State" shall be inserted."*

3 Section 7 of the Aadhaar Act 2016 stipulates that as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from the Consolidated Fund of India or the Consolidated Fund of States, the Central Government or the State Government may require the individual to undergo Aadhaar authentication or furnish proof of possession of Aadhaar number. Hon'ble Supreme Court of India in its judgment dated 26th September 2018 in the Writ Petition (Civil) No. 494 *Justice K.S. Puttaswamy v. Union of India*, has further clarified the interpretation of section 7 and held as under (*Ref. para 322 and para 447 (2)(m), page 555 of the judgement*):

> *'(a) 'benefits' and 'services' as mentioned in Section 7 should be those which have the colour of some kind of subsidies etc., namely, welfare schemes of the Government whereby Government is doling out such benefits which are targeted at a particular deprived class.*

Tel : 011-23478652
Website :

AADHAAR
मेरा आधार, मेरी पहचान

INDEX

(b) The expenditure thereof has to be drawn from the Consolidated Fund of India

(c) On that basis, CBSE, NEET, JET, UGC etc. cannot make the requirement of Aadhaar mandatory as they are outside the purview of Section 7 and are not backed by any law" (emphasis supplied)

The Supreme Court has, thus interpreted 'benefits' in section 7 as welfare measures targeted at a particular deprived class of persons. This class of persons as interpreted by the Supreme Court can be construed as a specific group of people having in common their socio-economic status as well as the broad causes of having that particular status. It has also been clarified by the aforementioned judgment that since earnings by an individual are a matter of right they cannot be covered by section 7 of the Aadhaar Act. Therefore, payment of remuneration, and other expenses to employees or contractual manpower cannot be considered as 'benefits' under section 7 of the Aadhaar Act.

Further, Section 3A(3) inserted vide the Aadhaar and Other Laws (Amendment) Act, 2019 stipulates that notwithstanding anything contained in section 7, a child shall not be denied any benefit, subsidy or service for failure to establish his identity by undergoing authentication or furnishing proof of possession of Aadhaar number or in case of a child to whom no Aadhaar number has been assigned, producing an application for enrolment.

4. Until now, using section 7 of the Aadhaar Act 2016, only Central Ministries/ Departments have been mandating use of Aadhaar of the beneficiaries under their respective schemes (both under Central administration and Central sponsorship) through publishing section 7 notifications in the Gazette of India, after due vetting of the same by the Ministry of Law & Justice. UIDAI has been facilitating the process of vetting of all these notifications since November 2016.

5 As per provisions in the Aadhaar and Other Laws (Amendment) Act, 2019, the State Governments can henceforth, mandate use of Aadhaar authentication for the beneficiaries under section 7 of the Aadhaar Act 2016 in those schemes which are funded out of Consolidated Fund of the State. In order to do so, the State Governments will need to issue notifications under section 7 of the Aadhaar Act, 2016 in respect of the specific schemes, similar to the ones as published by the Central Ministries/Departments.

6. Accordingly, it is suggested that the State Governments may take the following steps to issue section 7 notifications under their specific schemes which are funded out of Consolidated Fund of the State:

a) The State Governments may first identify the schemes for use of Aadhaar where 'benefits' are given to the 'individuals', and ensure that the schemes fulfil the criteria of being eligible under section 7 of the Aadhaar Act, as per

INDEX

the judgement of the Hon'ble Supreme Court dated 26th September 2018 (*Ref. para 3 above*).

b) Thereafter, a draft notification for the specific scheme may be prepared by the Department implementing the scheme, and vetted by the Legal Department of the State Government before publishing it, as per the extant procedure.

c) The State Governments may use a standard template of section 7 notification (***Annex-1***). In case, children are beneficiaries under any scheme, an additional paragraph is required to be inserted as per section 3A (3) of the Aadhaar and Other Laws (Amendment) Act, 2019. A sample of children specific scheme notification is enclosed at ***Annex-2***.

d) After publication of the section 7 notification in the State Gazette, the State Governments may approach Authentication Division of UIDAI HQ seeking necessary permission (if not already received) for online authentication of the beneficiaries under the respective schemes. In this regard, guidelines available on UIDAI's website may be referred to (https://www.uidai.gov.in/images/resource/Compendium_August_2019.pdf).

7. This circular has been placed on UIDAI's website (https://www.uidai.gov.in/about-uidai/legal-framework/circulars.html).

(Pankaj Kumar)
Chief Executive Officer, UIDAI

Enclosures:

1. Annex-1: *Sample Template of Aadhaar Section 7 Notification for the State Schemes where beneficiaries are other than children*
2. Annex-2: *Sample Template of Aadhaar Section 7 Notification for the State Schemes where beneficiaries are children*
3. Office Memorandum of DBT Mission Cabinet Secretariat dated 19th December 2017: *'Use of Aadhaar in Benefit Schemes of Government – Exception Handling'* (https://dbtbharat.gov.in/data/om/Aadhaar_Exception_Handling_OM_19122017.pdf)
4. UIDAI Circular dated 24th October 2017: *'Exception handling in Public Distribution Services and other welfare Schemes'* (https://uidai.gov.in/images/tenders/Circular_relating_to_Exception_handling_25102017.pdf)

To
Chief Secretaries, All State Governments

Copy for information to:

1. Secretary (Coordination), DBT Mission, Cabinet Secretariat
2. Joint Secretary (in charge of UIDAI), M/o Electronics and Information Technology
3. Dy. Director General, All Regional Offices, UIDAI
4. Authentication/Legal Divisions, UIDAI HQ

Page 3 of 3

INDEX

Annex-1: Sample Template of Aadhaar Section 7 Notification for the State Schemes where beneficiaries are other than children

---

[TO BE PUBLISHED IN THE [*insert name of relevant gazette*]]

Government of [*insert name of appropriate state government*]
[*insert name of relevant Department of the state government*]

NOTIFICATION

[*insert name of relevant city*], the ---------, 2019

S.O.....(E).__ Whereas, the use of Aadhaar as an identity document for delivery of services or benefits or subsidies simplifies the Government delivery processes, brings in transparency and efficiency, and enables beneficiaries to get their entitlements directly in a convenient and seamless manner by obviating the need to produce multiple documents to prove one's identity;

And whereas, the [***insert name of relevant department***] (*hereinafter referred to as the Department*), is administering the [***insert name of relevant scheme***] (*hereinafter referred to as the Scheme*) to [***insert description of the scheme***] , which is being implemented through the [***insert name of implementing agency at the state level***] (*hereinafter referred to as the Implementing Agency(ies)*)

And whereas, under the Scheme, [***insert description of the benefit***] (*hereinafter referred to as the benefit*) is given to the [***insert description of the beneficiaries***] (*hereinafter referred to as the beneficiaries*), by the Implementing Agency as per the extant Scheme guidelines;

And whereas, the aforesaid Scheme involves recurring expenditure incurred from the Consolidated Fund of [***insert name of the relevant state***],

Now, therefore, in pursuance of section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016) (hereinafter referred to as the said Act), the government of [***insert name of the relevant state***] hereby notifies the following, namely:-

1 (1) An individual eligible for receiving the benefits under the Scheme shall hereby be required to furnish proof of possession of the Aadhaar number or undergo Aadhaar authentication.

(2) Any individual desirous of availing benefits under the Scheme, who does not possess the Aadhaar number or, has not yet enrolled for Aadhaar, shall be required to make application for Aadhaar enrolment before registering for the Scheme provided that he is entitled to obtain Aadhaar as per section 3 of the

INDEX

said Act, and such individuals shall visit any Aadhaar enrolment centre (list available at the Unique Identification Authority of India (UIDAI) website www.uidai.gov.in) to get enrolled for Aadhaar.

(3) As per regulation 12 of the Aadhaar (Enrolment and Update) Regulations, 2016, the Department through its Implementing Agency, is required to offer Aadhaar enrolment facilities for the beneficiaries who are not yet enrolled for Aadhaar and in case there is no Aadhaar enrolment centre located in the respective Block or Taluka or Tehsil, the Department through its Implementing Agency shall provide Aadhaar enrolment facilities at convenient locations in coordination with the existing Registrars of UIDAI or by becoming a UIDAI Registrar themselves:

Provided that till the time Aadhaar is assigned to the individual, benefits under the Scheme shall be given to such individual, subject to the production of the following documents, namely –

(a) if he has enrolled, his Aadhaar Enrolment Identification slip; and

(b) any one of the following documents, namely :-

(i) Bank or Post office Passbook with Photo; or

(ii) Permanent Account Number (PAN) Card; or

(iii) Passport; or

(iv) Ration Card; or

(v) Voter Identity Card; or

(vi) MGNREGA card; or

(vii) Kisan Photo passbook; or

(viii) Driving license issued by the Licensing Authority under the Motor Vehicles Act, 1988 (59 of 1988); or

(ix) Certificate of identity having photo of such person issued by a Gazetted Officer or a Tehsildar on an official letter head; or

(x) any other document as specified by the Department.

Provided further that the above documents may be checked by an officer specifically designated by the Department for that purpose.

2. In order to provide benefits to the beneficiaries under the Scheme conveniently, the Department through its Implementing Agency shall make all the required arrangements to ensure that wide publicity through the media shall be given to the beneficiaries to make them aware of the said requirement.

INDEX

3 In all cases, where Aadhaar authentication fails due to poor biometrics of the beneficiaries or due to any other reason, the following remedial mechanisms shall be adopted, namely -

(a) in case of poor fingerprint quality, iris scan or face authentication facility shall be adopted for authentication, thereby the Department through its Implementing Agency shall make provisions for iris scanners or face authentication along with finger-print authentication for delivery of benefits in seamless manner;

(b) in case the biometric authentication through fingerprints or iris scan or face authentication is not successful, wherever feasible and admissible authentication by Aadhaar One Time Password or Time-based One-Time Password with limited time validity, as the case may be, shall be offered;

(c) in all other cases where biometric or Aadhaar One Time Password or Time-based One-Time Password authentication is not possible, benefits under the Scheme may be given on the basis of physical Aadhaar letter whose authenticity can be verified through the Quick Response (QR) code printed on the Aadhaar letter and the necessary arrangement of QR code reader shall be provided at the convenient locations by the Department through its Implementing Agency.

4 In addition to the above, in order to ensure that no bona fide beneficiary under the Scheme is deprived of his due benefits, the Department through its Implementing Agency shall follow the exception handling mechanism as outlined in the Office Memorandum of DBT Mission, Cabinet Secretariat, Government of India dated 19th December 2017.

5. This notification shall come into effect from the date of its publication in the Official Gazette.

[F No)

(Name)

[insert designation of appropriate official of the relevant state government who is adequately empowered for this purpose]

INDEX

Annex-2: Sample Template of Aadhaar Section 7 Notification for the State Schemes where beneficiaries are children

---

[TO BE PUBLISHED IN THE [*insert name of relevant gazette*]]

Government of [*insert name of appropriate state government*]
[*insert name of relevant Department of the state government*]

NOTIFICATION

[*insert name of relevant city*], the ----------, 2019

S.O.....(E).__ Whereas, the use of Aadhaar as an identity document for delivery of services or benefits or subsidies simplifies the Government delivery processes, brings in transparency and efficiency, and enables beneficiaries to get their entitlements directly in a convenient and seamless manner by obviating the need to produce multiple documents to prove one's identity;

And whereas, the [***insert name of relevant department***] (*hereinafter referred to as the Department*), is administering the [***insert name of relevant scheme***] (*hereinafter referred to as the Scheme*) to [***insert description of the scheme***], which is being implemented through the [***insert name of implementing agency at the state level***] (*hereinafter referred to as the Implementing Agency*);

And whereas, under the Scheme, [***insert description of the benefit***] (*hereinafter referred to as the benefit*) is given to the [***insert description of the beneficiaries***] (*hereinafter referred to as the beneficiaries*), by the Implementing Agency as per the extant Scheme guidelines;

And whereas, the aforesaid Scheme involves recurring expenditure incurred from the Consolidated Fund of [***insert name of the relevant state***];

Now, therefore, in pursuance of section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016) (*hereinafter referred to as the said Act*), the government of [***insert name of the relevant state***] hereby notifies the following, namely -

1 (1) A child desirous of availing the benefit under the Scheme shall hereby be required to furnish proof of possession of the Aadhaar number or undergo Aadhaar authentication.

(2) Any child desirous of availing the benefit under the Scheme, who does not possess the Aadhaar number or, has not yet enrolled for Aadhaar, shall be required to make application for Aadhaar enrolment subject to the consent of his parents or guardians, before registering for the Scheme provided that he is entitled to obtain Aadhaar as per section 3 of the said Act and such children shall visit any Aadhaar enrolment centre (list available at the Unique Identification Authority of India (UIDAI) website www.uidai.gov.in) to get enrolled for Aadhaar.

INDEX

(3) As per regulation 12 of the Aadhaar (Enrolment and Update) Regulations, 2016, the Department through its Implementing Agency, is required to offer Aadhaar enrolment facilities for the beneficiaries who are not yet enrolled for Aadhaar and in case there is no Aadhaar enrolment centre located in the respective Block or Taluka or Tehsil, the Department through its Implementing Agency shall provide Aadhaar enrolment facilities at convenient locations in coordination with the existing Registrars of UIDAI or by becoming a UIDAI Registrar themselves:

Provided that till the time Aadhaar is assigned to the child, the benefit under the Scheme shall be given to such children subject to production of the following documents, namely:-

(a) (i) if the child has been enrolled after attaining the age of five years (with biometrics collection), his Aadhaar Enrolment Identification slip, or of bio-metric update identification slip; and

(b) any one of the following documents, namely:-

(i) Birth Certificate; or Record of birth issued by the appropriate authority; or

(ii) School identity card duly signed by the Principal of the school containing parents' names; and

(c) any one of the following documents as proof of relationship of the beneficiary with the parent or legal guardian as per the extant Scheme guidelines, namely:–

(i) Birth Certificate; or Record of birth issued by the appropriate authority or

(ii) Ration Card; or

(iii) Ex-Servicemen Contributory Health Scheme (ECHS) Card; or Employees' State Insurance Corporation (ESIC) Card; or Central Government Health Scheme (CGHS) Card; or

(iv) Pension Card; or

(v) Army Canteen Card; or

(vi) any Government Family Entitlement Card; or

(vii) any other document as specified by the Department.

Provided further that the above documents shall be checked by an officer specifically designated by the Department for that purpose.

2. In order to provide benefits to the beneficiaries under the Scheme conveniently, the Department through its Implementing Agency shall make all the required arrangements to ensure that wide publicity through media shall be given to the beneficiaries to make them aware of the said requirement.

INDEX

3 In all cases, where Aadhaar authentication fails due to poor biometrics of the beneficiaries or due to any other reason, the following remedial mechanisms shall be adopted, namely:-

(a) in case of poor fingerprint quality, iris scan or face authentication facility shall be adopted for authentication, thereby the Department through its Implementing Agency shall make provisions for iris scanners or face authentication along with finger-print authentication for delivery of benefits in seamless manner;

(b) in case the biometric authentication through fingerprints or iris scan or face authentication is not successful, wherever feasible and admissible authentication by Aadhaar One Time Password or Time-based One-Time Password with limited time validity, as the case may be, shall be offered;

(c) in all other cases where biometric or Aadhaar One Time Password (OTP) or Time-based One-Time Password authentication is not possible, benefits under the scheme may be given on the basis of physical Aadhaar letter whose authenticity can be verified through the Quick Response (QR) code printed on the Aadhaar letter and the necessary arrangement of QR code reader shall be provided at the convenient locations by the Department through its Implementing Agency

4 Notwithstanding anything contained herein above, no child shall be denied benefit under the Scheme in case of failure to establish his identity by undergoing authentication, or furnishing proof of possession of Aadhaar number, or in the case of a child to whom no Aadhaar number has been assigned, producing an application for enrolment. The benefit shall be given to him by verifying his identity on the basis of other documents as mentioned in clauses (b) and (c) of the proviso of sub-paragraph (3) of paragraph 1, and where benefit is given on the basis of such other documents, a separate register shall be maintained to record the same, which shall be reviewed and audited periodically by the Department through its Implementing Agency.

5 This notification shall come into effect from the date of its publication in the Official Gazette.

[F No .....]

(Name .....)

[*insert designation of appropriate official of the relevant state government who is adequately empowered for this purpose*]

INDEX

सं .के 13028/1/2021/ यूआईडीएआई (ऑथ-I)
भारत सरकार
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)
(अधिप्रमाणन विभाग)

यूआईडीएआई मुख्यालय भवन, तीसरी मंजिल,
बंगला साहेब रोड, काली मंदिर के पीछे,
गोल मार्केट, नई दिल्ली- 110001.

दिनांक: 13 .01.2023

Circular

Subject: Use biometric modality in non-assisted mode

The Aadhaar based biometric authentication is extensively used by Central/State governments, financial institutions and other requesting entities across the country with fingerprint as the main biometric modality. These authentication transactions provide verification of the resident which forms the basis of further transactions of the user entity.

During various workshops and interactions, UIDAI advises AUAs that biometric authentication should invariably be performed in operator assisted mode. This provides a two factor authentication mechanism (one factor of UIDAI and the second factor of operator of the entity), which helps in future tracing of unscrupulous elements in case of fraudulent transactions.

However, in recent past various entities have approached UIDAI to permit for biometric authentication in non-assisted mode. This will help residents authenticate themselves from their home without the need to visit any operator. Therefore, it has been decided that biometric authentication may be performed in non-assisted mode, however the requesting entities shall add one more factor of their own in the form of OTP/PIN etc for biometric authentication transactions performed in non assisted mode, so as to ensure that two factor authentication of the resident is maintained.

This issues with the approval of the competent authority.

(Sanjeev Yadav)
Director (Auth-I, HQ UIDAI)

To,
All AUA/KUAs

Copy for information to:
DDG (Tech Ops), UIDAI

INDEX

F. No. HQ-13021/1/2021-Auth-I HQ
Government of India
Ministry of Electronics & Information Technology
Unique Identification Authority of India (UIDAI)
Authentication and Verification Division
Third Floor, UIDAI Headquarters,
Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi – 110001
Date: 27.01.2023

To

All AUA/KUAs/ASAs

Sub: Phase out of existing fingerprint L0 Registered Devices from Aadhaar authentication ecosystem.

Dear Partners,

Please refer: (i) UIDAI letter No. HQ-13021/1/2021-Auth-I HQ dated 25.04.2022 and 31.05.2022
(ii) Letter No. HQ-13023/1/2020-Auth-I HQ/2084 dated 20.06.2022 and 23.12.2022
(iii) Letter No. HQ- 13029/1/2021-Auth-I-HQ dated 23.12.2022

In order to enhance the security levels of finger print based authentication transaction, UIDAI takes several security measures from time to time to ensure security of authentication transactions and end to end encryption during the authentication process. In this regard, fingerprint devices being used in Aadhaar authentication ecosystem have been upgraded from the currently used fingerprint L0 RD to the next generation fingerprint L1 RD. First batch of devices have already been certified on 30.10.2022 (website link: https://uidai.gov.in/en/ecosystem/authentication-devices-documents/biometric-devices.html). The key features of fingerprint L1 Registered Devices (RD) were communicated in details vide letters at reference (i) to all authentication ecosystem partners and also during various Central/State government level workshops organised by UIDAI since notification.

2. Roll out of fingerprint L1 RD

Since at present all fingerprint devices in the authentication ecosystem are of L0 standards, the fingerprint biometric authentication transactions shall for the time being continue both in L0 RD and L1 RD. However, to avoid any disruptions in the system, all the existing deployed fingerprint L0 RD would be phased out of the authentication ecosystem in a gradual manner. To provide sufficient period for this transition, it has been decided that use of all the existing fingerprint L0 RD will be discontinued by 30.06.2024 and thereafter only fingerprint L1 RD will be allowed to perform Aadhaar based authentications. Therefore, all AUA/KUAs may like to procure fingerprint L1 RD for use in their authentication ecosystem.

3. Phase out of fingerprint L0 RD

(a) UIDAI vide letters No. HQ-13023/1/2020-Auth-I HQ/2084 dated 20.06.2022 and 23.12.2002 has issued directions to all AUA/KUAs regarding removal of old and deployed L0 RD. The devices whose STQC certification has not been renewed and on which there were nil or fewer transactions reported have already been hot listed w.e.f 01.01.2023. The devices reporting higher authentication transactions would be hot listed on 31.03.2024.

(b) UIDAI vide letter No. HQ- 13029/1/2021-Auth-I-HQ dated 23.12.2022 has also asked all AUA/KUA to identify the L0 registered devices having low authentication success rate (below 30%) or are more than five years old vintage and to remove such devices from the authentication ecosystem in a phased manner.

(c) Timelines for phase out of fingerprint L0 Registered devices are as follows:

Date	Roll out Plan of fingerprint L1 compliant Registered Device	Remarks
31/03/2023	Fingerprint L0 RD deployed before 31.12.2014	AUA/KUA to give self declaration, that no fingerprint L0 RD deployed are of before 31.12.2014
30/06/2023	Fingerprint L0 RD deployed before 31.12.2016	AUA/KUA to give self declaration, that no fingerprint L0 RD deployed are of before 31.12.2016
31/12/2023	Fingerprint L0 RD deployed before 31.12.2019	AUA/KUA to give self declaration, that no fingerprint L0 RD deployed are of before 31.12.2019
30/06/2024	Sunset of fingerprint L0 RD	No authentication transaction will be passed through fingerprint L0 RD

4. As the iris devices are relatively more secure, all the Iris L0 RD will continue to function as present.

5. This issues with the approval of competent authority.

(Sanjeev Yadav)
Director (Auth-1)

Copy for information to:

1. All Secretaries of Government of India Ministries/ Departments
2. All Chief Secretaries of States/UT
3. DG, STQC
4. All DDGs, UIDAI (Head Quarters, Tech Centre, Regional offices)

INDEX

F.No. HQ-13079/2/2023-AUTH-II HQ (E-10669) /5566
Government of India
Ministry of Electronics and Information Technology
Unique Identification Authority of India
(Authentication and Verification Division)

3rd Floor, UIDAI HQs,
Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi-110001
Dated: 23.03.2023

CIRCULAR NO. 01 of 2023

Ref: Ministry of Finance, Department of Revenue [DoR], Notification S.O. 5683(E) dated 6th December, 2022: e-KYC Setu System.

Vide the above referred notification the e-KYC setu system, to be put in place by NPCI, shall carry out Aadhaar authentication for the entities regulated by regulators under Section 11A of Prevention of Money Laundering Act, 2002 **[the PMLA hereinafter]** namely the Reserve Bank of India, the Securities Exchange Board of India, the Insurance Regulatory Authority of India and the Pension Fund Regulatory Authority of India.

2. Whereas the DoR has issued the *ibid* notification under PMLA for the Reporting Entities regulated therein, however, at the same time the Requesting Entities sending authentication requests to UIDAI are regulated under the relevant provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 **[the Aadhaar Act hereinafter]**. Under the eKYC setu system the regulated entities shall function as the Reporting Entities as per provisions of PMLA. However, since the functions like collection of Aadhaar number and biometrics/OTP, creation of authentication request, use of authentication license key, communication and storage of authentication response obtaining consent, providing grievance handling mechanism, etc. are done independently and separately by regulated entities and NPCI – their responsibilities under Aadhaar Act as Requesting Entities shall accordingly be limited to the extent of functions performed by them.

3. To aid NPCI and the Reporting Entities using this system for smooth on-boarding, compliance with the Aadhaar Act and Regulations there under and friction free services the roles and responsibilities of various stakeholders are hereby enumerated as below:

INDEX

Roles and Responsibilities

A. National Payments Corporation of India (NPCI):

i. NPCI shall design, develop and maintain e-KYC setu system in compliance with the standard of privacy and security laid down by Unique Identification Authority of India (UIDAI). NPCI shall perform Aadhaar-based eKYC authentication as a service to these Reporting Entities.

ii. NPCI shall get the e-KYC setu system audited from CERT-In empanelled IS Auditor before implementing it. Thereafter, NPCI shall undertake audit of the system, through a CERT-In empanelled IS Auditor, on yearly basis and shall submit the report to UIDAI. Further UIDAI reserves the right to undertake audit of the eKYC setu system, either by itself or through audit agencies appointed by it, to ensure the compliance with Aadhaar Act, rules, regulations, policies, procedures, directions, guidelines, circulars, MoU.

iii. NPCI shall ensure that Memorandum of Understanding (MoU) executed with Reporting Entities must incorporate relevant provisions of Aadhaar Act, 2016 and regulation there under. NPCI to seek concurrence of UIDAI on draft MoU with respect to provisions pertaining to Aadhaar.

iv. On receiving an on-boarding request or application from Reporting Entity, NPCI shall send the request details to UIDAI for issuing a unique/identifier entity code for the respective Reporting Entity.

v. NPCI to ensure that Reporting Entity puts up a grievance handling mechanism for the resident through its MoU/Agreement with the Reporting Entity.

vi. NPCI through adequate provisions of MoU shall ensure audit and inspection of Reporting Entities at such frequency or timeline as may be prescribed by NPCI and/or on the direction of UIDAI.

vii. UIDAI has notified the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021 dated 14.10.2021 whereby UIDAI raise invoices on the basis of criteria laid down in these aforementioned regulations. In this backdrop, following is mentioned for authentication transaction billing purposes:

INDEX

a) UIDAI CIDR provides response to authentication requests within 10 seconds and any response beyond that is not considered for pricing by UIDAI. Therefore, NPCI may keep the response timeout accordingly. It is the responsibility of NPCI to ensure proper connectivity with CIDR. If the response is given by CIDR, it cannot be considered a timeout transaction if not received at NPCI server.

b) UIDAI will raise invoice on NPCI as per the billing cycle for all the chargeable successful and failed Yes-No & e-KYC transactions as per the criteria mentioned in the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021.

c) It shall be responsibility of NPCI to pay authentication charges within the stipulated time as and when invoice raised by UIDAI in this regard. Any delayed payment or non-payment shall attract appropriate action from UIDAI including but not limited to imposition of interest, suspension of license key and termination of agreement. UIDAI shall not be concerned with any default in payment by clients of NPCI and no concessions/relaxations, whatsoever, be requested from UIDAI on this ground.

d) Any dispute between NPCI and its Reporting Entities regarding authentication transaction billing shall be exclusive to them and be dealt in accordance with their mutual agreement. UIDAI shall not have anything to do with that and it shall not be approached for any mediation or resolution of such disputes, whatsoever.

viii. NPCI shall, at all times, ensure compliance of provisions of Aadhaar Act, its associated regulations and other circulars/instructions issued by UIDAI from time to time and also obligations as per the agreement with UIDAI. It shall ensure compliance on the part of Reporting Entities also through its MoU/Agreement with them.

ix. Any Reporting Entity found to be in violation as per provisions of Para 6 of the DoR Notification shall be de-boarded by NPCI as per provisions of the said Para of the DoR notification.

B. Reporting Entity:

i. The Reporting Entity shall ensure that relevant provisions under the Aadhaar Act, 2016 and Regulations there under and relevant circulars/guidelines issued by UIDAI from time to time are duly complied at all times for continuation of smooth and friction-free authentication services.

INDEX

ii. The Reporting Entity shall submit license fee at prescribed rates to UIDAI subsequent to which a unique/identifier entity code shall be allotted to Reporting Entity from UIDAI.

iii. Reporting Entity shall not collect, use or store Aadhaar number or biometric information of any client or beneficial owner for any purpose.

iv. Reporting Entity shall obtain the consent of an individual before collecting his identity information for the purpose of authentication in such manner as specified by the Aadhaar Act, 2016 and regulations there under.

v. Reporting Entity shall notify its client or beneficial owner about any Aadhaar authentication, including success or failure of authentication of each request, performed by them through SMS, email or any other digital means or paper based acknowledgement.

vi. Reporting Entity shall provide a mechanism for the client or its beneficial owner to revoke his consent given to Reporting Entity and upon such revocation Reporting Entity shall delete the e-KYC data in a verifiable manner and provide an acknowledgment of the same to the client or beneficial owner.

vii. Reporting Entity, after receiving digitally signed response packet including last 4 digits of Aadhaar number of the client along with his demographic details, shall carry out identification of the client based on the above details provided by the client and NPCI. Reporting Entity shall not share e-KYC data, obtained from NPCI under eKYC setu system, with any other entity or agency for any whatsoever reason.

viii. Reporting Entity shall retain the logs of authentication transactions (including that of consent taken) in a verifiable and auditable manner for the period as prescribed under the Aadhaar (Authentication and Offline Verification) Regulations, 2021. Purging of such logs upon expiry of the period shall also be in accordance to the Aadhaar Act and/or regulations thereof.

ix. The Reporting Entity shall undertake audit of the operations, systems and procedures through CERT-In empanelled IS auditors to ensure the compliance with the Aadhaar Act, rules, regulations, policies, procedures, directions, guidelines, circulars, MoU laid down. Further UIDAI reserves the right to undertake audit of Reporting Entities, either by itself or through audit agencies, appointed by it to ensure the compliance

INDEX

with Aadhaar Act, rules, regulations, policies, procedures, directions, guidelines, circulars, MoU.

x. Reporting Entities shall ensure its audit and inspection by NPCI or by any CERT-In empanelled third party auditor appointed by NPCI or UIDAI, at such frequency or timeline as may be prescribed by NPCI and/or on the direction of UIDAI.

xi. The Reporting Entity if found in breach of compliances with Aadhaar Act, 2016, rules, regulations, policies, procedures, directions, guidelines, circulars, MoU shall be liable for offences and penalties as prescribed under the Aadhaar Act, 2016, rules and regulations framed there under.

xii. Reporting Entity shall immediately stop using the e-KYC Setu Services if its license or authorization to carry out regulated business has been suspended, cancelled or withdrawn by the appropriate regulatory authority.

xiii. Reporting Entity shall provide an effective grievance handling mechanism to the resident via multiple channels like website, call center, mobile app, SMS, physical center, etc.

4. This issues under approval of the Competent Authority.

Director (A&V)

To,

National Payments Corporation of India (NPCI)

Copy: for information to

(i) Department of Revenue, Ministry of Finance, Government of India
(ii) Reserve Bank of India
(iii) Securities Exchange Board of India
(iv) Insurance Regulatory and Development Authority of India
(v) Pension Fund Regulatory and Development Authority

INDEX

with Aadhaar Act, rules, regulations, policies, procedures, directions, guidelines, circulars, MoU.

x. Reporting Entities shall ensure its audit and inspection by NPCI or by any CERT-In empanelled third party auditor appointed by NPCI or UIDAI, at such frequency or timeline as may be prescribed by NPCI and/or on the direction of UIDAI.

xi. The Reporting Entity if found in breach of compliances with Aadhaar Act, 2016, rules, regulations, policies, procedures, directions, guidelines, circulars, MoU shall be liable for offences and penalties as prescribed under the Aadhaar Act, 2016, rules and regulations framed there under.

xii. Reporting Entity shall immediately stop using the e-KYC Setu Services if its license or authorization to carry out regulated business has been suspended, cancelled or withdrawn by the appropriate regulatory authority.

xiii. Reporting Entity shall provide an effective grievance handling mechanism to the resident via multiple channels like website, call center, mobile app, SMS, physical center, etc.

4. This issues under approval of the Competent Authority.

Director (A&V)

To,

National Payments Corporation of India (NPCI)

Copy: for information to

(i) Department of Revenue, Ministry of Finance, Government of India
(ii) Reserve Bank of India
(iii) Securities Exchange Board of India
(iv) Insurance Regulatory and Development Authority of India
(v) Pension Fund Regulatory and Development Authority

से.के. K-11022/632/2017-यूआईडीएआई(ऑथ-II)/८८८३
भारत सरकार
भारतीय विशिष्ट पहचान प्राधिकरण
अधिप्रमाणन एवं सत्यापन अनुभाग

यूआईडीएआई मुख्यालय भवन,
तृतीय तल, बंगला साहिब रोड,
काली मंदिर के पीछे, गोल मार्किट,
नई दिल्ली - 110001

दिनांक: 27.03.2023

CIRCULAR NO. 02 OF 2023

To

All AUAs/KUAs/Sub-AUAs/Sub-KUAs

Sub:- Renewal of License Fees of Sub-AUAs/Sub-KUAs.

In continuation to the UIDAI Circular Number.-1 of 2021 dated 09.02.2021 on the subject cited above, all the Sub-AUAs/Sub-KUAs are directed to deposit License fees of Rs. 3 Lakh along with GST @18%, which will be valid for 2 years. This renewal of License Fee is applicable on all the Sub-AUA/Sub-KUAs which were active on 31st March 2021.

2. Sub-AUA/Sub-KUAs which are on-boarded after 31.03.2021 are required to renew their License Fee before expiry of validity of 2 years.

3. Any delay in renewal of License fees beyond stipulated date i.e. 31st March 2023 will attract late payment charges @1% of License Fee per month or part thereof along with GST @18% thereupon. Further, non-payment of License Fee may lead to immediate suspension of authentication services.

4. It is reiterated that the above mentioned License Fee is non-refundable under any circumstances. Those Sub-AUA/Sub-KUAs who do not agree to the above terms and conditions may surrender their access through their respective AUA/KUA.

5. It may be noted that this License Fee is to be renewed every two years at the prescribed rate to continue access to the Aadhaar Authentication Services. The other terms and conditions mentioned in UIDAI circular 1 of 2021 dated 09.02.2021 regarding Sub-AUA/Sub-KUA License Fee shall remain valid & applicable as before.

(अमित भार्गव)
उप निदेशक

1

INDEX

F.No. HQ-13073/2/2023-AUTH-II HQ (E-10768)/5603
Government of India
Ministry of Electronics and Information Technology
Unique Identification Authority of India
(Authentication and Verification Division)

3rd Floor, UIDAI HQs,
Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi-110001
Dated:31.03.2023

Circular No. 03 of 2023

Subject:- Rationalization of Sub-AUA/Sub-KUA.

Regulations 15 and 16 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021 provide for appointment of Sub-Authentication User Agencies (Sub-AUAs) and Sub-eKYC User Agencies (Sub-KUAs) respectively. UIDAI vide circular No. K-11022/630/2017-UIDAI(Auth-II), dated 09-02-2021 has implemented license fees for Sub-AUAs/Sub-KUAs @ Rs. 3 Lakh (exclusive of applicable taxes) for a period of 02 years applicable w.e.f. 1st April 2021.

2. UIDAI has been receiving requests to consider reducing or waiving off Sub-AUA/Sub-KUA license fees for such government entities which perform miniscule number of transactions for their schemes/services. Hence, in order to simplify and rationalise the government Sub-AUA/Sub-KUA ecosystem and to encourage more government departments to onboard in Aadhaar authentication ecosystem for delivering of their services/benefits, following has been decided by the Competent Authority of UIDAI:

(i) The Central/State Govt. Departments performing less than 50,000 transactions per year to continue availing authentication services through the license keys of their respective AUAs/KUAs (NIC or State AUA/KUA) without paying any license fee to UIDAI. No Sub-AUA/Sub-KUA code will be issued to such Govt. Departments by UIDAI. They may create an internal identifier vis-à-vis their AUA for the purpose of identifying their respective scheme transactions.

INDEX

(ii) Sub-AUAs/Sub-KUAs which are performing more than 1 crore transactions per year are encouraged to become full-fledged AUA/KUA as it will grant them greater control over their respective databases and systems.

(iii) Sub-AUAs/Sub-KUAs which are performing transactions between 50,000 to 1 crore per year may continue on as-is-basis for the time being.

3. This shall come into effect from 1st July, 2023.

(अमित भार्गव)
उप निदेशक

To

(i) All Authentication Service Agencies
(ii) All Requesting Entities (AUAs/KUAs/Sub-AUAs/Sub-KUAs)

Copy for information

(i) All Secretaries (Govt. of India)/Chief Secretaries of all State/Union Territories
(ii) OSD to CEO
(iii) All DDGs(HQs, ROs, Tech Centers)

INDEX

F.No. HQ-13073/1/2023-AUTH-II HQ (E-10767) /5610
Government of India
Ministry of Electronics and Information Technology
Unique Identification Authority of India
(Authentication and Verification Division)

3rd Floor, UIDAI HQs,
Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi-110001
Dated:05.04.2023

Circular No. 04 of 2023

Subject:- Revising License Fee for AUA/KUA based on their transaction volume.

Reference is invited to UIDAI's circular No. K-11022/630/2017-UIDAI(Auth-II), dated 31-05-2017 which introduced license fees to be paid by Authentication User Agencies (AUAs), e-KYC User Agencies(KUAs) w.e.f. 01-06-2017 valid for a period of 2 years, as depicted in the table below:

Category of Entity	Environment	License fees (in Rs.)	Validity
AUA/KUA	Pre-production	5 lakh	3 months
	Production	20 lakh	2 years

2. There has been a demand to review license fees particularly for such entities which do lesser number of authentication transactions and are having small capital structure and may require support in terms of reduced license fee. The same has been reviewed and following has been decided by the competent authority of UIDAI.

(i) The AUAs performing upto 5 lakh transactions per year to be charged at ₹5 lakh for 2 years.

(ii) The AUAs performing 5 lakh to 20 lakh transactions per year to be charged at ₹10 lakh for 2 years.

(iii) The AUAs performing more than 20 lakh transactions per year to be charged at current rate i.e. ₹ 20 lakh for 2 years.

(iv) The newly onboarded AUAs may be granted free of cost access to pre-production environment for first three months. Further, if they move into production within the period of three months of onboarding into pre-production, they will pay full license fee for production environment at prescribed rates wef date of start of pre-production.

INDEX

(v) If the entity fails to move into production within three months of grant of free access to pre-production environment, it will have to pay pre-production license fee of Rs. 5 lakh valid for first three months for the free access period as well as each subsequent renewal. This is to incentivise entities for speedier onboarding as AUA/KUA in production environment.

(vi) The entities will be on-boarded initially on the basis of transaction estimates provided by them and license fees will be charged as per the applicable slab as mentioned above. However, at the time of subsequent renewal if the entity is found to have performed higher number of transactions, then differential amount of license fees of higher slab as mentioned above will be recovered along with interest @18% per annum. Such a provision is warranted in order to enable UIDAI to plan for the infrastructure requirements based on the number of expected authentication transactions. Any wide variation in projected number of authentication transactions may potentially affect the entire authentication ecosystem. Further, if the entity would have performed lesser number of transactions compared to initially submitted transactions estimate, no benefit of lower slab will be admissible. Hence, entities are advised to provide their estimates carefully.

3. This shall come into effect from 1st July, 2023.

(अमित भार्गव)
उप निदेशक

To

(i) All Authentication Service Agencies,
(ii) All Authentication User Agencies/eKYC User Agencies

Copy for information

(i) All Secretaries (Govt. of India)/Chief Secretaries of all State/Union Territories
(ii) OSD to the CEO, UIDAI
(iii) All DDGs(HQs, ROs, Tech Centers)

INDEX

F. No. K-11022/632/2017-UIDAI (Auth II)/ 5649

Government of India
Ministry of Electronics & Information Technology
Unique Identification Authority of India
(Authentication & Verification Division)

3rd Floor, UIDAI HQ Building
Bangla Sahib Road, Behind Kali Mandi,
Gole Market, New Delhi – 110001
Date :06-04-2023

Circular No. 05 of 2023

Sub: Chargeability of FMR-FIR auth. error code

A new security mechanism of FMR-FIR modality has been rolled-out by UIDAI for Aadhaar based fingerprint authentication, making Aadhaar authentication transactions more robust and secure by using combination of both finger minutia and finger image to check the liveliness of the finger print captured. All the Authentication User Agencies (AUAs) have migrated to this new FMR-FIR modality w.e.f. 28.02.2023. To differentiate the transactions in FMR-FIR modality, new authentication error codes of '320' and '589' have been introduced:

Error Code	Error Description
320	FMR+FIR not present in the Request
589	FMR+FIR not allowed as per License

2. Further, UIDAI vide notification No.K-11022/632/2019/Auth-UIDAI (No. 1 of 2021) dated 14.10.2021 has notified the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021. As per Regulation 2(1) of the ibid Regulations, each failed, but chargeable Aadhaar eKYC transaction or Yes/No authentication transaction shall be charged @ Rs. 0.50 (including applicable taxes) per such transaction from requesting entities.

3. In this regard, as decided by the competent authority of UIDAI, it is informed that any failed transaction due to error code 320 & 589 will now be chargeable w.e.f. 01.05.2023 at prescribed rate.

4. This issues with approval of the Competent Authority

(Amit Bhargav)
Deputy Director

To,
All AUAs/KUAs

INDEX

HQ-13062/4/2021-Auth-II HQ-Part (1) / (E-6071) / 6056

Government of India
Ministry of Electronics & Information Technology
Unique Identification Authority of India
(Authentication & Verification Division)

3rd Floor, UIDAI HQ Building
Bangla Sahib Road, Behind Kali Mandi,
Gole Market, New Delhi 110001
Date : 03-05-2023

CIRCULAR No. 06 OF 2023

Sub: Pricing of Aadhaar authentication transactions.

Ref.: (i) UIDAI Gazette Notification No.K-11022/632/2019/Auth-UIDAI (No. 1 of 2019), dated 07-03-2019 notifying the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2019.
(ii) UIDAI Circular No. 4 of 2019 (K-11022/632/2017-UIDAI(Auth II) dated 23-04-2019.
(iii) UIDAI Circular No. 4 of 2020 (K-11022/632/2017-UIDAI(Auth II) dated 14-07-2020.

*****

UIDAI vide Gazette Notification No. K-11022/632/2019/Auth-UIDAI (No. 1 of 2021) dated 14.10.2021 has notified the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021, amended vide Gazette Notification No. HQ-13062/4/2021-AUTH-II (No. 2 of 2023) dated 24-02-2023 notifying The Aadhaar (Pricing of Aadhaar Authentication Services) (First Amendment) Regulations, 2023.

2. In pursuance of the provisions of the Regulation cited in para (1) above, following is conveyed:

(a) Authentication transactions which fail due to UIDAI specific error will not be charged to the requesting entities. The details of error codes not to be charged are enclosed in Annexure I. All other error codes apart from mentioned in Annexure-I shall be charged as per prescribed rates.

(b) Biometric transactions failure (error Code 300) up to 12% shall be waived off for charging. However, this limit is subject to revision based on periodic review.

(c) Transactions where the response is not provided by UIDAI's CIDR within 10 seconds will not be charged.

(d) Transaction charges invoice will be generated every month applicable upon authentication services rendered from 01st April'23.

(e) All disputes/ grievances related to billing of authentication charges to be submitted before Director (Authentication and Verification Division) along with relevant documents for resolution/ redressal.

Contd., on page 2

3. The above mentioned are in addition to the rates, terms and conditions prescribed vide the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021 dated 14-10-2021 and the Aadhaar (Pricing of Aadhaar Authentication Services) (First Amendment) Regulations, 2023 dated 24-02-2023. Further, this circular is in supersession of UIDAI circulars at reference (ii) and (iii) above and shall come into effect immediately from the date of its issue.

This issues under approval of the Competent Authority.

Encl.: As above.

(Amit Bhargav)
Deputy Director

To,

(i) ASAs/AUAs/KUAs
(ii) All UIDAI Regional Offices

INDEX

Annexure-I

List of Error Codes not to be charged

S.N.	Auth Error Code	Error Description
1	330	Biometrics locked by Aadhaar number holder.
2	331	Aadhaar locked by Aadhaar number holder for all authentications.
3	332	Aadhaar number usage is blocked by Aadhaar number holder.
4	400	Invalid OTP value.
5	430	TOTP usage is not allowed for this aadhaar holder. Please install m-aadhaar and generate TOTP.
6	515	Invalid VID Number in input.
7	517	Expired VID is used as input.
8	532	VID not generated
9	811	Missing biometric data in CIDR for the given Aadhaar Number/Virtual ID.
10	930 to 939	Technical Error
11	950	OTP store related technical error.
12	951	Biometric lock related technical error.
13	980	Unsupported option.
14	995	Aadhaar suspended by competent authority.
15	996	Aadhaar cancelled (Aadhaar is not in authenticable status).
16	997	Aadhaar suspended (Aadhaar is not in authenticable status).
17	998	Invalid Aadhaar Number/Virtual ID.
18	999	Unknown error.
	eKYC Error Code	**Error Description**
19	K-100*	Auth Failure
20	K-200	Resident data currently not available
21	K-515	Invalid VID
22	K-517	Expired VID is used as input.
23	K-545	Resident has opted-out of this service. This feature is not implemented currently.
24	K-571	Technical Error during UIDAI response signing
25	K-955	Technical Failure
26	K-956	Technical Error during PDF generation
27	K-999	Unknown error

*K-100 is Auth related error and the Auth error codes not chargeable in Y/N auth shall not be charged in eKYC also.

(Amit Bhargav)
Deputy Director

INDEX

F. No. 10(22)/2017-EG-II(Vol-I)
Government of India
Ministry of Electronics and Information Technology

Electronics Niketan, 6, CGO Complex
Lodhi Road, New Delhi – 110 003
Dated 19 June 2023

Office Memorandum

Subject: Authentication/verification of Aadhaar

Aadhaar is being used by the Ministries, Departments, secretariats and offices of the Central Government and their entities for the purpose of establishing identity of individuals as a condition for receipt of subsidy, benefit or services for which expenditure is incurred from the Consolidated Fund of India or the State concerned. Further, entities permitted by Central law, such as telecom service providers, banks and Certifying Authorities licensed to issue Electronic Signature Certificates and other entities authorised under section 4(4)(b)(ii) of the Aadhaar (Targeted Delivery of Financial and Other. Subsidies, Benefits and Services) Act, 2016 for the purpose of good governance, social welfare benefits, innovation and spread of knowledge also use Aadhaar.

2. With Aadhaar becoming integral to delivery to residents of subsidies, benefits and services, performance of certain functions mandated by law and, where authorised, for the aforesaid purposes, it has become increasingly necessary that Aadhaar-using entities ensure the authenticity of Aadhaar being used by them, and not rely simply on Aadhaar cards or other secondary sources purporting to represent Aadhaar data.

3. The authenticity of Aadhaar may be established either by online authentication of the identity of the Aadhaar number holder or doing offline verification of the digital signature of UIDAI on the QR code, e-Aadhaar or Aadhaar Paperless Offline e-KYC (XML).

4. Under the Aadhaar (Authentication and Offline Verification) Regulations, 2021, online authentication is available to Requesting Entities appointed by UIDAI. Such authentication may be done through UIDAI's eKYC or Yes/No authentication services, using the fingerprint, iris or face biometrics of the Aadhaar number holder.

5. Offline Verification Seeking Entities may make use of any of the offline verification procedures provided for in the regulations to verify UIDAI's digital signature against—

(a) the secure QR code, which is printed on the Aadhaar Letter issued to residents upon enrolment or the Aadhaar PVC card and may also be scanned by "Aadhaar QR Scanner" application available on Google Play Store and iOS Appstore;

(b) eAadhaar (password-protected electronic copy of Aadhaar), which is downloadable from the UIDAI website or accessible using the mAadhaar app; and

INDEX

(c) Aadhaar Paperless Offline e-KYC (XML) (a secure, sharable document), which is downloadable from the UIDAI website or accessible using the mAadhaar app.

6. In this regard, it is also pertinent that regulation 16C of the said regulations provides that no Offline Verification Seeking Entity shall accept Aadhaar number in physical or electronic form (without authentication) as a proof of identity without first verifying UIDAI's digital signature.

7. For more details, the Headquarters or Regional Offices of UIDAI may be contacted.

8. Against this background, it is advised that suitable directions may be issued to all Aadhaar-using entities under the Ministry/Department/secretariat/office and any State-level counterparts to not accept Aadhaar number in physical or electronic form (without authentication) as a proof of identity without first verifying UIDAI's digital signature, and to carry out online authentication where the Aadhaar-using entity is a Requesting Entity appointed by UIDAI.

19/6/2023

(Kavita Bhatia)
Scientist G
Tel : 011-24364729
Email: kbhatia@meity.gov.in

To:

1. Secretaries to Government of India (as per list)
2. Chairman and Chief Executive Officer, Railway Board
3. Chief Executive Officer, NITI Aayog

Copy to:

Chief Executive Officer, Unique Identification Authority of India

List of addresses

1. Secretary, Department of Administrative Reforms and Public Grievances, 513, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001
2. Secretary, Department of Agriculture Research and Education, First floor, Krishi Bhawan, New Delhi – 110 001
3. Secretary, Department of Biotechnology, 7th floor, Block-2, CGO Complex, Lodhi Road, New Delhi – 110 003
4. Secretary, Department of Commerce, Udyog Bhawan, New Delhi – 110 011
5. Defence Secretary, Department of Defence, 101-A, South Block, New Delhi – 110 001
6. Secretary, Ministry of Development of North Eastern Region, Vigyan Bhawan Annexe, Maulana Azad Road, New Delhi – 110 011
7. Secretary, Department of Drinking Water and Sanitation, C Wing, 4th floor, Paryavaran Bhawan, CGO Complex, Lodhi Road, New Delhi – 110 003
8. Secretary, Department of Atomic Energy, E Block, Raisina Hill, New Delhi – 110 011
9. Secretary, Department of Space, Antariksh Bhavan, New BEL Road, Bangalore – 560 231
10. Secretary, Ministry of Earth Sciences, Mahasagar Bhawan, Block - 12, C.G.O Complex, Lodhi Road, New Delhi – 110 003
11. Secretary, Department of Empowerment of Persons with Disabilities, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
12. Secretary, Department of Fertilizers, A Wing, Shastri Bhawan, New Delhi – 110 001
13. Secretary, Department of Fisheries, Krishi Bhawan, New Delhi – 110 001
14. Secretary, Department of Food and Public Distribution, H Wing, Krishi Bhawan, New Delhi – 110 001
15. Secretary, Ministry of Food Processing Industries, Panchsheel Bhawan, August Kranti Marg, New Delhi – 110 049
16. Home Secretary, Ministry of Home Affairs, North Block, New Delhi - 110 001
17. Secretary, Department of Higher Education, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
18. Secretary, Ministry of Information and Broadcasting, Dr Rajendra Prasad Road, Shastri Bhawan, New Delhi – 110 001
19. Secretary, Department of Legal Affairs, A Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
20. Secretary, Legislative Department, A Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
21. Secretary, Department of Justice, A Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
22. Secretary, Ministry of Micro, Small and Medium Enterprises, Udyog Bhawan, Rafi Marg, New Delhi – 110 011
23. Secretary, Ministry of Mines, A Wing, 3rd floor, Shastri Bhawan, New Delhi – 110 001
24. Secretary, Ministry of Minority Affairs, 11th floor, Paryavaran Bhawan, CGO Complex, Lodhi Road, New Delhi – 110 003
25. Secretary, Ministry of New and Renewable Energy, Block no. 14, CGO Complex, Lodhi Road, New Delhi – 110 003
26. Secretary, Department of Official Language, NDCC-II Bhawan, A Wing, 3rd floor, Jai Singh Marg, New Delhi – 110 001
27. Secretary, Ministry of Panchayati Raj, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001

INDEX

28. Secretary, Department of Pension and Pensioners' Welfare, 514, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001
29. Secretary, Department of Pharmaceuticals, A Wing, Shastri Bhawan, New Delhi – 110 001
30. Secretary, Ministry of Power, 2nd floor, Shram Shakti Bhawan, New Delhi – 110 001
31. Secretary, Department of School Education and Literacy, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
32. Secretary, Department of Science and Technology, Technology Bhawan, New Mehrauli Road, New Delhi – 110 016
33. Secretary, Department of Scientific and Industrial Research, Technology Bhawan, New Mehrauli Road, New Delhi – 110 016
34. Secretary, Ministry of Skill Development and Entrepreneurship, 2nd floor, Shivaji Stadium Annexe, Shaheed Bhagat Singh Marg, New Delhi – 110 001
35. Secretary, Department of Social Justice and Empowerment, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
36. Secretary, Department of Sports, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
37. Secretary, Ministry of Statistics and Programme Implementation, 418, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001
38. Secretary, Department of Water Resources, River Development and Ganga Rejuvenation, Shram Shakti Bhawan, Rafi Marg, New Delhi – 110 001
39. Secretary, Ministry of Women and Child Development, Shastri Bhawan, A Wing, Dr Rajendra Prasad Road, New Delhi – 110 001
40. Secretary, Department of Youth Affairs, Room No. 1, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
41. Secretary, Department of Agriculture and Farmers Welfare, Krishi Bhavan, Dr Rajendra Prasad Road, New Delhi – 110 001
42. Secretary, Ministry of AYUSH, Ayush Bhawan, B Block, GPO Complex, Barapullah Road, INA Colony, New Delhi – 110 023
43. Secretary, Department of Chemicals and Petrochemicals, 236A, A Wing, 2nd floor, Shastri Bhawan, New Delhi – 110 001
44. Secretary, Ministry of Civil Aviation, Rajiv Gandhi Bhawan, Block B, Jor Bagh, Safdarjung Airport Area, New Delhi – 110 003
45. Secretary, Ministry of Coal, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
46. Secretary, Department for Promotion of Industry and Internal Trade, Vanijya Bhawan, New Delhi – 110 011
47. Secretary, Department of Telecommunications, Sanchar Bhawan, 20, Ashoka Road, New Delhi – 110 001
48. Secretary, Department of Posts, Dak Bhawan, Patel Chowk, New Delhi – 110 001
49. Secretary, Department of Consumer Affairs, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
50. Secretary, Ministry of Cooperation, 2nd floor, Atal Akshya Urja Bhawan, Pragati Vihar, New Delhi – 110 003
51. Secretary, Ministry of Corporate Affairs, A Wing, Shastri Bhawan, Rajendra Prasad Road, New Delhi – 110 001
52. Secretary, Ministry of Culture, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
53. Secretary, Ministry of Environment, Forest and Climate Change, Indira Paryavaran Bhawan, Jor Bagh Road, New Delhi – 110 003

INDEX

54. Secretary, Department of Animal Husbandry and Dairying, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
55. Secretary, Department of Health and Family Welfare, A Wing, Nirman Bhavan, New Delhi – 110 011
56. Secretary, Department of Health Research, 1, Red Cross Road, Gokul Nagar, New Delhi – 110 001
57. Secretary, Ministry of Heavy Industries, Udyog Bhawan, New Delhi – 110 001
58. Secretary, Ministry of Housing and Urban Affairs, Nirman Bhawan, C Wing, Dr Maulana Azad Road, New Delhi – 110 011
59. Secretary, Ministry of Labour and Employment, Shram Shakti Bhawan, Rafi Marg, New Delhi – 110 001
60. Secretary, Ministry of Parliamentary Affairs, Parliament House, Sansad Marg, New Delhi – 110 001
61. Secretary, Ministry of Petroleum and Natural Gas, Shastri Bhawan, Rajendra Prasad Road, New Delhi – 110 001
62. Secretary, Ministry of Ports, Shipping and Waterways, Transport Bhavan, 1, Parliament Street, New Delhi – 110 001
63. Secretary, Ministry of Road Transport and Highways, Transport Bhavan, 1, Parliament Street, New Delhi – 110 001
64. Secretary, Department of Rural Development, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
65. Secretary, Department of Land Resources, NBO Building, G Wing, Nirman Bhawan, Dr Maulana Azad Road, New Delhi – 110 011
66. Secretary, Ministry of Steel, Udyog Bhawan, New Delhi – 110 001
67. Secretary, Ministry of Textiles, Udyog Bhawan, New Delhi – 110 001
68. Secretary, Ministry of Tourism, Transport Bhavan, 1, Parliament Street, New Delhi – 110 001
69. Secretary, Ministry of Tribal Affairs, B Wing, Shastri Bhawan, New Delhi – 110 001
70. Secretary, National Security Council Secretariat, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001
71. Secretary, Department of Economic Affairs, North Block, New Delhi - 110 001
72. Secretary, Department of Expenditure, North Block, New Delhi - 110 001
73. Secretary, Department of Revenue, North Block, New Delhi - 110 001
74. Secretary, Department of Financial Services, 3rd floor, Jeevan Deep Building, Parliament Street, New Delhi -1
75. Secretary, Department of Public Enterprises, Block-14, CGO Complex, Lodhi Road, New Delhi
76. Secretary, Department of Investment and Public Asset Management, 4th floor, Block No. 11 CGO Complex, Lodhi Road New Delhi - 110003
77. Foreign Secretary, Ministry of External Affairs, Jawaharlal Neharu Bhawan, New Delhi
78. Secretary, Department of Personnel and Training, North Block, New Delhi - 110 001
79. Secretary, Department of Defence Production, South Block, New Delhi - 110 011
80. Secretary, Department of Ex-servicemen Welfare, South Block, New Delhi - 110 011
81. Secretary, Department of Military Affairs, South Block, New Delhi - 110 011
82. Secretary, Department of Defence Research and Development, DRDO Bhawan, New Delhi - 110 011
83. Secretary to President, President's Secretariat, Rashtrapati Bhawan, Raisina Hill, New Delhi – 110 011
84. Secretary, National Security Council Secretariat, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001

INDEX

F. No. HQ-13083/6/2021-AUTH-II HQ (E-3605)/6754
Government of India
Ministry of Electronics and Information Technology
Unique Identification Authority of India
(Authentication & Verification Division)

UIDAI HQ Building,
Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi - 110001

Dated: 11.07.2023

Circular No.: 07 of 2023

Sub: Availing Aadhaar authentication modalities by Requesting Entities – reg.

UIDAI provides three types of modalities for carrying out Aadhaar-based online authentications namely, Demographic, OTP-based and Biometric-based (Fingerprint/Iris/Face). As per Regulation 4(3) of the Aadhaar (Authentication and Offline Verification) Regulations 2021, any Requesting Entity (RE) can opt for one or more of these authentication modalities for a particular service or business function as per its requirement, including multiple factor authentication for enhanced security.

2. Presently, at the time of initial on-boarding only those authentication modalities are enabled for an RE which it has opted for. Subsequently, additional modalities are extended as and when requested by it as per its requirement. This requires approval from the Competent Authority and adds one more step to the process.

3. In this backdrop, in order to simplify the process and to encourage REs to opt for maximum number of authentication modalities, it has been decided to extend all authentication modalities to all REs. A RE may opt for one or more modalities as per its requirement and the same will be enabled for it. However, for availing these modalities in production environment, REs will be required to confirm their technical preparedness by submitting test transactions under opted modalities (done in pre-production environment) and an IS Audit report from a CERT-In empanelled IS Auditor as per the extant practice.

4. This issues under approval of the Chief Executive Officer.

(Sanjeev Yadav)
Director

To

All ASAs and AUAs/KUAs

INDEX

File no. HQ-13079/55/2021-AUTH-II HQ/6307
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Headquarter
Bangla Sahib Road, Behind Kali Mandir
Gole Market, New Delhi 110 001
Dated 8.8.2023

OFFICE MEMORANDUM

Subject: Clarifications on issues relating to sharing of Aadhaar and related data amongst government departments reg.

In partial modification of the UIDAI OM of even number dated 15.7.22, clarification to query no. 5 has been revised as given below:

Sl. No.	Query	Clarification
5	What should be the mechanism for sharing of Aadhaar and related data between Central Govt. and State Govts. in case the requirement is for the same purpose for which Aadhaar was collected?	It is understood that in many cases, while implementing Central Govt. schemes, the data is collected by the State Govts. In such a scenario, full Aadhaar number can be shared if the State Govt. had collected the data which is now in possession of a Central Govt. Ministry/Department. For example, the data collected in a particular state for a specified purpose like Pradhan Mantri-Fasal Bima Yojana (PM FBY), full Aadhaar number can be shared by Ministry of Agriculture with that State Govt. for that purpose. Similarly, if data has been collected for a centrally sponsored scheme or other scheme/purpose which is implemented/pursued jointly, data can be similarly shared between the Central Govt. and the State Govt. Further, as clarified in the response to query no. 1 above, while a State Govt. can be treated as a single entity for effective formulation of various government schemes and selection of beneficiaries, a separate consent of the beneficiary must be taken

		by the implementing State Govt. department at the time of final delivery of subsidy, benefit and service. Moreover, if the concerned State Govt. wants to utilize same data for some other purpose/ scheme, a separate consent must be taken from the residents by that State Govt.

This issues with the approval of the Competent Authority.

(Sanjeev Yadav)
Director

To,

(i) The Ministries/ Departments of Govt. of India
(ii) The Chief Secretaries of States/UTs

Copy to: For information

Secretary, Ministry of Electronics & Information Technology, Govt. of India.

INDEX

F.No. HQ-13021/l/2021-Auth-I HQ
Government of India
Ministry of Electronics & Information Technology
Unique Identification Authority of India (UIDAI)
Authentication Division

UIDAI Headquarters, Third Floor,
Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi – 110001
Date: 18.09.2023

To
All AUA/KUAs

Sub: Migration of fingerprint L0 registered devices to fingerprint L1 registered devices

Please refer:

i. **UIDAI Letter HQ-13021/1/2021-AUTH-I HQ dated 25.04.2022**
ii. **UIDAI Letter HQ-13021/1/2021-AUTH-I HQ dated 31.05.2022**
iii. **UIDAI Letter HQ-13021/l/2021-Auth-I HQ dated 27.01.2023**

Dear Partners,

Your entity has been appointed as an AUA/KUA by UIDAI for availing the Aadhaar authentication facility for authentication of the residents. UIDAI is committed towards providing the highest quality of service in an efficient and secured manner. To enhance the security levels, UIDAI has taken several security measures to ensure security of transactions and end to end traceability during the authentication process. In this regard, fingerprint devices being used in Aadhaar authentication ecosystem have been upgraded from the currently used fingerprint L0 Registered device to the next generation fingerprint L1 Registered device.

2. UIDAI vide letter HQ-13021/l/2021-Auth-I HQ dated 27.01.2023 has circulated the guidelines for phase out existing fingerprint L0 registered device from Aadhaar authentication ecosystem in phase manner and to provide sufficient period of this transition, the use of all the existing fingerprint L0 Registered device will be discontinued by 30.06.2024 and thereafter only fingerprint L1 Registered device will be allowed to perform Aadhaar based authentication transactions.

List of UIDAI certified fingerprint L1 Registered device are available at UIDAI website.

https://uidai.gov.in/images/resource/L1_RD_Devices.pdf

INDEX

3. Further, UIDAI vide letter HQ-13021/1/2021-AUTH-I HQ dated 25.04.2022 & letter 13043/2/2021 -AUTH-I-HQ dated 31.05.2022 had asked AUA/KUAs to carry out changes required in the application and backend servers to make the AUA/KUA application compatible with fingerprint L1 registered devices and need to be tested thoroughly. However it is noted that some of the AUA/KUAs have not carried out the required changes in the application and tested the application for compatibility with fingerprint L1 registered device in spite of lapse of more than one year.

4. In the view of above, AUA/KUA's are directed to carry out required changes in their AUA/KUA application and in the backend servers to support the fingerprint L1 compliant registered devices for smooth transition from fingerprint L0 registered device to L1 registered device without further delay.

Attached: As above

Dr. Mandeep Singh Lamba
Deputy Director (Auth-I)

INDEX

HQ-13030/1/2022-AUTH-I HQ

भारत सरकार
भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)
अधिप्रमाणन एवं सत्यापन अनुभाग

यूआईडीएआई मुख्यालय भवन,
तृतीय तल, बंगला साहिब रोड,
काली मंदिर के पीछे,
गोल मार्किट, नई दिल्ली - 110001
दिनांक : 10-10-2023

To,

All AUAs/KUAs

Sub: Advisory regarding improving Auth Success rate of OTP failures

Refer Letter No. 13030/1/2021-Auth-I HQ dated 20.01.2023

Dear Madam/Sir,

UIDAI has been providing Aadhaar authentication services using various modalities like Biometric (fingerprint, iris, face), OTP and demographics wherein Aadhaar number, along with other attributes (Demographics/Biometric/ OTP) is submitted to UIDAI's Central Identity Data Repository (CIDR) for verification; the CIDR verifies whether the data submitted matches the data available in CIDR and responds with a "Yes/No" or e-KYC.

2. The OTP API of UIDAI provides the definition of each error code in case of OTP authentication failure. To further explain the cause of the error codes accounting for more than 90% of failures and their remedial action an FAQ were prepared and circulated vide UIDAI letter No-13030/1/2021-Auth-I HQ dated 20.01.2023. However, based on additional observations, revised FAQ for AUA's have been prepared.

This letter supersedes UIDAI OM No-13030/1/2021-Auth-I HQ dated 20.01.2023.

Yours faithfully

(Sanjeev Yadav)
Director

Encl: Annexure-1
Copy for information to:
1. All ROs, UIDAI
2. Tech Centre, UIDAI

INDEX

Annexure-1

FAQs on OTP related Error Codes

1. **Error Code 400 – Invalid OTP value**

This error occurs due to the following reasons;
Reason 1: Less than 6-digit, numeric value is entered by the residents.
Reason 2: Wrong numeric value (OTP) is entered.
Reason 3: Alphabets ranging from a-z are mistakenly entered.
Reason 4: Special character like #,%,$,&,!,*,?,",/,=,+, etc. are entered.
Reason 5: If there is no waiting time set (for re-send OTP option) at AUA or Sub-AUA application end, application allowing to generate multiple OTP in a short time spam, Failures with error-400 will be more.

Preventive Action: AUA has to develop applications where in only 6-digit numeric value will be accepted so as to overcome this error. Please extend the waiting time for OTP resend option to minimum 1 minute (60 sec-120 sec) in AUA/Sub-AUA applications. Submit OTP button should remain disabled till the time OTP API response has been received at the AUA application which will minimize the input of wrong OTP.

2. **Error Code 402 - "txn" value did not match with "txn" value of Request OTP API**

This error occurs due to the following reasons:
Reason 1: Due to low internet connectivity at AUA/KUA side. This can be checked from the transactional logs of AUA/KUA.
Reason 2: Due to low internet connectivity at ASA side. This can be checked from transactional logs of ASA.
Reason 3: For OTP based transactions, if the "txn" value of Auth/KYC request is not matching with the "txn" value of request OTP API then Authentication transaction will be declined with error-402.

Preventive Action: AUA have to make sure to have full internet connectivity and to resolve it, transactional logs of AUA/KUA and ASA may be checked. Please check the transaction ID setting at AUA end, txn value should be same to initiate OTP and validate OTP request.

For example If OTP txn. id is 123456 then OTP based Auth txn id should be 123456 and OTP based KYC txn id should be UKC:123456

3. **Error Code 403 - Maximum number of attempts for OTP match is exceeded or OTP is not generated. Please generate a fresh OTP and try to authenticate again**

This error occurs due to the following reasons;
Reason 1: If wrong value is entered more than 3 times for submission.

INDEX

Reason 2: If Refresh button is used multiple times before submission.
Reason 3: If internet connectivity is low due to which OTP is not generated within the specific time period but user is trying to validate with any 6 digit number.
Reason 4: If Back button is used during the transaction, it may lead to commencement of new session in the existing session and hence, authentication will fail.

Preventive Action: Session should not be refreshed and Close/Back button should be disabled during the transaction. Enter OTP option should get enabled once OTP response has been received from UIDAI. In case Refresh/Back button is selected, the application should logout. Please don't allow AUA application to submit OTP with blank value or with any other value if OTP response (from OTP API) is not received for that particular transaction

4. Error Code 579 - OTP usage not allowed as per license

Reason: This error occurs when the entity doesn't have the approval related to OTP modality for performing Aadhaar authentication.

Preventive Action: The entity has to ensure whether they have sought approval for the OTP modality. If OTP modality is not active, AUA have to apply to UIDAI for activation of OTP modality.

5. Error Code 740 - Missing OTP data as specified in "Uses"

This error occurs due to the following reasons;
Reason 1: If the OTP field is left blank.
Reason 2: If complete 6-digit numeric value is not entered for submission.

Preventive Action: The OTP field can't be left blank and complete 6-digit numeric value has to be entered for submission. AUA shall make changes in the application wherein, Submit button should not be active till 6 numeric digits are fed.

6. Error Code 952 - OTP Flooding error

Reason: If multiple OTP requests initiated by the same resident in a short span of time (more than 1 OTP generation in 30 sec) 952 error will occur.

Preventive Action: Please do not allow the AUA application to generate two OTP requests within duration of 30 seconds. Please extend the waiting time for OTP resend option to minimum 1 minute (60 sec-120 sec) in AUA/Sub-AUA applications.

INDEX

7. **Error Code 953 - Exceeded Maximum OTP generation Limit. Max OTP generation limit is 5 (without submitting).**

   Reason: If resident generated 5 OTPs continuously in 30 minutes and have not submitted the OTP for validation, then the 6th attempt will be failed with error 953. OTP Generation will be blocked for certain duration (for 30 min) after exceeding the Max OTP generation limit.

   Preventive Action: If error-953 comes after "Exceeded Maximum OTP generation Limit" by the resident, please populate/notify a detailed error message as mentioned above. This will prevent resident to generate the OTP for next 30 minutes.

8. **Error Code 111 - Aadhaar number does not have mobile number.**

   Reason: If there is no mobile number linked to the Aadhaar.

   Preventive Action: A static message/notification can be populated in AUA application/portal/website that "Aadhaar holder should have registered mobile number updated against their Aadhaar". For resident awareness and to avoid these OTP API failures, this message can be populated in AUA website or portal (on OTP generation page). If still resident triggering OTP and getting error-111 due to non availability of mobile in his/her Aadhaar, AUA can notify with the clear error message that "Aadhaar number does not have mobile number, to update the mobile no. in Aadhaar please visit nearest Enrollment center.

In case of any issue, AUA may contact auth-support at authsupport@uidai.gov.in

F.No. HQ-13062/4/2021-AUTH-II HQ (E-3235) /8271
Unique Identification Authority of India
(Authentication & Verification Division)

UIDAI Head Office, Bangla Sahib Road
Behind Kali Mandir, Gole Market, New Delhi – 110 001
Dated:16-01-2024

CIRCULAR NO. 01 OF 2024

Sub: Revision of fees for performance of authentication transactions by AUAs/KUAs other than TSPs.

Ref.:(i) UIDAI Gazette Notification No. K-11022/632/2019/Auth-UIDAI (No. 1 of 2021) dated 14.10.2021 notifying the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021.

(ii) UIDAI Gazette Notification F. No. HQ-13073/1/2020-AUTH.II-HQ(E).— dated 29.9.2023 notifying the Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023.

(iii) UIDAI Circular No. 6 of 2023 (HQ-13062/4/2021-Auth-II HQ-Part (1) / (E-6071) /6058) dated 3.05.2023.

*****

UIDAI vide Gazette Notification No. K-11022/632/2019/Auth-UIDAI (No. 1 of 2021) dated 14.10.2021 has notified the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021 as superseded vide UIDAI Gazette Notification F. No. HQ-13073/1/2020-AUTH.II-HQ(E).— dated 29.9.2023 notifying the Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023.

2. In pursuance to the provisions under 3(3)(b) of the Regulation dated 29.09.2023 as cited in para 1 above, the fee for performance of authentication shall, upon completion of every period of twenty-four calendar months from the end of the calendar month in which the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021 came into force, stand revised in proportion to the ratio of the Consumer Price Index for the calendar month at the end of such period to that for the calendar month in which the said regulations came into force, rounded off to the nearest ten paise.

3. Accordingly following is conveyed :

(a) Fees payable by requesting entities is revised with effect from 1.11.2023 in proportion to the ratio of CPI (Combined) for October 2021 (165.50) to that for October 2023 (185.30), which works out to a percentage increase of 11.96%, rounded off to the nearest 10 paise.

Contd.. on page 2

INDEX

(b) The existing rates applicable upto 31.10.2023 and the revised rates applicable from 1.11.2023 are as under:

Authentication type	Category of requesting entity	Existing rate (₹) (inclusive of taxes) upto 31.10.2023	Revised rate (₹) (inclusive of taxes) w.e.f. 1.11.2023
Yes/No	All (AUA, sub-AUA, KUA and sub-KUA)	0.50	0.60
eKYC	KUA and sub-KUA other than TSP	(a) For successful authentication transaction: 3.00 (b) For failed authentication transaction: 0.50	(a) For successful authentication transaction: 3.40 (b) For failed authentication transaction: 0.60

4. The above mentioned are in revision to the rates prescribed under Regulation 3(1) and 3(2) of UIDAI Gazette Notification F. No. HQ-13073/1/2020-AUTH.II-HQ(E).— dated 29.9.2023 notifying the Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023. The other terms and conditions prescribed vide above regulation remains same.

This issues under approval of the Competent Authority.

(Manish Bhardwaj)
Deputy Director General (A&V)

INDEX

F.No. HQ-13062/4/2021-AUTH-II HQ (E-3235) / 8272

Unique Identification Authority of India
(Authentication & Verification Division)

UIDAI Head Office, Bangla Sahib Road
Behind Kali Mandir, Gole Market, New Delhi – 110 001
Dated:16-01-2024

CIRCULAR NO. 02 OF 2024

Sub: Revision of fees for performance of authentication transactions by TSPs.

Ref.:(i) UIDAI Gazette Notification No. K-11022/632/2019/Auth-UIDAI (No. 1 of 2021) dated 14.10.2021 notifying the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021.

(ii) UIDAI Gazette Notification F. No. HQ-13073/1/2020-AUTH.II-HQ(E).— dated 29.9.2023 notifying the Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023.

(iii) UIDAI Circular No. 6 of 2023 (HQ-13062/4/2021-Auth-II HQ-Part (1) / (E-6071)/6058) dated 3.05.2023.

*****

UIDAI vide Gazette Notification No. K-11022/632/2019/Auth-UIDAI (No. 1 of 2021) dated 14.10.2021 has notified the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021 as superseded vide UIDAI Gazette Notification F. No. HQ-13073/1/2020-AUTH.II-HQ(E).— dated 29.9.2023 notifying the Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023.

2. In pursuance to the provisions under 3(3)(b) of the Regulation dated 29.09.2023 as cited in para 1 above, the fee for performance of authentication shall, upon completion of every period of twenty-four calendar months from the end of the calendar month in which the Aadhaar (Pricing of Aadhaar Authentication Services) Regulations, 2021 came into force, stand revised in proportion to the ratio of the Consumer Price Index for the calendar month at the end of such period to that for the calendar month in which the said regulations came into force, rounded off to the nearest ten paise.

3. Accordingly following is conveyed :

(a) Fees payable by requesting entities is revised with effect from 1.11.2023 in proportion to the ratio of CPI (Combined) for October 2021 (165.50) to that for October 2023 (185.30), which works out to a percentage increase of 11.96%, rounded off to the nearest 10 paise.

(b) The existing rates applicable upto 31.10.2023 and the revised rates applicable from 1.11.2023 are as under:

Contd.. on page 2

INDEX

Authentication type	Existing rate (₹) (inclusive of taxes) upto 31.10.2023	Revised rate (₹) (inclusive of taxes) w.e.f. 1.11.2023
Yes/No	0.50	0.60
eKYC	(a) For successful authentication transaction: 1.00 (b) For failed authentication transaction: 0.50	(a) For successful authentication transaction: 1.00 (b) For failed authentication transaction: 0.60

4. The above mentioned are in revision to the rates prescribed under Regulation 3(1) and 3(2) of UIDAI Gazette Notification F. No. HQ-13073/1/2020-AUTH.II-HQ(E).— dated 29.9.2023 notifying the Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023. The other terms and conditions prescribed vide above regulation remains same.

This issue under approval of the Competent Authority.

(Manish Bhardwaj)
Deputy Director General(A&V)

INDEX

-F. No. HQ-13065/1/2022-AUTH-II HQ/
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office
Bangla Sahib Road, Behind Kali Mandir
Gole Market, New Delhi – 110 001
Dated 23 April 2024

To:

All Aadhaar User Agencies (AUAs) and e-KYC User Agencies (KUAs)

Subject: Clarification regarding usage of Aadhaar as proof of date of birth — regarding

Madam/sir,

Please refer to UIDAI's Circular No. 08 of 2023, dated 22.12.2023, regarding acceptance of Aadhaar as a proof of date of birth. It also drew attention to the contents of UIDAI OM F. no. 4(4)/57/186/2016-E&U-pt-II, dated 20.12.2018 (copy enclosed), on the above subject.

2. The said communications brought out that Aadhaar is intended to serve as a proof of identity, when used with authentication. They further highlighted that while the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") mentions that Aadhaar may be accepted for establishing identity in the manner specified by regulations, the same is silent with regard to its acceptance as proof of date of birth; therefore, in the event of dispute regarding correctness of date of birth in Aadhaar, the burden of proof lies with the Aadhaar number holder. In view of this and certain High Court judgements, they clarified that an Aadhaar number can be used for establishing identity of an individual subject to authentication; however, in itself, it is not a proof of date of birth.

3. Subsequently, UIDAI has received queries regarding use of Aadhaar for purposes relating to establishing the date of birth. In this regard, the undersigned is directed to hereby clarify as under:

(a) While the Aadhaar Act and regulations made by UIDAI there under are silent regarding use of Aadhaar for purposes relating to establishing the date of birth, the same provide for the collection, updating and maintenance of biometric information and demographic information including date of birth, sharing of the same with AUAs/KUAs by way of a response to an authentication query, and making of regulations in this regard. Accordingly, UIDAI has made regulations and has laid down procedure regarding the said matters.

(b) As per the same, the individual concerned submits supporting documents, or otherwise discloses information as per laid down procedure, regarding the date of birth as claimed by him/her at the time of enrolment/update.

INDEX

(c) As such, it is open to AUAs/KUAs to take a view on use of Aadhaar for purposes relating to establishing the date of birth.

4. This issues with the approval of competent authority.

Yours faithfully,

Encl.: as above

(Sanjeev Yadav)
Director
Tel: 011-23478609
Email: dir1.auth-hq@uidai.net.in

Copy to:

All Deputy Directors General, UIDAI

F. no. 13021/1/2021-AUTH-I HQ
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office
Bangla Sahib Road, Behind Kali Mandir
Gole Market, New Delhi – 110001
Dated 28 June 2024

To,

All AUA/KUAs, ASAs, Biometric device vendors in Aadhaar authentication ecosystem

Subject: Extension of deadline for sunset of existing L0 Fingerprint Registered Devices deployed in Aadhaar authentication ecosystem

Sir/Madam,

Reference is drawn to UIDAI letter no. HQ-13021/1/2021-Auth-I HQ, dated 25.04.2022 and 31.05.2022, letter no. HQ-13023/1/2020-Auth-I HQ/2084, dated 20.6.2022 and 23.12.2022 and letter no. HQ-13021/1/2021-Auth-I HQ, dated 27.1.2023, regarding complete migration of L0 Fingerprint Registered Devices to L1 Fingerprint Registered Devices.

2. UIDAI is committed towards providing the highest quality of service in an efficient and secured manner. To enhance the security levels, UIDAI has taken several security measures to ensure security of transactions and end to end traceability during the authentication process and as a step towards improving this UIDAI has launched L1 fingerprint registered devices.

3. UIDAI, *vide* its letter no. HQ-13021/1/2021-Auth-1 HQ, dated 31.05.2022, has asked all AUA/KUA to identify the L0 Fingerprint Registered Devices and to replace these devices with L1 Fingerprint Registered Devices in Aadhaar ecosystem. Also, UIDAI vide letter no. HQ-13021/1/2021-Auth-1 HQ, dated 20.6.2022 have shared the list of L0 Fingerprint Registered Devices whose Public Device Certificate (PDC) validity is already over and were not re-certified for new PDC's. Requesting entities (RE's) were asked to phase out these devices, as these devices are less secure and have less authentication success rate.

4. In view of aforesaid, the timelines for hot listing following devices is as under:

Sr No	Device Vendor	Model ID	Date of Hot listing
1	M/s Evolute Systems Pvt Ltd	IDENTI5 with MSO1300E2	31.07.2024
2	M/s Evolute Systems Pvt Ltd	IMPRESS	31.07.2024
3	M/s Evolute Systems Pvt Ltd	LILY	31.07.2024
4	M/s Maestro Electronics	SCRIPT	31.07.2024
5	M/s Smart Chip India Pvt Ltd	MSO1300E1.0SW	31.07.2024

INDEX

6	M/s Next Biometrics Solutions Pvt Ltd	NB-3023-U-UID	31.07.2024
7	M/s Tatvik Biosystems Pvt Ltd	TMF20	31.07.2024

5. UIDAI recognizes the importance of a smooth and efficient transition to L1 Fingerprint Registered Devices. In order to facilitate successful migration for all RE's, it has been decided that the sunset of L0 Fingerprint Registered Devices (except above list) will be extended till 30.9.2024. It is requested to take precautionary measures to complete the migration process.

6. This issues with the approval of competent authority.

28.06.24

(Pratik Choudhary)
Deputy Director
Tel.: 011-23478608
Email: dd1.auth-hq@uidai.net.in

Copy for information to:

1. DDG (All RO)
2. DDG (Technology Centre)

28.06.24

(Pratik Choudhary)
Deputy Director

INDEX

HQ-16031/1/2021-EU-I-HQ

I/35258/2024

F. No. HQ-16031/1/2021-EU-I-HQ
Unique Identification Authority of India (UIDAI)
(Enrolment and Update I-Division)
*****

7th floor, UIDAI Head Office
Behind Kali Mandir, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated 1st July 2024

Office Memorandum no. 2 of 2024

Subject: Revised specifications of Mobile & Tablet based Child Enrolment Lite Client (CELC) - reg.

In order to cope with the technological advancements at hardware and software level and in accordance with UIDAI's security policies, competent authority has approved the revised specifications of Child Enrolment Lite Client (CELC).

2. System Integrators (SIs) and vendors are required to get the Mobile & Tablet based CELC kit along with single Fingerprint/Iris scanner devices, tested at UIDAI Regional Offices/Tech Centre for interoperability with the latest UIDAI's CELC application.

3. Regional Offices shall inform the Registrars to procure Mobile/Tablet/ Biometric device as per the latest specifications. Registrars can procure devices with higher/upgraded specification based on the local requirement and availability through GeM portal.

4. The revised specifications (enclosed), supersedes the existing CELC specifications issued vide Circular No. 4(4)/57/50/2011-Vol II dated 04.02.2021 and HQ-16031/1/2021-EU-I-HQ dated 17.12.2021.

5. This is issue with the approval of competent authority.

Encl.: as above

(Prabhakaran C R)
Dy. Director (E&U-I)

To:
1. All UIDAI Regional Offices and Tech Centre
2. All Registrars /EA.
3. All System Integrators/OEMs
4. Guard file

INDEX

SPECIFICATION FOR MOBILE & TABLET based on CHILD ENROLMENT LITE CLIENT (CELC)

S. No.	Name/Description	Mobile Specifications	Mobile Properties	Tablet Specifications	Tablet Properties
1	Screen	Minimum 5.5" touch screen	Mandatory	Minimum 7" touch screen	Mandatory
2	Screen Resolution	1280x720 or higher	Mandatory	1280x720or higher	Mandatory
3	Colors Supported	16 Million	Mandatory	16 Million	Mandatory
4	Scratch resistant front screen	Yes. Corning Gorilla Glass 5 preferred	Mandatory	Gorilla Glass	Mandatory
5	Processor speed minimum	2 GHz or higher, 64 bit architecture	Mandatory	2 GHz or higher, 64 bit architecture	Mandatory
6	RAM	4GB or Higher	Mandatory	4GB or Higher	Mandatory
7	Internal Storage	32GB or Higher	Mandatory	32GB or Higher	Mandatory
8	Expandable Storage through micro SD	64 GB or higher	Mandatory	64 GB or higher	Optional
9	GSM SIM card slot	Yes	Mandatory	Yes	Mandatory
10	Rear Camera with auto focus	8 M Pixel or higher	Mandatory	8 M Pixel or higher	Mandatory
11	Front Camera	5 M Pixel or higher	Mandatory	5 M Pixel or higher	Mandatory
12	Camera with LED flash	Yes	Mandatory	Yes	Mandatory
13	Micro USB Port/Type C Port	1	Mandatory	1	Mandatory
14	Support for USB OTG	Yes	Mandatory	Yes	Mandatory
15	Micro USB/Type C host cable	Yes	Mandatory	Yes	Mandatory
16	Connectivity	Wi-Fi IEEE 802.11 b/g/n/ac	Mandatory	Wi-Fi IEEE 802.11 b/g/n/ac	Mandatory

INDEX

17	GPS & AGPS or NavIC facility for capturing the location coordinates	Yes	Mandatory	Yes	Mandatory
18	Additional Charging port	Yes	Optional	Yes	Optional
19	Mobile Data Support	Minimum compliance to 4G LTE or above standards	Mandatory	Minimum compliance to 4G LTE or above standards	Mandatory
20	Battery Capacity	Minimum 5000 mAH	Mandatory	Minimum 5000 mAH	Mandatory
21	Battery Backup Time	Minimum 8 hours	Mandatory	Minimum 8 hours	Mandatory
22	Software Requirements for development support	Android 11.0 or above	Mandatory	Android 11.0 or above	Mandatory
23	SAR Value	Within acceptable limits permitted in India	Mandatory	Within acceptable limits permitted in India	Mandatory
24	Certifications Available	BIS, or any other relevant Indian Certificates	Mandatory	BIS, or any other relevant Indian Certificates	Mandatory
25	Certifications Available	UL	Optional	UL	Optional
26	BIS Registration under CRS of Meity	Yes	Mandatory	Yes	Mandatory
Note: Mobile/Tablets should not be made in China.					

INDEX

Single Finger Print Scanner Registered Device (RD)

II. Group	Name/Description	Specifications	Properties
1	Single Finger Print Scanner Registered Device (L1 Compliant)	Yes	Mandatory
2	Single Finger Print Scanner Registered Device for Aadhaar Authentication with STQC UIDAI certified RD Service	Yes	Mandatory
3	STQC Certified (STQC Certificate for the Registered device must be submitted)	Yes	Mandatory
4	STQC Certificate Number & its validity(L1 compliant)	Yes	Mandatory
5	Connector Cable to connect the Device to Micro USB/Type C Port	Yes	Mandatory
6	Finger Print Device Connectivity	Through Integrated USB 2.0 or higher	Mandatory
7	Finger Print Device Power	Through USB	Mandatory
8	Sample application for Android platform to test sensor/extractor	Yes	Mandatory
Note: (Refer approved **Single Finger Print Scanner Registered Device** on URL https://uidai.gov.in/images/resource/L1_RD_Devices.pdf			

Single Iris Scanner RD device

Note: (Refer approved **Single Iris Scanner RD devices** on URL

https://uidai.gov.in/images/resource/List_of_UIDAI_certified_Iris_device_vendors_01_04_2023.pdf)

INDEX

HQ-16031/1/2021-EU-I-HQ 1/35259/2024

F. No. HQ-16031/1/2021-EU-I-HQ
Unique Identification Authority of India (UIDAI)
(Enrolment and Update I-Division)
7th floor, UIDAI Head Office
Behind Kali Mandir, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated 1st July, 2024

Office Memorandum no. 1 of 2024

Subject: Revised specifications of Aadhaar Enrolment Kit (AEK) - reg.

In order to cope with the technological advancements at hardware and software level and in accordance with UIDAI's security policies, competent authority has approved the revised specifications of Aadhaar Enrolment Kit (AEK) functioning under Enrolment Client Multiple Platform (ECMP), Update Client Lite (UCL) and Universal Client (UC).

2. All the components/devices as mentioned in the revised specification (enclosed) shall constitute the AEK for ECMP and UC. However, Slap scanner and Dual Iris scanner do not form a part of the AEK for UCL.

3. As part of revised specifications, the System Integrator (SIs)/OEMs of Biometric Devices (Slap/Iris Scanner/Single Iris Scanner/Camera) shall provide following to the Technology Centre, Bengaluru:
   a. Standard drivers for the devices compatible with Windows 11 professional or higher;
   b. SDK supporting Java and .Net for Windows drivers at (a);
   c. VDMs with source code based on the publicly available drivers and SDK versions.

4. System Integrators (SIs) and vendors are required to get the Kit tested at UIDAI Regional Offices/Tech Centre for interoperability with the latest UIDAI's enrolment application as per the existing process.

5. Regional Offices shall inform the Registrars to procure devices as per the latest specifications. Registrars can procure devices with higher/upgraded specification based on the local requirement and availability through GeM portal.

6. The enclosed specifications supersede the existing AEK specifications issued vide Circular No. 4(4)/57/122/2012/UIDAI/Pt dated 31.12.2018.

7. This is issued with the approval of competent authority.

Encl.: as above

(Prabhakaran C R)
Dy. Director (E&U-I)

To
1. All UIDAI Regional Offices and Tech Centre
2. All Registrars
3. All System Integrators/OEMs
4. Guard file

INDEX

Aadhaar Enrolment Kit

Aadhaar enrolment kit consists of a set of hardware devices required to carry out successful Aadhaar enrolments & update. This set of devices comprises of following devices.

I. Laptop/Desktop
II. Monitor
III. Multifunction Device
IV. White screen
V. Focus Light
VI. Surge Protector spike
VII. Iris Scanner
VIII. Camera
IX. Slap scanner
X. Global Navigation Satellite System (GNSS) Device
XI. Single Finger Print RD L1 device
XII. Single Iris Scanner RD device

1. All these devices shall be as per UIDAI's specifications.
2. Biometric devices (Slap/Iris Scanner/Single Iris Scanner/Camera) L0 RD device and Single Finger Print RD L1 device shall be STQC certified.
3. Complete kit warranty shall be for 3 years except White screen, Focus light & surge protector.
4. **During warranty, faulty equipment's shall be replaced/repaired within 7 days.**
5. Aadhaar Enrolment Kit comprising of specific make/model of device shall be UIDAI certified for its working with latest UIDAI's enrolment client (ECMP)
6. AEK vendors to provide Manufacturers Authorization Form (MAF) issued by OEM for warranty support.
7. It is the responsibility of the AEK vendor/OEM to provide Standard drivers, java and .net supporting SDK, **digitally signed VDM** with source code based on the publicly available drivers & SDK versions and on demand support for the devices which are part of the AEK.
8. OEMs to support UIDAI for Forensic analysis in case of any requirement or need arises

Aadhaar Enrolment Kit

Minimum Specification of Aadhaar Enrolment Equipment

Item S.1.1. – Laptop

Specification	Details
Machine Form Factor	Laptop
CPU	4 Core processor or higher with minimum Frequency 4.0 GHz or higher and 10 MB Cache or higher
Display	Minimum 14" HD Anti-Glare (16:9)
Display type	LED
Connectivity	Wi-Fi (IEEE 802.11b/g/n/ac) and Ethernet (10/1000 Base-T)
MEMORY	Min. 16-GB DDR4RAM or higher expandable up to 32-GB or higher with 1 DIMM SLOT FREE
Solid-State Drive (SSD)	Minimum 512GB SSD
Input/output Ports	One HDMI – minimum
	Two(VGA/ DP Port/Type C/HDMI) port with Display Transfer feature
	Dedicated Minimum 3 USB 2.0 port*
	One Ethernet (RJ-45)
Battery Backup	6hrs backup time in case of laptop
Chipset	System-on-a-Chip
Graphics	Integrated Graphics
Keyboard	Integrated for laptop sized (Minimum 84 Keys) Windows compatible Spill-resistant keyword
Touchpad	Wide Touchpad below keyboard for laptop
Preloaded OS	Windows 11 professional or higher (Standard and Home edition of windows are not allowed)
Certification	BIS,or any other relevant Indian Certificates
ACCESSORIES	*USB Hub with multiple USB connections (enabling 5 devices plug-in through USB port)*, Laptop carrying case
WARRANTY	3 years comprehensive onsite-warranty including Battery and power adapter
ANTI-VIRUS	Reputed Antivirus/EDR software with regular signature updates
TPM	System should support Trusted Platform Module (TPM) version 2.0 or higher version

Aadhaar Enrolment Kit

Item S.1.1.1 – Desktop

Specification	Details
Machine Form Factor	Desktop(Small form Factor)
CPU	4 Core processor or higher with minimum Frequency 4.0 Ghz or higher and 10 MB Cache or higher
MEMORY	Min. 16-GB DDR4RAM or higher expandable up to 32-GB or higher with 1 DIMM SLOT FREE
Connectivity	Ethernet (10/1000 Base-T)
Solid-State Drive (SSD)	Minimum 512GB SSD
Input/output Ports	Min 1 HDMI
	One (VGA/ DP Port/Type C) port with Display Transfer feature supported by Monitor
	Dedicated Minimum 5 USB 2.0 port
	One Ethernet (RJ-45)
Battery Backup	0.5KVA UPS with 30 min backup time For desktop
Chipset	Integrated with CPU or equivalent
Graphics	Integrated Graphics
Keyboard	(Minimum 104 Keys) Windows compatible Spill-resistant keyword
Touchpad	Optical USB mouse
Preloaded OS	Windows 11 professional or higher (Standard and Home edition of windows are not allowed)
Certification	BIS, or any other relevant Indian Certificates
WARRANTY	3 years comprehensive onsite-warranty
ANTI-VIRUS	Reputed Antivirus/EDR software with regular signature updates(Licensed version required)
TPM	System should support Trusted Platform Module (TPM) version 2.0or higher version

Aadhaar Enrolment Kit

Item S.1.2. - Monitor

Specification	Details
Size	15-16 inch or higher
Type	LED
Resolution	1024 x 768 or above
Note: One additional Monitor with Desktop & Laptop - One for Operator view and other for applicant of enrolment and update view	

Item S.1.3. – Multi Functional Device (MFD)

Specification	Details
Function	PRINTCOPY SCAN (COLOR)
DUTY CYCLE IN PAGES	3000 PAGES per month
Print Speed PPM – BLACK(A4)	18 PPM or better
Resolution	600 X 600 DPI
Printing Technology	Ink Tank /laser
Custom media size	A4
Standard operating system supported	Compatible with Windows 11 professional or higher
Scan resolution	600 X 600 DPI OPTICAL
Bit/color depth	24 BITS
Copy speed	18 CPM or better
Copy resolution	600 X 600 DPI
Scan file format	Minimum PDF,JPEG,
BIS Registration under CRS of MeitY	Yes
Onsite OEM Warranty	Minimum 3 years

Aadhaar Enrolment Kit

Item S.1.4. – White Screen

Specification	Details
Size	4 X 5 ft Stand mountable / wall mountable
Accessories	Stand
Non-Reflecting	Yes
Opaque	Yes

Item S.1.5. – Focus Light

Specification	Details
Type	LED, minimum 5 W
Accessories	Stand, 2Mrts Wire and on/off Switch near the operator

Item S.1.6. – Surge Protector Spike

Specification	Details
General	6 nos. of 5A sockets (4 Indian style + 2 International Style), Fuse, on/off Switch and ISO mark

Aadhaar Enrolment Kit

Item S.2.1 – Iris Device Specification

Specification	**Stationary (mounted: wall, tripod or stand)[1]**	**Hand_held[2]**	**Hand-held with alignment aid[3]**
Standard compliance for image capture	ISO/IEC 19497-6 (2005 or preferable2011 version)		
Iris Diameter (In pixel)	> 190		
Spatial Resolution Pixel Resolution	> 60% @ 4.0 Lp/mm > =18 Pixels/mm		
# of simultaneous captured	2		
eyes[4]			
Viewfinder	External	Internal	External or Internal
Capture distance	> 750 mm	> 50mm	> 20 mm
Capture volume (width/height/depth)	>250x500x500mm	> 20x15x12mm	> 20x15x12mm
Exposure time	< 15ms	< 33ms	< 33ms
Imaging wavelength	700-900 nm		
Spectral Spread	Power in any 100nm band > 35% of total power		
Scan type	Progressive		
Image margins	Left & right: 0.50x iris diameter, Top & bottom: 0.25x iris diameter		
Pixel depth	> 8 bits/pixel		
Image evaluation frame rate	>= 7 frames/sec, continuous image capture		
Capture mode	Auto capture with built-in quality check (incorporates NIST quality considerations)		
Sensor signal to noise ration	> 40 DB		
Connectivity[5]	USB 2 or higher, USB-IF certified or Networked (TCP/IP)	USB 2 or higher, USB-IF certified	

INDEX

Aadhaar Enrolment Kit

Power	USB or independent PS		
Weight	NA	< 1 kg	< 1 kg
Dimension	<300 x 100 x 300mm	< 220 x 200 x 100 mm	< 220 x 200 x 100 mm
Operating temperature	0-49C		
Humidity	10 - 90% non-condensing		
Durability/Shock	IP54		
Safety Standard	Exempt Group per IEC 62471:2006-07		
Standards	FCC Class A, RoHS		
Liveness	Liveness detection compliance as per IEEE Std 2790™-2020 & ISO/IEC 30107-3		
Software AP	Compliant with latest UIDAI Device Capture API Specifications. Windows 11 Professional VDM ready certified by UIDAI		
[1]Stationary: Any capture process where the device is stationary and the subject is required to position and rest himself/herself [2]Handheld: Operator operates and holds the camera and the subject is stationary. [3]Alignment aid: Camera has mechanical fixture for alignment. Optical viewfinder is not considered alignment aid. [4]Considered simultaneous if second eye is captured within 2 seconds of first eye done without moving the device. [5]Total of only 1 USB port will be available for connectivity and power			
Security – Digital Signature(Preferably at firmware level)			

Item S.2.2 – Camera

Specification	Details
Standard compliance for image capture	ISO/ IEC 19794-5
Capture Mode	Plain live capture
Image Quality	Full Frontal (0x01) as per ISO/IEC 19794-5
Minimum Resolution	1920x1080
Capture Mode	Manual Capture with Auto Focus and Auto Lighting Adjustment

Aadhaar Enrolment Kit

Sensor	>2 Mega Pixel Native
Connectivity[6]	High Speed USB 2.0 or higher, USB-IF certified
Lens	Fixed, SLR
Power	Through USB/Independent PS/Lithium Ion
Mount	Tripod/Universal Clip
Operating Temperature	0 to 50 degree Celsius
Humidity	10 – 90%
Safety Standard	UL, IS 616:2017
Software API	Compliant with latest UIDAI Device Capture API Specifications
Durability / Shock	IP 54
[6]Total of only 1 USB port will be available for connectivity and power	
Security – Digital Signature(Preferably at firmware level)	

Item S.2.3 – Finger Print Device Specification (Slap Scanner)

Specification	Details
Standard compliance for image capture	ISO/IEC 19794-4
Capture Mode	Plain live scan capture
Image Acquisition Requirements	Setting level 31 or higher (Section 9.1 of Biometric Design Standards for UID Applications V1.0
Image evaluation frame rate	> 3 frames/sec, continuous image capture

Aadhaar Enrolment Kit

<table>
<tr><td>Capture mode</td><td>Auto capture with built-in quality check (incorporates NIST quality considerations)</td></tr>
<tr><td>Capture area</td><td>>76mm x 80mm</td></tr>
<tr><td>Capture sizes</td><td>
<table>
<tr><th rowspan="2">Finger prints</th><th colspan="2">Preferred width</th><th colspan="2">Preferred height</th></tr>
<tr><th>(in)</th><th>(mm)</th><th>(in)</th><th>(mm)</th></tr>
<tr><td>Roll finger</td><td>1.6</td><td>40.6</td><td>1.5</td><td>38.1</td></tr>
<tr><td>Plain Thumb</td><td>1</td><td>25.4</td><td>2</td><td>50.8</td></tr>
<tr><td>Plain 4 fingers (Sequence check)</td><td>3.2</td><td>81.3</td><td>3</td><td>76.2</td></tr>
<tr><td>Plain 4 fingers (identification flat)</td><td>3.2</td><td>81.3</td><td>3</td><td>76.2</td></tr>
</table>
</td></tr>
<tr><td>Pixel depth</td><td>1 to 16 bits (size 1 byte)</td></tr>
<tr><td>Image resolution (horiz) and (vert)</td><td><=scan resolution (horiz) --2 bytes size and <=scan resolution (vert) --2 bytes size</td></tr>
<tr><td>Resolution of final output image</td><td>500 ppi, plus or minus 5 ppi</td></tr>
<tr><td>Signal - to - noise ratio</td><td>Both the ratio of signal to white noise standard deviation and the ratio of signal to black noise standard deviation of the digital scanner >= 125</td></tr>
<tr><td>Connectivity[7]</td><td>USB 2.0 or higher, USB-IF certified</td></tr>
<tr><td>Power</td><td>Through USB</td></tr>
<tr><td>Dimension (W X H X D)</td><td><180MM x 180mm x 180mm</td></tr>
<tr><td>Weight</td><td>Maximum 2.5Kg.</td></tr>
<tr><td>Operating temperature</td><td>0 – 50 C</td></tr>
<tr><td>Humidity</td><td>10 – 90% non-condensing</td></tr>
<tr><td>Durability / Shock</td><td>IP 54</td></tr>
</table>

Aadhaar Enrolment Kit

Standards	UL certified (if applicable). Meets ISO 19794-4:2005 Section7 and Annex A certification requirements (IAFIS Appendix F certified).
Software API	Compliant with latest UIDAI Device Capture API Specifications Linux/Windows 64 bit VDM ready certified by UIDAI
Platen Area Hardness	Hardness Test: 6H compliant Tested as per ASTM D3363; RCA Test: 175g, 400 cycles Abrasion test compliant as per ASTM F 2357-04
Liveness	Liveness detection compliance as per IEEE Std 2790™-2020 & ISO/IEC 30107-3
Note: [7]Total of only 1 USB port will be available for connectivity and power	
Security – Digital Signature(Preferably at firmware level)	

Item S.2.4 – GNSS Device

Specification	Details
Environmental Specifications	
Operating temperature	-10 ~ 85°C
Storage temperature	-40 ~ 85°C
Humidity	5% toUp to 95% non-condensing
Water proof	IP54 or higher
GNSS+NavIC Specification	
GNSS Chipset	SIRF Star III/SIRF Star IV GSD4e /Mediatek/u-blox/sky traq *Must support NavIC with other constellation
Frequency	L1&L5 Dual band
Position Accuracy	<5m 3drms
Time Accuracy	15 ns
Channels	>=34 channel + GAGAN SBAS(Preferable)
Acquisition Sensitivity (in –dBm)	-142dBm or better
Tracking Sensitivity (in –dBm)	-156dBM or better
Protocol/Standard support	NMEA 0183 V3.0or latest protocol@ 115200/9600 baud rate, and supports messages: GGA, GSA, GSV, RMC, VTG, GLL,ZDA v2.2
Position fix time	
Hot Start	1-2 sec

INDEX

Aadhaar Enrolment Kit

Warm Start	< 30 sec
Cold Start	< 60 sec
Position Update Rate	>= 1Hz
Electrical characteristics	
Voltage	3.5V ~ 6.5V
Current draw	55-80mA
Other Parameters	
Type of connection and Range	Location and Time/NMEA data transmission to be Wireless with min. 50 m range For Wired min.20 m range
Ensuring Coordinate Accuracy	The coordinate must be captured with over 99% accuracy
Accessories	With all necessary required cables and accessories to connect to the PC/Laptop
Warranty	3 years Comprehensive on-site Warranty
Note: **1.* GNSS receiver should be capable of computing location from NavIC constellation** **2. Total of only 1 USB port shall be available for connectivity and power**	

Item S.2.5 – Single Finger Print Scanner L1 Registered Device (RD)

S. No.	Name/Description	Specifications	Properties
1	Single Finger Print Scanner Registered Device (L1 Compliant)	Yes	Mandatory
2	Single Finger Print Scanner Registered Device for Aadhaar Authentication with STQC UIDAI certified RD Service to the L1 compliant Fingerprint Registered Device	Yes	Mandatory

Aadhaar Enrolment Kit

3	STQC Certified (STQC Certificate for the Registered L1 device must be submitted)	Yes	Mandatory
4	STQC Certificate Number & its validity(L1 compliant)	Yes	Mandatory
5	Connector Cable to connect the Device to Micro USB/Type C Port	Yes	Mandatory
6	Finger Print Device Connectivity	Through Integrated USB 2.0 or higher	Mandatory
7	Finger Print Device Power	Through USB	Mandatory
8	Sample application for Android platform to test sensor/extractor	Yes	Mandatory

Note: (Refer approved **Single Finger Print Scanner Registered Device** devices on UIDAI website)

Item S.2.6 – Single Iris Scanner Registered Device (RD)

Note: (Refer approved **Single Iris Scanner Registered Device** devices on UIDAI website)

SPECIAL TERMS AND & CONDITIONS FOR AADHAAR ENROLMENT KIT

1. Installation & commissioning: Bidder shall provide Remote support Facility for installation of Aadhaar Enrolment Kit
2. Delivery Period: - Bidder shall complete the entire delivery to consignee within 30 days from date of purchase order.
3. Performance bank guarantee – Bidder shall submit the PBG of 10% of the contract value to the purchaser before payment is released
4. Payments: 100 percent of the payment shall be made within 10 days of supply of Aadhaar enrolment kit to consignee after its acceptance & submission of PBG.
5. SLA: Incase failing to replace/repair of faulty equipment's within 7 days (equipment's within warranty), Rs100 penalty per day per equipment till the replacement/repair shall be deducted from PBG.

F. no.: HQ-13021/1/2021-AUTH-I HQ
Unique Identification Authority of India
(Authentication and Verification Division)

3rd Floor, UIDAI Head Office
Bangla Sahib Road, Gole Market, New Delhi – 110001
Dated: 27.09. 2024

To

All Requesting entities/ASAs, Biometric device vendors in Aadhaar Authentication ecosystem

Subject: Phase out of existing L0 Registered Devices from Aadhaar Authentication ecosystem

Reference is invited to UIDAI letter no. HQ-13021/1/2021-Auth-1 HQ, dated 25.04.2022 and 31.05.2022, letter no. HQ-13023/1/2020-Auth-1 HQ/2084, dated 20.6.2022 and 23.12.2022, letter no. HQ-13021/1/2021-Auth-I HQ, dated 27.1.2023 and 28.06.2024 regarding migration of L0 Fingerprint Registered Devices to L1 Fingerprint Registered Devices.

2. UIDAI sent a letter HQ-13021/1/2021-Auth-I HQ dated 28.06.2024 wherein all requesting entities were directed to replace L0 finger print registered devices with L1 Fingerprint Registered Devices in Aadhaar ecosystem by 30.09.2024.

3. UIDAI has already stopped issuing RD certification to L0 Fingerprint Registered Device models. In this regard, series of workshops and handholding meetings were held with all registered device providers and sent multiple intimation to all AUA/KUAs to migrate their devices from L0 Fingerprint Registered Devices to L1 Fingerprint Registered Devices which were at different stages of migration.

4. Registered Device is a critical requirement for enhanced security and privacy in the Aadhaar authentication eco-system. Therefore, it is important to mention that all requesting entities, ASAs and device providers should fulfill the necessary requirements in a time bound manner. However, given the status of preparedness of requesting entities at para 3 above, it has been decided that the sunset of L0 Fingerprint Registered Devices (except models listed at Annexure-1) will be extended till 31.12.2024 to facilitate successful migration for all RE's.

5. Requesting entities are directed to complete the migration of L0 Fingerprint Registered Devices to L1 Fingerprint Registered Devices by 31.12.2024. This extension includes the following conditions:

a) The sunset period for L0 fingerprint devices is extended upto 31-12-2024 (except models listed at Annexure-1).

INDEX

b) Total 19 Nos. L0 fingerprint registered device models, as listed at Annexure-1, will be hot listed on the specified dates.

c) An additional fee may be levied to transactions conducted by using L0 fingerprint registered devices from 01.11.2024 onwards, in accordance with Regulation 3 of the Aadhaar (Payment of fees for performance of Authentication) Regulations, 2023 read with sub-regulation (7) of regulation 12 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021.

d) No white listing of new L0 fingerprint registered devices will be done from 01.10.2024 onwards.

6. In view of the aforesaid, all requesting entities, ASA's and device providers are directed to take precautionary measures to complete the migration of L0 finger print registered devices to L1 finger print registered devices.

7. This issues with the approval of competent authority.

27.09.2024

(Abhijeet)
Director
Tel.: 011-23478615
Email: dir1.auth-hq@uidai.net.in

Copy to:

1. All UIDAI Regional Offices
2. Technology Centre, Bangalore

INDEX

UIDAI letter F. no.: HQ-13021/1/2021-AUTH-I HQ/C-15305 , Dated 27.9.2024

Annexure-1

L0 Fingerprint device models to be hot listed as per timelines

S. No.	Device Provider	Model ID	Date of Hot listing
1	M/s Integra Micro Systems Pvt Ltd	IMS.IMS.1300E.W	30-09-2024
2	M/s Integra Micro Systems Pvt Ltd	IMS.IMS.CSD2.W	30-09-2024
3	M/s Precision Biometric India Private Limited	PBCS200	30-09-2024
4	M/s Matrix Comsec Pvt Ltd	MCP.FAX.500OH.E	30-09-2024
5	M/s Matrix Comsec Pvt Ltd	MCP.FOT.500OH.E	30-09-2024
6	M/s Linkwell Telesystems	VTK.GL11.A400.E	31-10-2024
7	M/s Integra Micro Systems Pvt Ltd	IMS.PAX.A400.A	31-10-2024
8	M/s Integra Micro Systems Pvt Ltd	IMS.OAS.CBME3.E	31-10-2024
9	M/s Integra Micro Systems Pvt Ltd	IMS.IMS.MF100.W	31-10-2024
10	M/s Integra Micro Systems Pvt Ltd	IMS.IMS.MF100.A	31-10-2024
11	M/s Secugen India Pvt Ltd	HU20A	31-10-2024
12	M/s Smartchip India Pvt Ltd	293658783	31-10-2024
13	M/s Secugen India Pvt Ltd	HU10	31-10-2024
14	M/s Evolute Systems Pvt Ltd	EVOLUTEFPSA600	31-10-2024
15	M/s Linkwell Telesystems	VTK.Q2POS.TCS1S.A	31-10-2024
16	M/s Integra Micro Systems Pvt Ltd	IMS.AQT.TCS1S.A	31-10-2024
17	M/s Evolute Systems Pvt Ltd	LEOPARD	31-10-2024
18	M/s Evolute Systems Pvt Ltd	FALCON	31-10-2024
19	M/s Bioenable Tech	BIOENABLE-BETPV	31-10-2024

Abhijeet 27.09.2024

(Abhijeet)
Director
Tel.: 011-23478615
Email: dir1.auth-hq@uidai.net.in

F. No. HQ-13079/15/2024-AUTH-II HQ/15213
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road
Behind Kali Mandir, Gole Market
New Delhi – 110 001
Dated 20 December 2024

Circular 3 of 2024

Subject: Guidelines on requiring Aadhaar number for receipt of subsidy, benefit or service under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

Please refer to the following Circulars of UIDAI, a copy each of which is annexed herewith for ready reference, namely:—

(a) Circular no. 23011/Gen/2014/Legal-UIDAI, dated 15.9.2016, on the subject "Notification for use of Aadhaar under Section 7 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") for targeted delivery of financial and other subsidies, benefits and services funded from Consolidated Fund of India" **(Annexure-II)**; and

(b) Circular no. 1-1/2019-UIDAI (DBT), dated 25.11.2019, on the subject "Guidelines on use of Aadhaar under section 7 of the Aadhaar Act 2016 (as amended by the Aadhaar and Other Laws (Amendment) Act, 2019) by the State Governments for the schemes funded out of Consolidated Fund of State" **(Annexure-III)**.

2. On the basis of a review of the existing templates to take into account further evolution of the policies, procedures and systems for the issuing Aadhaar number and performing authentication thereof and with a view to offering greater clarity, in partial modification of the aforesaid Circulars, a revised template that may be used for the issuance of a notification pursuant to requirement of Aadhaar number under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 is attached herewith **(Annexure-I)**.

3. The revised template, among other things, makes clear the following:

(a) The officer designated by the Ministry or Department concerned shall check the documents or information presented by an individual who is desirous of availing of subsidy, benefit or service but to whom Aadhaar number has not been assigned in the manner specified in clause (4) of paragraph 1 of the template. Accordingly, *the Enrolment ID (EID) contained in the enrolment acknowledgement must be used to check the status of the enrolment request by submitting the EID on myAadhaar portal (https://myaadhaar.uidai.gov.in/portal) to confirm that the EID is valid and that the enrolment request does not stand rejected.*

(b) Where the authentication of the Aadhaar number of the beneficiary done through any of the biometric-based modes of authentication (namely, facial image,

INDEX

fingerprints or iris scan based authentication) fails due to any reason, such as poor quality of biometric information, and where no other biometric-based or OTP-based mode of authentication is possible, the manner in which the genuineness of his Aadhaar number may be established through offline verification for giving him the benefit is specified in clause (b) of paragraph 3 of the template. Accordingly,—

(i) *an Aadhaar card, Aadhaar letter or e-Aadhaar must be verified by scanning the QR code using the Aadhaar QR Scanner or mAadhaar apps.* Both apps may be downloaded from the Google Play Store or iOS App Store; and

(ii) an Aadhaar Paperless Offline e-KYC document must be verified through an application developed by the Ministry or Department or scheme implementing agency concerned. Details regarding such application may be accessed by searching on the UIDAI website for "About Aadhaar Paperless Offline e-KYC" or "Offline verification and role of OVSEs under Authentication Ecosystem".

4. *It is also requested that as and when any notification as aforesaid is issued, a copy of the published notification may be mailed to UIDAI at notification.auth-hq@uidai.net.in for information. Further, a set of all such previously published notifications may also please be mailed at the said address.*

5. A copy of this Circular is available on UIDAI's website (www.uidai.gov.in) and may be accessed by searching on it for "Template for section 7 notification".

6. This issues with the approval of competent authority.

Encl.: as above

(Sanjeev Yadav)
Director
Tel.: 011-23478609
Email: dir2.auth-hq@uidai.net.in

To:

1. Secretaries in charge of Ministries and Departments in Government of India (as per list attached)
2. Chairperson and Chief Executive Officer, Railway Board
3. Chief Secretaries of State Governments (as per list attached)
4. Chief Secretary, Government of Jammu and Kashmir / National Capital Territory of Delhi / Puducherry / Andaman and Nicobar Islands Administration
5. Advisor to Administrator, Chandigarh Administration
6. Advisor to Lieutenant Governor, Ladakh Administration
7. Administrator, Dadra and Nagar Haveli and Daman and Diu Administration / Lakshadweep Administration

INDEX

Copy, for information, to:

1. Advisor to Prime Minister, Prime Minister's Office
2. Chief Executive Officer, NITI Aayog
3. Secretary (Coordination), Cabinet Secretariat
4. All Deputy Directors General, UIDAI

INDEX

F.no. HQ-13073/2/2023-AUTH-II HQ/C-10768
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road,
Behind Kali Mandir, Gole Market,
New Delhi – 110 001
Dated 26 December 2024

Circular No. 03 of 2023

Subject: Rationalization of Sub-AUA/Sub-KUA

In partial modification of UIDAI's office circular bearing F. No. HQ-13073/2/2023-AUTH-II HQ (E-10768) dated 31.3.2023 on the subject matter Rationalization of Sub-AUA/Sub-KUA, the following amendments are being executed to simplify and rationalize the government Sub-AUA/Sub-KUA ecosystem and to encourage more government departments to onboard in Aadhaar authentication ecosystem for delivering of their services/benefits:

Para No	Existing provisions	Revised provisions
2. (i)	The Central/State Govt. Departments performing less than 50,000 transactions per year to continue availing Authentication services through the license keys of their respective AUAs/KUAs (NIC or State AUA/KUA) without paying any license fee to UIDAI. No Sub-AUA/Sub-KUA code will be issued to such Govt. Departments by UIDAI. They may create an internal identifier vis-à-vis their AUA for the purpose of identifying their respective scheme transactions.	The Central/State Govt. Departments performing less than 1 lakh transactions in a financial year (FY) to continue availing Authentication facility through the separate code without paying any license fee to UIDAI. A separate Sub-AUA/Sub-KUA code comprising prefix LITE (Less in Transaction Entity) as prefix shall be issued to such Govt. Departments by respective AUA/KUA.
2. (iii)	Sub-AUAs/Sub-KUAs which are performing transactions between 50,000 to 1 crore per year may continue as-is-basis for the time being.	Sub-AUAs/Sub-KUAs which perform authentication transactions between 1 lakh to 1 crore per financial year (FY), may continue as-is-basis for the time being.

2. AUA/KUA are directed to assign a separate Sub-AUA/Sub-KUA code comprising LITE as prefix to all Sub-AUA/Sub-KUA which have been onboarded under the said circular before 31.12.2024 and confirm the same to UIDAI.

3. This shall come in effect from the date of issue of the letter.

4. This issue with the approval of Chief Executive Officer, UIDAI

(Sanjeev Yadav)
Director
Tel.: 011-23478609
Email: dir2.auth-hq@uidai.net.in

To:

(i) All ASAs, AUAs and KUAs

Copy for information to:

(i) All Deputy Director General, UIDAI (HQs, ROs, Tech Center)

INDEX

F. No. HQ-13064/1/2024-AUTH-I HQ/C. 15014
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated: 01 January 2025

Circular 1 of 2025

Subject: Execution of Supplementary Agreement or Agreement to supplement AUA Agreement under sub-regulation (3A) of regulation 9 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021

With the Aadhaar (Authentication and Offline Verification) Amendment Regulations, 2024 dated 31.1.2024, UIDAI has introduced a provision, for sharing of update of status of Aadhaar number upon entering Supplementary Agreement or Agreement to supplement AUA Agreement ("agreement") by requesting entity ("RE") with UIDAI, as sub-regulation (3A) under regulation 9 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021. The said provision is as below—

"(3A) Where the requesting entity has entered into a Memorandum of Understanding or agreement with the Authority for the performance of authentication with update of status regarding whether an Aadhaar number previously submitted has been subsequently omitted or deactivated or reactivated, in the event of such Aadhaar number being omitted or deactivated or such a deactivated Aadhaar number being reactivated, the Authority shall send a subsequent digitally signed appropriate response, along with related technical details."

2. The purpose of the agreement is to set out the terms and conditions for RE for performance of authentication with update of status of Aadhaar numbers previously submitted, in the event of such an Aadhaar number being subsequently omitted or deactivated Aadhaar number being re-activated. This sharing of data will be helpful for RE for their data cleansing and preventing any misuse of facilities and services being offered by it.

3. Further the entity which is already appointed as RE with UIDAI is only eligible to make request for such update of status of Aadhaar number upon entering the agreement with UIDAI. The said agreement shall be executed on non-judicial stamp paper of value as applicable.

4. Two copies of the agreement (original and duplicate) duly signed by the authorized representative of the RE shall be sent to UIDAI for signature. The original signed copy shall be retained by UIDAI for record purposes and duplicate signed copy will be sent to RE by UIDAI.

INDEX

5. The RE, for the performance of authentication under the said agreement, shall be charged to pay such fees, including applicable taxes, as UIDAI may specify in the Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023.

6. Enclosed with this letter is the agreement for its immediate execution.

7. *For any queries regarding the agreement, you are requested to mail to UIDAI at onboarding@uidai.net.in.*

8. This issues with the approval of competent authority.

Encl: as above

(Sanjeev Yadav)
Director
Tel.: 011-23478609
Email: dir2.auth-hq@uidai.net.in

To:

1. Secretaries in charge of Ministries and Departments in Government of India (as per list attached)
2. Chairperson and Chief Executive Officer, Railway Board
3. Chief Secretaries of State Governments (as per list attached)
4. Chief Secretary, Government of Jammu and Kashmir / National Capital Territory of Delhi / Puducherry / Andaman and Nicobar Islands Administration
5. Advisor to Administrator, Chandigarh Administration
6. Advisor to Lieutenant Governor, Ladakh Administration
7. Administrator, Dadra and Nagar Haveli and Daman and Diu Administration / Lakshadweep Administration

Copy, for information, to:

1. Advisor to Prime Minister, Prime Minister's Office
2. Chief Executive Officer, NITI Aayog
3. Secretary (Coordination), Cabinet Secretariat
4. All Deputy Directors General, UIDAI
5. All Authentication User Agency and e-KYC User Agency

INDEX

[On non-judicial stamp paper of value as applicable]

AGREEMENT

This Agreement (hereinafter referred to as **"Supplementary Agreement"** or **"Agreement to supplement AUA Agreement"**) is entered into by and between:

THE UNIQUE IDENTIFICATION AUTHORITY OF INDIA, a statutory authority established under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 [**"Act"**], having its Head Office at New Delhi (current address: Aadhaar Building, Bangla Sahib Road, Gole Market, New Delhi – 110 001) (hereinafter referred to as **"UIDAI"** or **"Authority"** or **"First Party"**, which expression shall, unless the context otherwise requires, include its authorized representatives and successors), of the **First Part**:

AND

_____[1] (hereinafter referred to as **"Second Party"**), acting through its authorised representative, _____[2], which expression shall, unless the context otherwise requires, include its authorised representatives and such successors of the **Second Part**.

The said parties are collectively referred to hereinafter as **'Parties'** and individually as **'Party'**.

WHEREAS the Second Party is a requesting entity appointed by UIDAI as an _____[3] for the purpose of use of the Aadhaar Authentication facilities of UIDAI:

AND WHEREAS the Second Party has, under the Aadhaar (Authentication and Offline Verification) Regulations, 2021, entered into an AUA agreement with UIDAI for the use of the Aadhaar Authentication facilities of UIDAI ("AUA Agreement") and is desirous of entering into this Supplementary Agreement that sets out the terms and conditions for us of the said facilities for performance of authentication with update of status of Aadhaar numbers previously submitted, in the event of such an Aadhaar number being subsequently omitted or deactivated Aadhaar number being re-activated:

AND WHEREAS the Second Party understands and acknowledges that the terms and conditions set out herein are in addition to and not in derogation of the powers of UIDAI and the obligations and liabilities of requesting entities under the Act, the regulations made thereunder and the obligations and liabilities of the Second Party under the AUA Agreement:

NOW THEREFORE, this Supplementary Agreement witnesses as under:

---

[1] Name of the Second Party

[2] Full name and full designation

[3] <Authentication User Agency (AUA)>or<Authentication User Agency (AUA) and an e-KYC User Agency (KUA)> (whichever is applicable)

INDEX

1. The Supplementary Agreement shall come into force from the date it is signed and shall remain in effect until it is replaced by another Supplementary Agreement or is terminated.

1.1 The Parties may, by mutual agreement, amend the terms and conditions of the Supplementary Agreement.

1.2 The Supplementary Agreement may be terminated by either Party by giving notice, in writing, to the other Party on this behalf.

1.3 The Second Party acknowledges that it shall be obligated to pay such fees, including applicable taxes, as UIDAI may specify in regulations made by it in exercise of its powers under sub-sections (1) and (2) of section 54 read with sub-section (1) of section 8 of the Act, and on such terms as to payment thereof as UIDAI may stipulate from time to time.

1.4 UIDAI shall provide the AUA the use of Aadhaar Authentication facilities at its sole discretion and reserves the right to add to, to revise or to suspend in whole or in part such provision at any time, without prior notice, at its sole discretion, in the interest of protection of the information of Aadhaar number holders or the Aadhaar ecosystem, or in public interest, or in public interest, or in any of the interests referred to as per the terms of the AUA Agreement.

2. **Principles**

2.1 This Supplementary Agreement sets forth a statement of intent of the Parties to thus Supplementary Agreement to establish a framework to facilitate the use of Authentication facility including any subsequent appropriate response returned by UIDAI regarding the status as to whether any Aadhaar number previously submitted has been subsequently omitted or deactivated or re-activated in the event of any omission or deactivation of such Aadhaar number or re-activation of such a deactivated Aadhaar number.

2.2 The Parties to Supplementary Agreement shall use their best endeavors to meet the terms of this Supplementary Agreement.

3. **Safeguards and Confidentiality**

3.1 The Parties to Supplementary Agreement undertake to implement and maintain security procedures and measures in order to ensure the protection against the risks of unauthorised access, alteration, delay, destruction or loss of information regarding status update.

3.2 The Parties to Supplementary Agreement agree that the status update response provided shall be subject to the confidentiality rules and other safeguards to ensure necessary level of confidentiality.

4. **Consultation**

4.1 The Parties may consult one another informally at any time about a new request or proposed request.

INDEX

4.2 The Parties may consult and revise terms of the Supplementary Agreement in the event of a substantial change in the laws, practices, market or business conditions affecting the operation of this Supplementary Agreement.

4.3 Any dispute arising out of the interpretation and implementation or application of this Supplementary Agreement shall be settled amicably by consultation between the Parties.

5. **Nodal Officer**

5.1 The Parties to Supplementary Agreement shall appoint Nodal Officer and alternate Nodal Officer with the following responsibilities to—

(a) act as point of contact for coordinating in respect of anything relating to this Supplementary Agreement;
(b) accord due priority and resources for timely completion of tasks related to this Supplementary Agreement;
(c) establish a mechanism for resolving status update response quality issue, if any, within a reasonable time-frame; and
(d) establish a mechanism for periodic review of Supplementary Agremeent.

6. **Validity and exit clause**

6.1 This Supplementary Agreement will be in force until unless terminated in writing with the mutual consent of both Parties.

IN WITNESS WHEREOF, the Parties hereto have signed this Supplementary Agreement to confirm their approval of, an agreement with, its contents.

Signed at **<<PLACE>>** on **<<DATE>>**

FOR AND ON BEHALF OF UIDAI:	FOR AND ON BEHALF OF SECOND PARTY:
Signature:	Signature:
Name:	Name:
Designation:	Designation:
Date:	Date:
IN THE PRESENCE OF:	IN THE PRESENCE OF:

INDEX

Signature:	Signature:
Name:	Name:
Designation:	Designation:
Date:	Date:

INDEX

F. No. HQ-13079/38/2024-AUTH-II HQ/C. 16542
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road
Behind Kali Mandir, Gole Market
New Delhi – 110 001
Dated: 7 February 2025

Circular 02 of 2025

Subject: Appointment of Sub-Authentication User Agency and Sub-eKYC User Agency

Please refer to the Circular bearing F. No. K-11022/460/2016-UIDAI (Auth-II) dated 06.7.2017, on the subject "Appointment of Sub-AUA.

2. On the basis of review of the existing format for application form and joint undertaking to take into account enhanced accountability, compliance mechanisms and adherence to strict authentication and data protection standards, a revised format that may be used for submitting application for appointment of Sub-Authentication User Agency (Sub-AUA) and Sub-eKYC User Agency (Sub-KUA) in pursuance to clause (ga) of sub-regulation (1) of regulation 14 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021 is attached herewith.

3. *For any queries regarding the revised formats, you are requested to mail to UIDAI at onboarding@uidai.net.in.*

4. A copy of this Circular is available on UIDAI's website (https://www.uidai.gov.in/en/ecosystem/authentication-devices-documents/authentication-document.html).

5. This issues with the approval of competent authority.

(Sanjeev Yadav)
Director
Tel.: 011-23478609
Email: dir2.auth-hq@uidai.net.in

INDEX

(On the Letter Head of AUA/KUA)

To:

The Chief Executive Officer, Unique Identification Authority of India
[Attention: Deputy Director (Authentication-II), UIDAI]
UIDAI Head Office, Bangla Sahib Road,
Gole Market,
New Delhi-110001

Subject: Appointment of _____[1] as a Sub-AUA and Sub-KUA

Sir/madam,

Regulation 14(1)(ga) of the Aadhaar (Authentication and Offline Verification) Regulations, 2021 ["**regulations**"] requires an AUA/KUA to obtain approval from the Unique Identification Authority of India (hereinafter referred to as "Authority") before appointing any third party entity as a Sub-AUA and Sub-KUA for the use of Yes/No authentication facility under regulation 15 and e-KYC authentication facility under sub-regulation (2) of regulation 16, respectively of the said regulations by submitting an application and executing joint undertaking.

2. In this regard, we are submitting herewith an application (**Annexure – I**) for appointment of _____[2] as our Sub-AUA and Sub-KUA along with a Joint Undertaking (**Annexure – II**) with the proposed Sub-AUA and Sub-KUA.

3. We request you to approve the appointment of _____[3], as our Sub-AUA and Sub-KUA.

Thanks & Regards,

(Authorized Signatory)
Name:
Designation:
Mobile no.
Enclosures: Application Form along with Joint Undertaking

[1] Insert name of the proposed Sub-AUA and Sub-KUA
[2] Insert name of the proposed Sub-AUA and Sub-KUA
[3] Insert name of the proposed Sub-AUA and Sub-KUA

INDEX

Annexure-I

Application for appointment as a Sub-AUA and Sub-KUA under regulation 15 and 16(2) read with regulation 14(1)(ga) of the Aadhaar (Authentication and Offline Verification) Regulations, 2021

1. Details of the Sub-AUA and Sub-KUA:

(a) Name of the Sub AUA and Sub-KUA	
(b) Registration/Incorporation No.[4] *(Please attach copy of the document, if applicable)*	
(c) License No.[5] *(Please attach copy of the document, if applicable)*	
(d) Registered Office address	
(e) Correspondence address *{If other than address mentioned against (d)}*	
(f) GSTN registration number of Sub-AUA and Sub-KUA, as per Form GST REG-06 (*Please attach copy of the document, if applicable)*	
(g) Tax Deduction and Collection Account Number (TAN) of Sub-AUA and Sub-KUA	
(h) Type of Aadhaar Authentication facility; Corresponding category of requesting entity (*Tick as applicable)*	☐ Yes/No Authentication facility; and ☐ e-KYC Authentication facility
(i) Board Resolution/minutes (or other valid letter/instrument of authorisation) citing approval for submitting the application form and signing Joint Undertaking and doing other Acts in relation to the same. (*Please attach a certified copy of the document)*	

[4] Copy of Certificate of Incorporation/registration to be attached in case of "other than Govt. entities"
[5] Copy of Certificate of Registration/License from the concerned regulator issued from RBI, SEBI, IRDAI and PFRDA

INDEX

(j) The provision of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 under which authentication is required/permitted *{If such provision is section 7 or section 4(4)(b)(ii) or section 4(4)(b)(i) read with the Prevention of Money-laundering Act, 2002, please attach copy of the relevant notification published in the Official Gazette}*	☐ Section 7 ☐ Section 4(4)(b)(i), read with the Prevention of Money-laundering Act, 2002 ☐ Section 4(4)(b)(i), read with relevant Central Act other than the Prevention of Money-laundering Act, 2002 ☐ Section 4(4)(b)(ii) ☐ Section 4(7)
(k) Gazette notification details	Gazette notification no: Gazette notification dated: Gazette notification published date: Gazette notification published by:

INDEX

E - AUTHENTICATION & VERIFICATION

(l) Category of the Sub-AUA and Sub-KUA	☐ AMinistry, Department, secretariat, office, or agency of the Central Government, which has required, in terms of the provisions of section 7 of the Act, that an individual undergo authentication for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of the Consolidated Fund of India ☐ A Ministry, Department, secretariat, office or agency of the Government of _____[6], which requires, in terms of the provisions of section 7 of Act, that an individual undergo authentication for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of the Consolidated Fund of State ☐ An entity permitted under sub-clause (i) of clause (b) of sub-section (4) of section 4 of the Act to offer authentication services under[7] _____ of _____[8]. ☐ An entity permitted under sub-clause (i) of clause (b) of sub-section (4) of section 4 of the Act to offer authentication services under section 11A of the Prevention of Money-laundering Act, 2002, by virtue of being a reporting entity under the said Act as a _____[9], in terms of _____[10] of sub-section (1) of section 2 of the said Act. ☐ An entity that has been allowed/authorised under sub-clause (ii) of clause (b) of sub-section (4) of section 4 of the Act, vide Ministry of Electronics and Information Technology's letter no. _____[11], dated _____[12]. ☐ An entity that is required, in terms of the provisions of sub-section (7) of section 4 of the Act, to perform mandatory authentication by _____ of _____[13].

6 Name of the concerned State, or the concerned Union territory with Legislature

7 Reference of the relevant provision (section, sub-section, clause etc.) of the relevant Act of Parliament, other than the Prevention of Money-laundering Act, 2002 ("PML Act")

8 Name of the relevant Act of Parliament, other than the PML Act

9 banking company, or financial institution, or intermediary, or a person carrying on activities for playing games of chance for cash or kind, or Inspector-General of Registration appointed under section 3 of the Registration Act, 1908, or Central-Government-notified real estate agent, or Central-Government-notified dealer in precious metals, precious stones and other high value goods, or Central-Government-notified person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, or Central-Government-notified person carrying on such other activities (whichever is applicable)

10 clause (wa), or sub-clause (i) of clause (na), or sub-clause (ii) of clause (na), or sub-clause (iii) of clause (na), or sub-clause (iv) of clause (na), or sub-clause (v) of clause (na), or sub-clause (vi) of clause (na) (whichever is applicable)

11 Number of the letter so allowing/authorising

12 Date of the letter so allowing/authorising

13 the provision (section, sub-section, clause etc.) of the Act made by Parliament, other than the Aadhaar Act

INDEX

(m) Purpose for which authentication facility will be used	1. 2.

2. Contact details:

(a) Details of Key Managerial Personnel (KMP)[14]			
Name			
Full designation			
Official email address			
Mobile number			
Alternate office telephone number			
(b) Details of Chief Information Security Officer (CISO)			
Name			
Official Email Address			
Mobile number			
Alternate Office Telephone number			
(c) Management Point of Contact (MPOC)		Person authorised on the basis of Board resolution/minutes (or other valid letter/instrument of authorisation)	Other key personnel (if any)
Name			
Full designation			
Official email address			
Mobile number			
Alternate office telephone number			
(d) Technical Point of Contact (TPOC)	CXO/ Head of the functional vertical, who reports to the chief executive or governing body of the Sub-AUA and Sub-KUA		Other key personnel (if any)
Name			
Full designation			
Official email address			
Mobile number			
Alternate office telephone number			

14 For the purpose of this "Key Managerial Personnel (KMP)" means a KMP as defined under sub-section (51) of section 2 of the Companies Act, 2013

(e) Sub-AUA and Sub-KUA infrastructure details[15]	DC (Data Centre)	DR (Data Recovery Centre)
MPOC/TPOC Name		
Email address		
Telephone/Mobile No.		
Address		
District		
State		
PIN Code		
(f) Contact details for Grievance redressal:		
Website URL		
Email Address		
Helpdesk Number		
3. Details of Authentication Service Agency (ASA)		
(a) Name(s) of ASA (*In case of multiple ASAs, please provide their names*)	1. _____ 2. _____ 3. _____	
(b) Declaration by the ASA(s) agreeing to provide its/their secure network connectivity and related services for the performance of authentication (*Please attach letter of ASA in original)*		
4. Authentication requirements		
(a) Territorial extent for use of Authentication facility	☐ Whole of India	
	☐ Name of State(s) and Union Territory(s):	
(b) Whether Authentication will be used to establish identity for	☐ Yes ☐ No	

[15] If using infrastructure of its AUA/KUA, then details of the same

INDEX

carrying out financial transaction	
(c) Device form factor *(select one or more option)*	☐ Discrete Biometric Device ☐ Integrated Biometric Device ☐ Laptop/Desktop ☐ Mobile phone
(d) Whether Authentication will be operator-assisted or by the user himself/herself *(select one or more option)*	☐ Operator-assisted use Self-use ☐
(e) Mode of Authentication *(select one or more option)*	☐ Demographic ☐ OTP ☐ Fingerprint ☐ Iris ☐ Face
(f) Connectivity supported between AUA/KUA and ASA *(select one or more option)*	☐ VPN ☐ Leased line ☐ Other; Please specify: _____
(g) Confirmation that the Sub-AUA and Sub-KUA has perused and understood UIDAI's Information Security Policy – External Ecosystem – Authentication User Agency/ KYC User Agency v6.0 *(Copy of the said policy document, after affixing the signatures of the authorised signatory, to be attached)*	☐ Yes ☐ No

INDEX

(h)	Confirmation that the Sub-AUA and Sub-KUA has perused and understood UIDAI's Model Privacy Policy for Protecting Personal data of Aadhaar number holders by Requesting Entities *(Copy of the said policy document, after affixing the signatures of the authorised signatory, to be attached)*	☐ Yes ☐ No

INDEX

Declarations and Undertakings:

It is hereby declared that the information furnished in this application form is true and correct to the best of its knowledge and that no material particulars or information have been concealed or withheld, and that the (name of AUA/KUA) and (name of Sub-AUA and Sub-KUA) hereby undertakes—

(a) to abide by the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") and the regulations made thereunder;

(b) to facilitate, on receipt of in-principle approval from UIDAI, audit as per UIDAI "Compliance Checklist for Onboarding the Requesting Entity" and submit all compliance related documents attached as annexures before signing the AUA/KUA Agreement;

(c) to fulfil all requirements with respect to use of the Aadhaar Authentication facility as per the Aadhaar (Authentication and Offline Verification) Regulations, 2021;

(d) to set up and maintain within the territory of India, at all times, requisite infrastructure (including, but not limited to, servers, databases etc.) for the use of Aadhaar Authentication facilities, capable of handling a minimum of one lakh Authentication transactions per month;

(e) to carry out appropriate due diligence before engaging any sub-contractor, business correspondent or field operator for performing any functions in relation to the use of Aadhaar Authentication facilities, including on boarding of user/beneficiary/customer, Authentication application development, etc.;

(f) to store Aadhaar numbers, if authorised so to do, only in the Aadhaar Data Vault, in accordance with such policies, procedures, standards and technical specifications as UIDAI may specify from time to time;

(g) to ensure the carrying out of audit of its own operations and systems and those of its Sub-AUAs and Sub-KUAs, if any, as required under the Aadhaar Act, the regulations made thereunder and the AUA Agreement;

(h) to not share or disclose e-KYC data that may be received on use of e-KYC Authentication facility, except in accordance with the provisions of the Aadhaar Act and the regulations made thereunder; and

(i) to inform UIDAI of any change in the name, address and other particulars of the applicant and contact persons as furnished in this application form;

(j) to inform the UIDAI with a complete record of the total number and names of all schemes/portals associated with Sub-AUA/ Sub-KUA .

(Authorized signatory on behalf of Sub-AUA and Sub-KUA)
Signature: _____
Name: _____
Designation: _____
Organization: _____
Date: _____

All the details mentioned above have been verified.

INDEX

(Authorized signatory on behalf of AUA/KUA)
Signature: _____
Name: _____
Designation: _____
Organization: _____
Date: _____

INDEX

Annexure-II

[Joint Undertaking to be drawn on non-judicial stamp paper of value as applicable. Please follow guidance given in referenced footnotes regarding filling up of underscored blank portions in this draft. Wherever guidance includes one or more text options bracketed by symbols "<" and ">", relevant option should be used without modification. Omit guidance and inapplicable text options.]

Joint Undertaking

We, (name of AUA/KUA), intend to appoint (name of Sub-AUA and Sub-KUA) as Sub Authentication User Agency ("Sub-AUA") and Sub-e-KYC User Agency ("Sub-KUA") and both of us are fully aware of and understand the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ["the Aadhaar Act"] and the regulations made there under. Further, we warrant that we shall at all times abide by the Act, regulations, various circulars, guidelines, directions, notifications, etc. issued by UIDAI from time to time.

We, (name of AUA/KUA) and (name of Sub-AUA and Sub-KUA), 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 material particulars have been concealed.

By this, the undersigned on behalf of (name of AUA/KUA) and (name of Sub-AUA and Sub-KUA) affirm, declare and undertake the following:

1. We (name of AUA/KUA) shall ensure that the Aadhaar authentication services are used by (name of Sub-AUA and Sub-KUA) only for the purpose as mentioned in the application form.
2. (name of Sub-AUA and Sub-KUA) shall use the separate License Key and unique Sub-AUA and Sub-KUA code allocated to it by UIDAI and/or AUA/KUA, as the case may be, and shall not share these further with any other person or entity for any purpose, and shall keep such License Key and unique Sub-AUA and Sub-KUA Code secured from unauthorized access in any form.
3. (name of AUA/KUA) shall ensure that the (name of Sub-AUA and Sub-KUA) complies with the provisions of the Aadhaar Act and its regulations, directions, processes, standards, guidelines, notifications, specifications and protocols of the Authority that are applicable to the requesting entity.
4. (name of AUA/KUA) shall ensure that the (name of Sub-AUA and Sub-KUA) is audited by information system auditor certified by a recognized body on an annual basis to ensure compliance with the UIDAI's standards and specifications and report shall be submitted to UIDAI upon request.

5. (name of AUA/KUA) understands that time period for moving from pre-production to production is of 3 months or such longer period as UIDAI may permit in writing. However, if (name of Sub-AUA and Sub-KUA) defaults in meeting the requirements for moving from pre-production to production environment within the specified period,

   (a) the approval from UIDAI to the application of (name of Sub-AUA and Sub-KUA) shall cease on expiry of that period, unless UIDAI permits in writing.

   (b) the fees paid shall be forfeited in favour of UIDAI; and

   (c) no liability shall lie against the UIDAI, in any manner whatsoever, in this regard.

6. (name of AUA/KUA) shall ensure that the (name of Sub-AUA and Sub-KUA) is a regulated entity under (Name of Regulator) and it compulsorily maintains this status during the period of using authentication facility. ***(strike out if not applicable).***

7. To enhance the security level, the (name of Sub-AUA and Sub-KUA) shall maintain Aadhaar Data Vault (ADV) for storing Aadhaar number and related Personal Identity Information (PII) in their database, as per the guidelines issued by UIDAI from time to time.[16]

8. (name of Sub-AUA and Sub-KUA) shall ensure that, the Aadhaar number and any connected Aadhaar data (ex. e-KYC XML containing Aadhaar number and data) maintained on the ADV or in rest or in motion shall always be kept encrypted and access to it strictly controlled only for authorised systems. Keys for encryption are to be stored in Hardware Security Module (HSM) devices only. The ADV implemented must have strong access controls, authentication measures, monitoring and logging of access and raising necessary alerts for unusual and/or unauthorized attempts to access. Any non-compliance would result in cancellation of their license key and termination of their Agreement.[17]

9. (name of AUA/KUA)in compliance with sub-regulation (2) of regulation 16 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021 shall share the e-KYC data received from UIDAI with (name of Sub-AUA and Sub-KUA)only and that too in encrypted format (using its own encryption key), as per the guidelines issued by the Authority from time to time with the specific consent of the Aadhaar number holder and after obtaining permission from Authority. Further, (name of Sub-AUA and Sub-KUA) shall not share this information with any other entity or agency as per sub-regulation (3).

10. (name of AUA/KUA) shall ensure that, in the event of revocation of consent given by the Aadhaar number holder, at any time, to Sub-AUA and Sub-KUA for storing his e-KYC data, the Sub-AUA and Sub-KUA shall delete the e-KYC data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder.

[16] Strike out if not applicable
[17] Strike out if not applicable

INDEX

11. (name of AUA/KUA) shall maintain auditable logs of all such transactions where e-KYC data has been shared with (name of Sub-AUA and Sub-KUA), for a period specified by the Authority in due compliance of sub-regulation (6) of regulation 16, sub-regulations (2) and (3) of regulation 18 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021.

12. We (name of AUA/KUA) shall ensure that the client application to be used for Aadhaar authentication is developed and digitally signed by us, ***OR*** (name of Sub-AUA and Sub-KUA) shall integrate digitally signed SDK developed by us in their client application for capturing Aadhaar information like Aadhaar number, biometric information, demographic information, etc.

13. (name of AUA/KUA) shall ensure that the (name of Sub-AUA and Sub-KUA)'s client application or SDK, as the case may be, for Aadhaar authentication is audited as per standards set by the Authority, at the time of appointment of (name of Sub-AUA and Sub-KUA) and also every year thereafter, by information systems auditor(s) certified by CERT-IN empanelled auditors and submit compliance audit report against Compliance Checklist for certifying compliance with controls that the Sub-AUA and Sub-KUA is required to have in place, to UIDAI.

14. (name of AUA/KUA) and (name of Sub-AUA and Sub-KUA) shall inform UIDAI, without undue delay and in no case beyond _____ hours/days after having knowledge of misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information.

15. We, (name of AUA/KUA) and (name of Sub-AUA and Sub-KUA) shall be jointly and severally liable for non-compliance of the provisions of the Aadhaar Act and its Regulations, specifically the Aadhaar (Authentication and Offline Verification) Regulations 2021,and directions, information security policies, processes, standards, specifications, guidelines and protocols issued by the Authority from time to time and shall be jointly and severally liable for disincentives and penalties as per the schedule of disincentives of Authentication User Agency Agreement v____.0 executed by (name of AUA/KUA) in addition to initiation of action under other applicable laws and other provisions including section 33A of the Aadhaar Act.

16. (name of AUA/KUA) and (name of Sub-AUA and Sub-KUA) have ensured that the declared information filled up in the application form as well as this joint undertaking was placed before the board of directors[18] of their respective organizations in their meetings dated _____[19] and dated _____[20], respectively and has been read over and verified to be true and correct.

17. No material particulars have been concealed and upon verification of the application, the board has approved the same for submission at the hands of

[18] This is applicable for other than the government entities. Mention "NA" if not applicable
[19] Meeting date of AUA/KUA
[20] Meeting date of Sub-AUA and Sub-KUA

INDEX

_____[21]. Any change in the name, contact details, addresses etc. as filled up in the application form shall also be immediately conveyed to the Authority.

18. The board resolutions/minutes of the meetings dated _____[22] and dated _____[23] approving the application form and authorizing _____[24] on behalf of (name of AUA/KUA) and (name of Sub-AUA and Sub-KUA), respectively to submit the same are being annexed herewith.

19. The application form having been duly filled up and all its particulars having been verified by all the directors/head of department, 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 _____202__ at _____.

Authorized signatory of (name of AUA/KUA)
Signature: _____
Name: _____ _____
Designation: _____
Organization: _____ Date: _____

Authorized signatory of (name of Sub-AUA and Sub-KUA)
Signature: _____
Name: _____ _____
Designation: _____
Organization: _____ Date: _____

[21] Name along with designation of the person authorised based onBoard resolution/minutes in this regard for AUA/KUA and Sub-AUA and Sub-KUA, respectively
[22] Meeting date of AUA/KUA
[23] Meeting date of Sub-AUA and Sub-KUA
[24] Name along with designation of the person authorised based onBoard resolution/minutes in this regard for AUA/KUA and Sub-AUA and Sub-KUA, respectively

INDEX

UIDAI letter F. no.: HQ-13021/1/2021-AUTH-I HQ/C-16262, dated 16th April 2025

Copy to:

1. All UIDAI Regional Offices
2. Technology Centre, Bangalore
3. M/s. Smart Chip Pvt. Ltd, M/s. Precision Biometric India Pvt Ltd & M/s. Access Computech Pvt. Ltd. — *directed to push latest RDS version to their already whitelisted devices of above-mentioned respective models.*

F. No. HQ-13079/10/2024-AUTH-I HQ-Part(1)/(C. no. 15597)
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road
Behind Kali Mandir, Gole Market
New Delhi – 110 001
Dated: 17 February 2025

Circular 03 of 2025

Subject: Submission of Declaration and Undertaking regarding general character of management and the financial condition of the applicant entity under regulation 12(6) of the Aadhaar (Authentication and Offline Verification) Regulations, 2021

With the Aadhaar (Authentication and Offline Verification) Second Amendment Regulations, 2024 dated 03.12.2024 has amended the sub-regulation (6) of regulation 12 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021. The said amendment intents to secure the interest of privacy and security of information of the general public by having a sound general character of management and financial condition of the applicant entity. The said amendment is as below—

"(6) After verification of the application, documents, information furnished by the applicant and its eligibility, the Authority may, if it is satisfied that the general character of management and the financial condition of the applicant are sound for securing the interests of privacy and security of information of the general public,".

2. The objective behind taking the general character of management and financial condition of the applicant entity into consideration as part of the application process for appointment of requesting entity or Authentication Service Agency (ASA) is to ensure integrity, reputation, and ethical standing of the entity's management along with financial stability and the ability to sustain operations within the Aadhaar authentication ecosystem. The affirmation and documentary evidence in this regard would help the Authority to identify applicant entities in respect of whom courts, regulators and statutory authorities may have found violations of law, issued censures or reprimands, instituted proceedings, taken adverse note, etc. and to take into account any such history in relation to activities as part of the Aadhaar ecosystem, which are of a nature that reflect unsound management, moral turpitude or carrying on of the affairs of such entity in a manner prejudicial to privacy and security of information of the general public.

3. To comply with the amended regulation, all applicant entities while submitting the request for appointment as requesting entity or ASA must furnish following required details in the prescribed Declaration and Undertaking format, regarding:

INDEX

(a) Good Character of Management: providing assurance with robust governance standards; and

(b) Sound Financial Condition: demonstrating financial viability to sustain operation within the Aadhaar authentication ecosystem.

4. This Declaration and Undertaking format is annexed as **Annex 1A** to **Annex 1**, which is the application form for the appointment of a requesting entity and ASA, respectively.

5. All requesting entities and ASAs are hereby directed to ensure that the duly filled and signed Annex 1A is submitted along with their application form for further processing of their appointment.

6. Enclosed with this letter is the declaration and undertaking format.

7. *For any queries regarding the agreement, you are requested to mail to UIDAI at onboarding@uidai.net.in.*

8. This issues with the approval of competent authority.

Encl: as above

(Sanjeev Yadav)
Director
Tel: 011-23478609
Email: dir2.auth-hq@uidai.net.in

Annex 1

Application form
for
Appointment as Authentication User Agency (AUA) and e-KYC User Agency (KUA)

To:

The Chief Executive Officer, Unique Identification Authority of India
[Attention: Deputy Director (Authentication-II), UIDAI]
UIDAI Head Office, Bangla Sahib Road
Gole Market, New Delhi – 110 001

1. Details of the applicant Ministry, Department, secretariat, office or agency of the Central Government, a State Government or the Government/Administration of a Union territory, or other entity:	
(a) Name of the applicant[1]	
(b) Registration/ Incorporation No.[2] *(Please attach copy of the document, if applicable)*	
(c) License No.[3] *(Please attach copy of the document, if applicable)*	
(d) Registered office address	
(e) Correspondence address *{If other than address mentioned against (d)}*	
(f) GSTN registration number of the applicant, as per Form GST REG-06 *(Please attach copy of the document, if applicable)*	
(g) Tax Deduction and Collection Account Number (TAN) of the applicant *(Please attach copy of the document, if applicable)*	
(h) Type of Aadhaar Authentication facility; Corresponding category of requesting entity *(Tick as applicable)*	☐ Yes/No Authentication facility; AUA ☐ Yes/No Authentication facility and e-KYC Authentication facility; AUA and KUA

1Name of the applicant Ministry, Department, secretariat, office or agency of the Central Government or the Government of State or Union territory, or other applicant entity
2 Copy of Certificate of incorporation/registration to be attached in case of "other than Govt. entities"
3 Copy of Certificate of Registration/License from the concerned Regulator issued from RBI, SEBI, IRDAI and PFRDA

INDEX

(i) Board resolution/minutes (or other valid letter/instrument of authorisation) citing approval for submitting the application form, signing Authentication User Agency Agreement and doing other acts in relation to the same *(Please attach certified copy of the document)*	
(j) The provision of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 under which authentication is required/permitted *{If such provision is section 7 or section 4(4)(b)(ii) or section 4(4)(b)(i) read with the Prevention of Money-laundering Act, 2002, please attach copy of the relevant notification published in the Official Gazette}*	☐ Section 7 ☐ Section 4(4)(b)(i), read with the Prevention of Money-laundering Act, 2002 ☐ Section 4(4)(b)(i), read with relevant Central Act other than the Prevention of Money-laundering Act, 2002 ☐ Section 4(4)(b)(ii) ☐ Section 4(7)
(k) Category of the applicant Ministry/Department/ secretariat/office/agency/entity	☐ AMinistry, Department, secretariat, office, or agency of the Central Government, which has required, in terms of the provisions of section 7 of the Act, that an individual undergo authentication for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of the Consolidated Fund of India ☐ A Ministry, Department, secretariat, office or agency of the Government of _____[4], which requires, in terms of the provisions of section 7 of Act, that an individual undergo authentication for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of the Consolidated Fund of State ☐ An entity permitted under sub-clause (i) of clause (b) of sub-section (4) of section 4 of the Act to offer authentication services under _____[5] of _____[6]. ☐ An entity permitted under sub-clause (i) of clause (b) of sub-section (4) of section 4 of the Act to offer authentication services under section 11A of the Prevention of Money-laundering Act, 2002, by virtue of being a reporting entity under the said Act as a

4 Name of the concerned State, or the concerned Union territory with Legislature

5 Reference of the relevant provision (section, sub-section, clause etc.) of the relevant Act of Parliament, other than the Prevention of Money-laundering Act, 2002 ("PML Act")

6 Name of the relevant Act of Parliament, other than the PML Act

INDEX

	_____[7], in terms of _____[8] of sub-section (1) of section 2 of the said Act. ☐ An entity that has been allowed/authorised under sub-clause (ii) of clause (b) of sub-section (4) of section 4 of the Act, vide Ministry of Electronics and Information Technology's letter no. _____[9], dated _____[10]. ☐ An entity that is required, in terms of the provisions of sub-section (7) of section 4 of the Act, to perform mandatory authentication by _____ of _____[11].

2. Contact details:

(a) Management Point of Contact (MPOC)		Person authorised on the basis ofBoard resolution/minutes (or other valid letter/instrument of authorisation)	Other key personnel (if any)
Name			
Full designation			
Official email address			
Mobile number			
Alternate office telephone number			

(b) Technical Point of Contact (TPOC)	CXO/ Head of the functional vertical, who reports to the chief executive or governing body of the applicant Ministry/ Department/secretariat/office/agency/entity	Other key personnel (if any)
Name		

7 banking company, or financial institution, or intermediary, or a person carrying on activities for playing games of chance for cash or kind, or Inspector-General of Registration appointed under section 3 of the Registration Act, 1908, or Central Government-notified real estate agent, or Central Government-notified dealer in precious metals, precious stones and other high value goods, or Central Government-notified person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, or Central Government-notified person carrying on such other activities (whichever is applicable)

8 clause (wa), or sub-clause (i) of clause (ra), or sub-clause (ii) of clause (ra), or sub-clause (iii) of clause (ra), or sub-clause (iv) of clause (ra), or sub-clause (v) of clause (ra), or sub-clause (vi) of clause (ra) (whichever is applicable)

9 Number of the letter so allowing/authorising

10 Date of the letter so allowing/authorising

11 the provision (section, sub-section, clause etc.) of the Act made by Parliament, other than the Aadhaar Act

INDEX

	_____[7], in terms of _____[8] of sub-section (1) of section 2 of the said Act. ☐ An entity that has been allowed/authorised under sub-clause (ii) of clause (b) of sub-section (4) of section 4 of the Act, vide Ministry of Electronics and Information Technology's letter no. _____[9], dated _____[10]. ☐ An entity that is required, in terms of the provisions of sub-section (7) of section 4 of the Act, to perform mandatory authentication by _____ of _____[11].

2. Contact details:

(a) Management Point of Contact (MPOC)		Person authorised on the basis ofBoard resolution/minutes (or other valid letter/instrument of authorisation)	Other key personnel (if any)
Name			
Full designation			
Official email address			
Mobile number			
Alternate office telephone number			

(b) Technical Point of Contact (TPOC)	CXO/ Head of the functional vertical, who reports to the chief executive or governing body of the applicant Ministry/ Department/secretariat/office/agency/entity	Other key personnel (if any)
Name		

7 banking company, or financial institution, or intermediary, or a person carrying on activities for playing games of chance for cash or kind, or Inspector-General of Registration appointed under section 3 of the Registration Act, 1908, or Central Government-notified real estate agent, or Central Government notified dealer in precious metals, precious stones and other high value goods, or Central Government-notified person engaged in safekeeping and administration of cash and liquid securities on behalf of other persons, or Central Government-notified person carrying on such other activities (whichever is applicable)

8 clause (wa), or sub-clause (i) of clause (za), or sub-clause (ii) of clause (za), or sub-clause (iii) of clause (za), or sub-clause (iv) of clause (za), or sub-clause (v) of clause (za), or sub-clause (vi) of clause (za) (whichever is applicable)

9 Number of the letter so allowing/authorising

10 Date of the letter so allowing/authorising

11 the provision (section, sub-section, clause etc.) of the Act made by Parliament, other than the Aadhaar Act

INDEX

Full designation		
Official email address		
Mobile number		
Alternate office telephone number		
(c) AUA/KUA infrastructure details	DC (Data Centre)	DR (Data Recovery Centre)
MPOC/TPOC Name		
Email address		
Telephone/Mobile No.		
Address		
District		
State		
PIN Code		
(d) Contact details for grievance redressal:		
(i) Website URL		
(ii) Email address		
(iii) Helpdesk number		
3. Details of Authentication Service Agency (ASA)		
(a) Name(s) of ASA *(In case of multiple ASAs, please provide their names)*	1. _____ 2. _____ 3. _____	
(b) Declaration by the ASA(s) agreeing to provide its/their secure network connectivity and related services for the performance of authentication		

INDEX

(Please attach letter of ASA in original)	
4. Authentication requirements	
(a) Territorial extent for use of Authentication facility	☐ Whole of India ☐ Name of State(s) and Union Territory(s):
(b) Whether Authentication will be used to establish identity for carrying out financial transaction	☐ Yes ☐ No
(c) Device form factor *(select one or more option)*	☐ Discrete Biometric Device ☐ Integrated Biometric Device ☐ Laptop/Desktop ☐ Mobile phone
(d) Whether Authentication will be operator-assisted or by the user himself/herself *(select one or more option)*	☐ Operator-assisted use ☐ Self-use
(e) Mode of Authentication *(selectone or more option)*	☐ Demographic ☐ OTP ☐ Fingerprint ☐ Iris ☐ Face
(f) Connectivity supported between AUA/KUA and ASA *(selectone or more option)*	☐ VPN ☐ Leased line ☐ Other; Please specify: _____
(g) Confirmation that the applicant has perused and understood UIDAI's Information Security Policy – External Ecosystem – Authentication User Agency/ KYC User Agency v6.0 *(Copy of the said policy document, after*	☐ Yes ☐ No

INDEX

affixing the signatures of the authorised signatory, to be attached)	
(h) Confirmation that the applicant has perused and understood UIDAI's Model Privacy Policy for Protecting Personal data of Aadhaar Number Holders by Requesting Entities *(Copy of the said policy document, after affixing the signatures of the authorised signatory, to be attached)*	☐ Yes ☐ No
(i) Confirmation that the applicant has executed Declaration and Undertaking annexed as Annex 1A *(Attach duly filled and signed Declaration and Undertaking)*	☐ Yes ☐ No

Declarations and Undertakings:

It is hereby declared that the information furnished in this application form is true and correct to the best of its knowledge and that no material particulars or information have been concealed or withheld,and that the _____ (name of applicant Ministry/Department/secretariat/office/agency/entity) hereby undertakes—

(a) to abide by the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") and the regulations made thereunder;

(b) to facilitate, on receipt of in-principle approval from UIDAI, audit as per UIDAI "Compliance Checklist for On boarding the Requesting Entity" and submit all compliance related documents attached as annexures before signing the AUA/KUA Agreement;

(c) to fulfil all requirements with respect to use of the Aadhaar Authentication facility as per the Aadhaar (Authentication and Offline Verification) Regulations, 2021;

(d) to set up and maintain within the territory of India, at all times, requisite infrastructure (including, but not limited to, servers, databases etc.) for the use of Aadhaar Authentication facilities, capable of handling a minimum of one lakh Authentication transactions per month;

(e) to carry out appropriate due diligence before engaging any sub-contractor, business correspondent or field operator for performing any functions in relation to the use of Aadhaar Authentication facilities, including onboarding of user/beneficiary/customer, Authentication application development, etc.;

(f) to store Aadhaar numbers, if authorised so to do, only in the Aadhaar Data Vault, in accordance with such policies, procedures, standards and technical specifications as UIDAI may specify from time to time;

(g) to ensure the carrying out of audit of its own operations and systems and those of its Sub-AUAs and Sub-KUAs, if any, as required under the Aadhaar Act, the regulations made thereunder and the AUA Agreement;

(h) to not share or disclose e-KYC data that may be received on use of e-KYC Authentication facility, except in accordance with the provisions of the Aadhaar Act and the regulations made thereunder;

(i) to furnish such other declaration and undertaking regarding the general character of management and financial condition of the applicant including any of the members of its management in the form as the UIDAI may specify from time to time in this behalf; and

(j) to inform UIDAI forthwith of any change in the name, address and other particulars of the applicant and contact persons as furnished in this application form.

(Signature with stamp/seal of authorised signatory)

Name: _____

Full designation: _____

Date: _____

Place: _____

INDEX

Annex 1A

(To be submitted on the official letterhead of the applicant entity)

Declaration and Undertaking

To:

The Chief Executive Officer, Unique Identification Authority of India
[Attention: Deputy Director (Authentication-II), UIDAI]
UIDAI Head Office, Bangla Sahib Road
Gole Market, New Delhi – 110 001

Subject: Declaration and undertaking regarding general character of management and financial condition of _____[1]

We, _____[2] hereby submit this declaration and undertaking in compliance with sub-regulation (6) of regulation 12 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021.

2. We hereby confirm and declare the following regarding the general character of management and the financial condition of _____[3]:

Part A: General Character of Management	
I. Proceeding, if any, against the applicant entity or management of the applicant entity (*in past 3 years*)	
(a) The applicant entity has been appointed as a requesting entity with UIDAI earlier.	☐ Yes ☐ No
(b) If yes, any disincentive imposed on the applicant entity earlier.	☐ Yes ☐ No
(c) Any member of the management has been debarred or disqualified under the mentioned law (i) (ii) (iii) (iv)	☐ The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations framed thereunder ☐ The Information Technology Act, 2000 read with Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ☐ The Digital Personal Data Protection Act, 2023 (*pending*)

[1]Name of applicant Ministry/Department/secretariat/office/agency/entity
[2]Name of applicant Ministry/Department/secretariat/office/agency/entity
[3]Name of applicant Ministry/Department/secretariat/office/agency/entity

	☐ The Prevention of Money Laundering Act, 2002 ☐ The Telecommunication Act, 2023 ☐ The Indian Penal Code, 1860 or the Bharatiya Nyaya Sanhita,2023 ☐ Any other law, specify, _____ _____ _____ *(if yes, certified copy of the relevant orders/decree of conviction or acquittal or as on date status of it, be attached)*
(d) Details of disciplinary action, if any, pending or commenced or resulting in conviction in the past against any member of the management or whether any member of the management has been debarred from entry at any profession/occupation at any time	☐ Yes ☐ No *(if yes, certified copy of the relevant orders/decree of conviction or acquittal or debarment or as on date status of it, be attached)*
(e) Details of prosecution, if any, pending or commenced or resulting in conviction in the past against any member of the management	☐ Yes ☐ No *(if yes, certified copy of the relevant orders/ decree of conviction or acquittal or as on date status of it, be attached)*
(f) Whether the applicant entity or any member of the management of it attracts dissociation in the past or any disqualification by or has to come to the adverse notice of the concerned or any regulator	☐ Yes ☐ No *(if yes, certified copy of the relevant orders of such disqualification or adverse notice of any member of management of applicant entity by any regulator or as on date status of it, be attached)*
(g) Whether the applicant entity or any member of the management has been subject to any investigation at the instance of the Government department or agency	☐ Yes ☐ No *(if yes, certified copy of the relevant orders of such investigation by the Government department or agency concerned or as on date status of it, be attached)*
(h) Any other explanation / information	

INDEX

regarding above or any other information considered relevant for assessing 'fit and proper', provide details thereof	
(i) The applicant entity has consistently complied with the applicable laws, regulations and guidelines including those pertaining to data protection, information security and statutory obligations	☐ Yes ☐ No (*if yes, copy of the said policy document, if any, after affixing the signatures of the authorised signatory, to be attached*)
(j) The applicant entity has a strong information security policy defining checks and balances to ensure ethical and lawful handling of sensitive data	☐ Yes ☐ No (*if yes, copy of the said policy document, after affixing the signatures of the authorised signatory, to be attached*)
(k) The applicant entity has been convicted of or plead guilty to or *nolo contendere* with respect to any offence that involves moral turpitude	☐ Yes ☐ No (*if yes, certified copy of the relevant orders/decree of conviction or acquittal or as on date status of it, be attached*)
Note: The applicant entity shall not be eligible to be appointed as requesting entity of UIDAI until: *(i) a period of 5 years has not elapsed from the date of imposition of disincentives/penalty on the applicant entity by UIDAI;* *(ii) a period of 5 years has not elapsed from the date of expiry of any sentence resultant of conviction or disqualification of applicant entity or its management under any law for the time being in force; and/or* *(iii) a period of 5 years has not elapsed since the date the applicant entity or its management is disqualified by or disassociated by the regulator concerned.*	
Part B: Financial Condition	
(a) Audited financial statements[4] for the last three years (*certified copy to be attached*)[5]	☐ Yes ☐ No
(b) Certificate of good financial standing issued by a recognised authority or auditor (*copy to be attached*)	☐ Yes ☐ No
(c) The applicant entity has been declared insolvent and has filed for bankruptcy or has been declared insolvent by any court or tribunal or the management of the affairs of the applicant entity has been entrusted to a receiver	☐ Yes ☐ No (*if yes, certified copy of the relevant orders/decree declaring the entity as insolvent or bankrupt or appointment of receiver or as on date status of it, be*

[4]For this, "financial statement" means financial statement as defined under sub-section (40) of section 2 of the Companies Act, 2013

[5]Copy of financial statement to be attached in the form as laid down under Schedule III of the Companies Act, 2013

INDEX

	attached)

Declaration and Undertaking:

It is hereby declared that the information furnished above is true and correct to the best of its knowledge and that no material particulars or information have been concealed or withheld, and that the _____[6] hereby undertakes —

(a) to adhere to the highest, ethical and legal standards of integrity and probity;

(b) to ensure that members of management or key managerial personnel is not involved in any fraudulent or illegal activities;

(c) to comply with all applicable laws, including data protection laws;

(d) to abide by the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") and the regulations made thereunder;

(e) to be financially sound and capable of investing in the necessary infrastructure and measures to ensure secured operations as a requesting entity; and

(f) to implement appropriate safeguards, policies, and procedures to protect Aadhaar related data and ensure privacy of individuals.

(Signature with stamp/seal of authorised signatory)

Name: _____

Full designation: _____

Date: _____

Place: _____

[6]Name of applicant Ministry/Department/secretariat/office/agency/entity

INDEX

F. No. HQ-13081/6/2024-AUTH-II HQ/C. 15832
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated: 18 March 2025

Circular 4 of 2025

Subject: Guidelines on requiring Aadhaar number in the interest of good governance, preventing leakage of public funds, promoting ease of living of residents and enabling better access to services by them for the purposes prescribed under sub-rule (1) of rule 3 of the Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020

Unique Identification Authority of India (UIDAI) *vide* the Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020 ["SWIK Rules"] allows Aadhaar Authentication by requesting entities for the following purposes, namely: -

(a) usage of digital platforms to ensure good governance;
(aa) promoting ease of living of residents and enabling better access to services for them;
(b) prevention of dissipation of social welfare benefits; and
(c) enablement of innovation and the spread of knowledge.

2. If any Department or entity belonging to the State Government is desirous of utilizing Aadhaar Authentication facility on voluntary basis for any of the above-mentioned purposes it may submit such proposal to the Ministry of Electronics and Information Technology ["MeitY"], Government of India, which in consultation with UIDAI and in the interest of State, may allow such a requesting entity to perform Aadhaar Authentication under section 4(4)(b)(ii) of the Aadhaar (Targeted Delivery of Financial and Other Subsides, Benefits and Services) Act, 2016 [Aadhaar Act]. The requesting entity after the approval, gets its purpose notified in the Gazette of India for availing Aadhaar authentication facility.

3. UIDAI has been receipt of numerous gazette notifications wherein following key ingredients of the sub-clause (ii) of clause (b) of sub-section (4) of section 4 of the Aadhaar Act read with rule 3 of the SWIK Rules are missing:

(a) Informed Consent;
(b) Voluntary; and
(c) Alternative and viable means of identification

INDEX

4. Therefore, Ministry or the Department of the Government of India or the State Government desirous of utilising Aadhaar Authentication for a purpose specified in rule 3 of the SWIK Rules are required to issue a notification including following points: -

(a) The notification shall mention that the Aadhaar Authentication under the SWIK Rules shall be on voluntary basis;
(b) The notification shall mention that for Aadhaar Authentication under the SWIK Rules, informed consent of the Aadhaar number holder shall be obtained with respect to the manner in which the Aadhaar number shall be collected and stored and uses to which the information received during authentication may be put to;
(c) The notification shall mention that the Aadhaar number holder shall be informed of alternate and viable means of identification or verification so that no subsidy, benefit or service shall be denied to the Aadhaar number holder on account of refusing to, or being unable to, undergo authentication.

5. Basis above, a sample template for a notification pursuant to section 4(4)(b)(ii) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 may be used for the issuance of a notification pursuant to requirement of Aadhaar number under section 4(4)(b)(ii) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, is attached as Annexure-A.

6. *It is also requested that as and when any notification as aforesaid is issued, a copy of the published notification may be mailed to UIDAI at notification.auth-hq@uidai.net.in for information. Further, for any queries regarding the same, you are requested to mail to UIDAI at onboarding@uidai.net.in.*

7. A copy of this Circular is available on UIDAI's website https://uidai.gov.in/en/ecosystem/authentication-devices-documents/authentication-document.html.

8. This issues with the approval of competent authority.

(Sanjeev Yadav)
Director
Tel.: 011-23478609
Email: dir2.auth-hq@uidai.net.in

To:
1. Secretaries in charge of Ministries and Departments in Government of India (as per list attached)
2. Chairperson and Chief Executive Officer, Railway Board
3. Chief Secretaries of State Governments (as per list attached)

INDEX

4. Chief Secretary, Government of Jammu and Kashmir / National Capital Territory of Delhi / Puducherry / Andaman and Nicobar Islands Administration
5. Advisor to Administrator, Chandigarh Administration
6. Advisor to Lieutenant Governor, Ladakh Administration
7. Administrator, Dadra and Nagar Haveli and Daman and Diu Administration / Lakshadweep Administration

Copy, for information, to:

1. Advisor to Prime Minister, Prime Minister's Office
2. Chief Executive Officer, NITI Aayog
3. Secretary (Coordination), Cabinet Secretariat
4. All Deputy Directors General, UIDAI
5. All Authentication User Agency and e-KYC User Agency

INDEX

Sample template for a notification pursuant to Rule 5 of The Aadhaar authentication for good Governance (Social Welfare, Innovation, knowledge) Rules, 2020 read with section 4(4)(b)(ii) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

[TO BE PUBLISHED IN _____[1]]

Government of _____[2]
_____[3]

Notification

_____[4], the _____[5], 20__[6]

S.O.____(E).—Whereas the use of Aadhaar number to establish identity enables individuals to receive subsidies, benefits and services in a convenient and seamless manner, obviates the need for multiplicity of documents to establish identity, simplifies processes and promotes transparency and efficiency:

And whereas the Ministry of Electronics and Information Technology, Government of India, after consultation with the Unique Identification Authority of India (UIDAI), had allowed *vide* its letter no. _____, dated _____ to the _____[7] (hereinafter referred to as the said Ministry or the said department or the said Agency), Government of _____[8] (hereinafter referred to as the said Government) for the purposes prescribed under sub-rule (1) of rule 3 of the Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020 (hereinafter referred to as the said rules) that the said Government/Ministry/Department/Agency may be allowed to perform authentication and be permitted the use of Aadhaar number during authentication for establishing identity of Aadhaar number holder and notify the same under rule 5 of the said rules read with sub-clause (ii) of clause (b) of sub-section (4) of section 4 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereinafter referred to as the Act):

And whereas, the Aadhaar authentication shall be performed for _____ (hereinafter referred to as the said purpose) as prescribed under sub-rule (1) of rule 3 of the said rules and the performance of Aadhaar authentication for the said purpose shall be on voluntary basis and that the said Ministry/Department/Agency shall perform the Aadhaar authentication only for _____[hereinafter referred to as the use case(s)].

---

[1] <THE GAZETTE OF INDIA, EXTRAORDINARY, PART II, SECTION 3, SUB-SECTION (i)> *OR*, in respect of a State, appropriate reference to the Official Gazette of the State concerned
[2] <India> *OR* name of State
[3] Name of Ministry or Department or both
[4] Name of city
[5] Date and month
[6] Year
[7] Name of Ministry or Department or Agency
[8] <India> *OR* name of State

INDEX

Now, therefore, in pursuance of rule 5 of the said rules read with sub-clause (ii) of clause (b) of sub-section (4) of section 4 of the Act, the said Ministry/Department/Agency hereby notifies the following, namely: —

1. (1) The Ministry/Department/Agency, as provided in the Act, shall obtain the consent of the Aadhaar number holder for the purpose of authentication herein.

(2) As per sub-rule (2) of rule 3 of the said rules, Aadhaar authentication is on voluntary basis the Ministry/Department/Agency shall inform to the Aadhaar number holder of alternate and viable means of identification and shall not deny any service to the Aadhaar number holder for refusing to, or being unable to, undergo Aadhaar authentication, namely; —

(a) .....

(b) .....

(c) .....

(d) .....

2. This notification shall come into effect from the date of its publication in the official Gazette.

[F. no. _____]

_____ [9]

_____ [10]

[9] Name of officer

[10] Designation of officer

INDEX

F. no. HQ-13021/1/2021-AUTH-I HQ (Comp. No-16262)
Unique Identification Authority of India
(Authentication and Verification Division)
3rd floor, UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110 001
Dated 25th March 2025

To:

All requesting entities and ASAs in the Aadhaar authentication ecosystem

Subject: Phase out of existing L0 fingerprint registered devices from Aadhaar authentication ecosystem

Reference is invited to UIDAI letter no. HQ-13021/1/2021-Auth-1 HQ (Comp. No-16262), dated 29.11.2024 regarding phase out of L0 fingerprint registered devices from Aadhaar authentication ecosystem by 31.3.2025.

2. It is informed that UIDAI has already stopped whitelisting of new L0 fingerprint registered devices from 1.10.2024.

3. In this regard, the undersigned is directed to convey that—

(a) The sunset period for L0 fingerprint registered devices which are valid as per Public Device Certificate (PDC) is hereby extended to 30.6.2025. The date of hot listing of individual L0 fingerprint registered device models is indicated at 'Annexure A'.

(b) An additional fee may be levied to transactions conducted by using L0 fingerprint registered devices from 1.7.2025 onwards, in accordance with sub-regulation (7) of regulation 12 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021.

4. In view of the aforesaid, all requesting entities and ASAs are directed to take precautionary measures to complete the migration of L0 fingerprint registered devices to L1 fingerprint registered devices before the sunset timelines.

5. This supersedes all previous communications regarding to the phase out of L0 fingerprint devices from Aadhaar authentication ecosystem.

6. This issue with the approval of competent authority.

Abhijeet
Digitally signed by Abhijeet
Date: 2025.03.25 11:57:05 +05'30'

(Abhijeet)
Director
Tel.: 011-23478615
Email: dir1.auth-hq@uidai.net.in

Copy to:

1. All fingerprint device vendors
2. All UIDAI Regional Offices
3. Technology Centre, Bangalore

INDEX

UIDAI letter F. no.: HQ-13021/1/2021-AUTH-I HQ/C-16262, dated 25.3.2025

Annexure A

S. No.	Name of the Manufacturer	Device_model_id	PDC Validity	Date of Hotlisting
1	M/s Precision Biometric India Private Limited	PBCS200	16-04-2020	01-05-2025
2	M/s Bioenable Tech Pvt. Ltd.	BIOENABLE-BETPV	31-05-2020	01-05-2025
3	M/s Smartchip India Pvt Ltd	MSO1300E2L0SW	07-02-2022	01-05-2025
4	M/s Matrix Comsec Pvt Ltd	MCP.FAX.500OH.E	25-09-2023	01-05-2025
5	M/s Matrix Comsec Pvt Ltd	MCP.FOT.500OH.E	25-09-2023	01-05-2025
6	M/s Secugen India Pvt Ltd	HU20A	03-01-2025	01-05-2025
7	M/s Evolute Systems Pvt Ltd	LEOPARD	31-01-2025	01-05-2025
8	M/s Evolute Systems Pvt Ltd	FALCON	31-01-2025	01-05-2025
9	M/s Evolute Systems Pvt Ltd	IDENTI5	31-01-2025	01-05-2025
10	M/s Smartchip India Pvt Ltd	MSO1300E3L0SW	31-01-2025	01-05-2025
11	M/s. Mantra Softech (India) Pvt Ltd	MFS100	03-05-2025	01-06-2025
12	M/s. Access Computech Pvt. Ltd	FM220U	03-05-2025	01-06-2025
13	M/s Integra Micro Systems Pvt Ltd	IMS.IMS.MF100.A	19-09-2025	01-07-2025
14	M/s Integra Micro Systems Pvt Ltd	IMS.VTK.TCS1S.E	19-09-2025	01-07-2025
15	M/s Integra Micro Systems Pvt Ltd	IMS.AQT.TCS1S.A	19-09-2025	01-07-2025
16	M/s Integra Micro Systems Pvt Ltd	IMS.ANA.TCS1S.E	19-09-2025	01-07-2025
17	M/s Integra Micro Systems Pvt Ltd	IMS.AQT.TCS1S.W	19-09-2025	01-07-2025
18	M/s Integra Micro Systems Pvt Ltd	IMS.ARA.A600.W	19-09-2025	01-07-2025
19	M/s Integra Micro Systems Pvt Ltd	IMS.PAX.A400.A	19-09-2025	01-07-2025
20	M/s Integra Micro Systems Pvt Ltd	IMS.VTK.1300E.E	19-09-2025	01-07-2025
21	M/s Integra Micro Systems Pvt Ltd	IMS.ANA.1300E.E	19-09-2025	01-07-2025
22	M/s Linkwell Telesystems	VTK.VA21POS.TCS1S.A	08-11-2025	01-07-2025
23	M/s Linkwell Telesystems	VTK.Q2POS.TCS1S.A	08-11-2025	01-07-2025
24	M/s Aratek	A400	11-12-2025	01-07-2025
25	M/s Aratek	A600	11-12-2025	01-07-2025
26	M/s Evolute Systems Pvt Ltd	EVOLUTEFPSA600	11-12-2025	01-07-2025
27	M/s Secugen India Pvt Ltd	HU20AP	01-06-2026	01-07-2025
28	M/s Secugen India Pvt Ltd	HU10	01-06-2026	01-07-2025
29	M/s Secugen India Pvt Ltd	HU20	04-10-2026	01-07-2025
30	M/s Linkwell Telesystems	VTK.GL11.A600.E	29-11-2026	01-07-2025
31	M/s Linkwell Telesystems	VTK.VA21POS.A400.A	29-11-2026	01-07-2025
32	M/s Precision Biometric India Private Limited	PB510	29-11-2026	01-07-2025

Abhijeet Digitally signed by Abhijeet Date: 2025.03.25 11:57:54 +05'30'

(Abhijeet)
Director
Tel.: 011-23478615
Email: dir1.auth-hq@uidai.net.in

INDEX

F. no. HQ-13021/1/2021-AUTH-I HQ (Comp. No-16262)

Unique Identification Authority of India

(Authentication and Verification Division)

3rd floor, UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110 001
Dated 16th April 2025

To:

All requesting entities and Authentication Service Agencies in the Aadhaar authentication ecosystem

Subject: Technical and functional upgrade of fingerprint L1 registered devices

Please refer to UIDAI letters no. HQ-13021/1/2021-Auth-1 HQ, dated 1.11.2024, 29.11.2024 and 07.01.2025 regarding cited subject.

2. In this regard, the undersigned is directed to convey that:

(a) the whitelisting of M/s. Precision Biometric India Pvt Ltd (Model – PB1000/PB510) with RDS version 1.2.3 and M/s. Access Computech Pvt. Ltd (Model - FM220UL1/CMOS) with RDS version 1.3.2 are hereby allowed with immediate effect.

(b) the RD Service, NXP.IDEMIA.001 for M/s Smart Chip Pvt. Ltd. fingerprint L1 registered device (Model - MSO 1300 E3 RD/CBME3RD) has been upgraded from RDS version 1.1.1 to RDS version 1.1.3

3. UIDAI vide letter no. HQ-13021/1/2021-Auth-1 HQ, dated 01.02.2025 & 06.03.2025 has already allowed the whitelisting of five fingerprint L1 registered device models.

4. The complete list of fingerprint L1 registered device models for which whitelisting has been allowed till date is as follows:

S. No	Device Supplier	Device Model No. (Sensor)	Latest RDS Version
1	M/s. Mantra Softech (India) Pvt. Ltd.	MFS110 (MOPv110)	1.3.0
2	M/s. Mantra Softech (India) Pvt. Ltd.	MARC11 (MOPvC11)	1.2.0
3	M/s. Smart Chip Pvt. Ltd.	MSO 1300 E3 RD (CBME3RD)	1.1.3
4	M/s. Linkwell Telesystems Pvt. Ltd	V400 (V400-M)	1.1.3
5	M/s. Access Computech Pvt. Ltd	AST300 (NB-65210-S)	1.3.2
6	M/s. Access Computech Pvt. Ltd	FM220UL1 (CMOS)	1.3.2
7	M/s Precision Biometric India Pvt Ltd	PB1000 (PB510)	1.2.3

4. All requesting entities are hereby requested to ensure that the RD service of the existing L1 fingerprint registered devices is upgraded to their latest RDS version as mentioned above.

5. UIDAI recognizes the importance of smooth and efficient transition to L1 fingerprint registered devices. The stipulated sunset date of L0 fingerprint registered devices is 30.06.2025 or Public Device Certificate validity whichever is earlier. For ensuring the uninterrupted services at your end, it is requested to take all precautionary measures to complete the migration process within date as indicated above.

6. This issues with the approval of competent authority.

Abhijeet

Digitally signed by Abhijeet
Date: 2025.04.16 11:05:31 +05'30'

(Abhijeet)
Director

INDEX

UIDAI letter F. no.: HQ-13021/1/2021-AUTH-I HQ/C-16262, dated 16th April 2025

Copy to:

1. All UIDAI Regional Offices
2. Technology Centre, Bangalore
3. M/s. Smart Chip Pvt. Ltd, M/s. Precision Biometric India Pvt Ltd & M/s. Access Computech Pvt. Ltd. — *directed to push latest RDS version to their already whitelisted devices of above-mentioned respective models.*

F. No. HQ- HQ-13014/1/2024-AUTH-I HQ/C-14670
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road,
Gole Market, New Delhi – 110 001
Dated 5th May 2025

To,
All Authentication user agency (AUA)/e-KYC user agency (KUA)

Subject: Annual declaration to be submitted by AUA/KUA for a financial year

Sir/Madam,

Reference is invited to Circular 02 of 2025 dated 7 February 2025, wherein the revised application and undertaking for the appointment of Sub-AUAs/Sub-KUAs were issued by UIDAI.

2. Attention is specifically drawn to Paragraph 4 of Annexure-II of the aforementioned circular, which mandates that AUAs/KUAs must ensure their Sub-AUAs/Sub-KUAs undergo an annual Information System (IS) audit conducted by a CERT-In empaneled auditor. This audit is to verify compliance with UIDAI's standards and specifications, and the report must be submitted to UIDAI upon request.

3. It has been repeatedly emphasized through email communication that all entities must submit an undertaking confirming that all Sub-AUAs/Sub-KUAs mapped to the respective AUA/KUA have been audited annually by a CERT-In empaneled auditor and no non-compliances exist for any Sub-AUA/Sub-KUA in audited financial year.

4. Considering the above, UIDAI hereby issues the enclosed standard undertaking format to be duly completed and submitted by all AUAs/KUAs annually on or before closing of audited financial year. For financial year 2024-25, addressed AUA's are requested to submit the required undertaking in the given format by 30th June 2025.

5. This issued with the approval of Competent Authority.

Yours faithfully,

(Pratik Choudhary)
Deputy Director
Tel: 011- 23478608
Email: dd1.auth-hq@uidai.net.in

INDEX

Undertaking format for AUA/KUA

(To be printed on letter head of AUA / KUA)

Declaration Regarding IS Audit of Sub-AUA/Sub-KUA for Financial Year_____

It is hereby declared that the following Sub AUA / Sub KUA mapped under our organization as AUA/KUA have undergone Annual Information Security audit for the financial year <F.Y.> by a CERT In empaneled audit agency. The audit report has confirmed that there are no open non-compliances for the listed entities:

S.No.	Sub AUA/Sub KUA Name
1	
2	
3	

This declaration is issued in good faith based on audit findings.

Authorized Signatory details (of AUA/KUA):

Signature:

Name:
Designation:
Organization:
Date:

INDEX

F. No. HQ-13079/5/2023-AUTH-II HQ/C-10846
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110 001
Dated 29 May 2025

Circular No. 5 of 2025

Subject: Revision of license fee for Authentication Service Agency on their transaction volume.

Reference is invited to UIDAI Circular No. 2 of 2019, dated 2.4.2019 and regulation 12(7) of the Aadhaar (Authentication and Offline Verification) Regulations, 2021, wherein 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.

2. In this regard, I am directed to convey, that—

(a) the license fee for Authentication Service Agency (ASA) shall be levied on the basis of transactions per annum of ASA. These transactions will be calculated as per billing cycle. The ASA will be required to submit the undertaking (attached as Annexure-I) along with the application form as per the slabs mentioned under:

S. No.	Volume of authentication Transactions performed by ASA per annum	Applicable License Fee Payable by ASA (existing /new entities)	Validity	Bank Guarantee with validity of 10 years to be submitted by the ASA during the time of application
(i)	upto 10 crore transactions	₹20 Lakh + GST	2 years	₹50 Lakh + GST
(ii)	between 10 to 20 crore transactions	₹40 Lakh + GST		
(iii)	20 crore and above transactions	₹60 Lakh + GST		

(b) any delay in deposit of renewal of license fees beyond the due date by existing ASAs will attract late payment charges @1% of license fees per month or part thereof along with GST @18% thereupon. Further, non-payment of license fee may also lead to immediate suspension of license key;

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

IN ADD.
INDEX

(d) to consider extending ASA services to other AUAs/KUAs to optimize the utilization of its existing infrastructure, contributing significantly to enhancing the accessibility and efficiency of Aadhaar authentication services for a broader spectrum, as enshrined under regulation 19 (i) of the Aadhaar (Authentication and Offline Verification) Regulations, 2021 regarding the roles, responsibilities and code of conduct of an ASA; the ASA at all times; and

(e) to have dual redundant connectivity, which is essential for ensuring high availability and failover support with sufficient MPLS bandwidth in proportion to existing load for ensuring of uninterrupted services.

3. The entities will be on-boarded initially on the basis of transaction estimates provided by them and license fees will be charged as per the applicable slab as mentioned above. However, at the time of subsequent renewal if the entity is found to have performed higher number of transactions, then differential amount of license fees of higher slab as mentioned above will be recovered along with interest @18% per annum. Such a provision is warranted in order to enable UIDAI to plan for the infrastructure requirements based on the number of expected authentication transactions. Any wide variation in projected number of authentication transactions may potentially affect the entire authentication ecosystem. Further, if the entity would have performed lesser number of transactions compared to initially submitted transactions estimate, no benefit of lower slab will be admissible. Hence, entities are advised to provide their estimates carefully.

4. The existing or prospective ASAs are advised for the strict compliance of the above. The terms and conditions mentioned above, shall come in force with immediate effect.

5. This issues with the approval of competent authority.

(Sanjeev Yadav)
Director
Tel. 011-23478609
Email: dir2.auth-hq@uidai.net.in

INDEX

F. No. HQ-13079/5/2023-AUTH-II HQ/C-10846
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110 001
Dated 29 May 2025

Circular No. 6 of 2025

Subject: Streamlining the process of onboarding of Authentication Service Agency (ASA) with revised ASA Agreement and compliance checklist.

To streamline the process of onboarding of ASA, further to bring it inline with the current AUA onboarding, to fasten the process of onboarding of ASA and to make more resilient infra of ASA, there is a need to revise the framework of onboarding of ASA. In this regard, the revised version of documents are attached as mentioned below:

(a) Revised ASA application form **(Annex-I)**

(b) ASA agreement V 6.0 **(Annex-II)**

(c) Compliance Checklist for certifying compliance with controls that ASA is required to have in place (Pre Onboarding) Version 1.0 (60 controls) **(Annex-III)**

(d) Compliance Checklist for certifying compliance with controls that ASA is required to have in place Version 1.0 (102 controls) **(Annex-IV)**

(e) Undertaking of estimated ASA transactions per annum to be submitted by ASAs during the time of application. **(Annex-V)**

(f) **Circular 5 of 2025** for intimation of differential license fee pricing based on ASA transactions per annum and advisory regarding extending of ASA services to other AUAs/KUAs as well as for taking measures to ensure uninterrupted services to all ASAs. **(Annex-IV)**

2. In view of the above, it is intimated that the new onboarding and renewal shall be facilitated through the above mentioned terms and conditions, with immediate effect.

(Sanjeev Yadav)
Director
Tel. 011-23478609
Email: dir2.auth-hq@uidai.net.in

INDEX

Application form
for Appointment as Authentication Service Agency (ASA)

To:

The Chief Executive Officer, Unique Identification Authority of India
[Attention: Deputy Director (Authentication-II), UIDAI]
UIDAI Head Office, Bangla Sahib Road
Gole Market, New Delhi – 110 001

1. Details of the applicant	
(a) Name of the applicant[1]	
(b) Registration/ Incorporation No.[2] *(Please attach copy of the document, if applicable)*	
(c) License No.[3] *(Please attach copy of the document, if applicable)*	
(d) Registered office address	
(e) Correspondence address *{If other than address mentioned against (d)}*	
(f) GSTN registration number of the applicant, as per Form GST REG-06 *(Please attach copy of the document, if applicable)*	
(g) Tax Deduction and Collection Account Number (TAN) of the applicant (*Please attach copy of the document, if applicable*)	
(h) Board resolution/minutes (or other valid letter/instrument of authorisation) citing approval for submitting the application form, signing Authentication Service Agency Agreement and doing other acts in relation to the same *(Please attach certified copy of the document)*	
(i) Category of the applicant *(Tick the applicable box)*	☐ **Category 1:** A Ministry or Department of the Central Government or a State Government, or an undertaking owned or controlled by the Central Government or a State Government ☐ **Category 2:** An authority constituted under any Central or State Act

1 Name of the applicant Ministry, Department, secretariat, office or agency of the Central Government or the Government of State or Union territory, or other applicant entity
2 Copy of Certificate of incorporation/registration to be attached in case of "other than Govt. entities"
3 Copy of Certificate of Registration/License from the concerned Regulator issued from RBI, SEBI, IRDAI and PFRDA

INDEX

	☐ **Category 3:** Any other entity of national importance in the opinion of the Authority ☐ **Category 4:** A company registered in India under the Companies Act, 2013 (18 of 2013) ☐ **Category 5:** An AUA or a KUA
(ia) Financial or technical requirement *(tick boxes in case applicant ticks against category 4)*	☐ **Financial requirement:** Annual turnover of at least ₹100 crore as per the audited financial statements for last three financial years; and **Technical requirement:** ☐ A Telecom Service Provider {Unified Licensee having Access Services authorisation or Unified Access Services Licensee, granted licence under section 4 of the Indian Telegraph Act, 1885 (13 of 1885)}, having a minimum of 100 Multiprotocol Label Switching (MPLS) Points of Presence (PoP) in India. OR ☐ A Network Service Provider or System Integrator having pan-India network connectivity for data transmission, having at least 100 MPLS PoPs in India.
(ib) Technical requirement *(tick box in case applicant has ticked against category 5)*	☐ **Technical requirement:** An AUA or KUA that meets such authentication transaction criteria as the Authority may determine from time to time.
2. Contact details:	

(a) Details of Key Managerial Personnel (KMP)[4]		
Name:		
Full designation:		
Official email address:		
Mobile number:		
Alternate office telephone number:		
(b) Details of Chief Information Security Officer (CISO)		
Name:		
Full designation:		
Official email address:		
Mobile number:		
Alternate office telephone number:		
(c) Details of Management Point of Contact (MPOC)	Person authorised on the basis of Board resolution/minutes (or other valid letter/instrument of authorisation)	Other key personnel (if any)

4 For the purpose of this "Key Managerial Personnel (KMP)" means a KMP as defined under sub-section (51) of section 2 of the Companies Act, 2013

INDEX

E - AUTHENTICATION & VERIFICATION

Name:		
Full designation:		
Official email address:		
Mobile number:		
Alternate office telephone number:		
(d) Details of Technical Point of Contact (TPOC)	CXO/ Head of the functional vertical, who reports to the chief executive or governing body of the applicant Ministry/ Department/secretariat/office/agency/entity	Other key personnel (if any)
Name:		
Full designation:		
Official email address:		
Mobile number:		
Alternate office telephone number:		
(e) Details for Grievance redressal		
Website URL		
Email address		
Helpdesk number		
Designated Grievance Officer Name		
Grievance Officer Mobile No.		
Grievance Officer E-Mail ID		
ASA infrastructure details		

(f) Proposed location(s) within India for installation of ASA servers, hardware, equipment etc used for Aadhaar authentication *(Please specify multiple districts/states in case of Primary, Secondary, DR sites etc.) with the minimum specification for the server grade hardware as follows:*

i. *Each server has 4 CPU cores*
ii. *32-64 GB Memory*
iii. *1TB Storage (recommended)*

Site	*District*	*State*

DC (Data Centre)	DR (Data Recovery Centre)
MPOC/TPOC Name – Email address Telephone/Mobile No. Address District –	MPOC/TPOC Name – Email address Telephone/Mobile No. Address District –

INDEX

E - AUTHENTICATION & VERIFICATION

	State- Country-	State- Country-
(g)	No. of leased lines planned at UIDAI DC *(It is highly recommended that ASAs create dual redundant leased line connectivity to both UIDAI data centre to provide AUAs with highest service availability)*	☐ 2 each at Manesar and Hebbal Data Centre (Recommended) ☐ 1 each at Manesar and Hebbal Data Centre ☐ 2 at Manesar and 1 at Hebbal Data Centre ☐ 1 at Manesar and 2 at Hebbal Data Centre
(h)	Connectivity supported between AUAs/KUAs & ASA *(select one or more option)* *This could be any kind of secured network depending on the needs of AUAs. UIDAI recommends that this be a private leased line to have better control of availability, bandwidth, reliability, and security*	☐ MPLS ☐ Leased line *[No. of links at least: 8 (Recommended)* *- 2 Primary, 2 Secondary link for MDC and HDC at ASA DC site* *- 2 Primary, 2 Secondary link for MDC and HDC at ASA DR site]*
(i)	Name of leased line service provider *(Can select multiple options – this is an indicative list; additional names may be added in the Others category)*	☐ BSNL / MTNL ☐ Jio ☐ Airtel ☐ Tata ☐ Vodafone-Idea Ltd ☐ Others,_____
(j)	Planned leased line capacity (in Mbps): *[At least 20 Mbps each link depending on the transaction load]*	
(k)	IP Address(es) to be whitelisted	
(l)	Expected authentication transaction volume *(tick against the applicable box)*	☐ Less than 5,00,000 per day ☐ 5,00,000 - 25,00,000 per day ☐ 25,00,000 - 1,00,00,000 per day ☐ More than 1,00,00,000 per day
(m)	Name of Router make & model to be deployed at CIDR Partner DMZ having following hardware: a. Rack mountable 19" standard b. Minimum 1G interfaces c. Redundant Router at each DC d. Redundant Power supply for each Router	
AUA/KUAs Related Information		
(n)	Geographies Catered/ Territorial extent for use of Authentication facility (Please specify states in case multiple states / single state selected)	☐ Whole of India ☐ Name of State(s) and Union Territory(s):
(o)	AUA/KUA Supported *(Select any one option)*	☐ Self as AUA/KUA only ☐ Other entities as AUA/KUA only ☐ Self as AUA/KUA and Other entities as AUA/KUA

INDEX

(p)	Details of DC/DR certification *(please attach certificate)*	
(q)	Details of Audit certificate with reports	
(r)	Published Data Privacy Policy in line with UIDAI requirements and IT Act 2011	
(s)	Details of fraud monitoring capabilities	
(t)	Confirmation that the applicant has perused and understood UIDAI's Information Security Policy –External Ecosystem – Authentication Service Agency v6.0 *(Copy of the said policy document, after affixing the signatures of the authorised signatory, to be attached)*	☐ Yes ☐ No

Declarations and Undertakings:

It is hereby declared that the information furnished in this application form is true and correct to the best of its knowledge and that no material particulars or information have been concealed or withheld, and that the _____[5] hereby undertakes—

(a) to abide by the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") and the regulations made thereunder;

(b) to facilitate, on receipt of in-principle approval from UIDAI, audit as per UIDAI Compliance Checklist for Onboarding the ASA and submit all compliance related documents attached as annexure before signing the ASA Agreement;

(c) to fulfil all requirements with respect to use of the Aadhaar Authentication facility as per the Aadhaar (Authentication and Offline Verification) Regulations, 2021 including financial/technical requirement defined in Schedule A;

(d) to set up and maintain within the territory of India, at all times, requisite infrastructure (including, but not limited to, servers, databases etc.) for the use of Aadhaar Authentication facilities, capable of handling Authentication transactions of AUA/KUA and their Sub-AUAs/Sub-KUAs per month with minimum additional capacity of 25%, maintaining logs and white listed IP Address (es);

(e) to ensure carrying out of audit of its own operations and systems, as required under the Aadhaar Act, the regulations made there under and the ASA Agreement;

(f) to ensure roles, responsibilities and code of conduct of ASA, as required under the Aadhaar Act, the regulations made there under and the ASA agreement;

(g) to inform UIDAI forthwith of any change in the name, address and other particulars of the applicant and contact person as furnished in this application form.

(Signature with stamp/seal of authorised signatory)

[5] Name of applicant

INDEX

Name: _____
Full designation: _____

Date: _____
Place: _____

INDEX

Annex II

[Agreement to be drawn on non-judicial stamp paper of value as applicable. Please follow the guidelines given in referenced footnotes regarding filing up of underscored blank portions in this draft. Wherever guidance includes one or more text options bracketed by symbols "<" and ">", relevant option should be used without modification. Strike out guidance and inapplicable text options.]

AUTHENTICATION SERVICE AGENCY AGREEMENT

This Agreement ("hereinafter referred to as "**Agreement**") is entered into by and between:

UNIQUE IDENTIFICATION AUTHORITY OF INDIA, a statutory authority established under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ["**Act**"], having its Head Office at New Delhi (current address: Aadhaar Building, Bangla Sahib Road, Gole Market, New Delhi 110001) (hereinafter referred to as "**UIDAI**" or "**Authority**", which expression shall, unless the context otherwise requires, include its authorised representatives and successors), of the **First Part**;

AND

_____[1], a _____[2] _____[3] and having its registered office at _____ (hereinafter referred to as "ASA"), acting through its authorised representative, _____[4], authorised *vide* _____[5] of _____[6] to enter into and execute this Agreement, which expression shall, unless the context otherwise requires, include its authorised representatives and such successors as UIDAI may approve, of the **Second Part**.

The parties mentioned above are collectively referred to as **'Parties'** and individually as a **'Party'**.

WHEREAS the Second Party has, under the Aadhaar (Authentication and Offline Verification) Regulations, 2021, applied to UIDAI for appointment as an Authentication Service Agency (ASA) for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility

[1]Name of the Second Party, as stated in the certificate of registration/incorporation or the law or instrument by which registered, established, constituted or incorporated

[2]<company> or <co-operative society> or <trust> or <public trust> or <society> or <firm> or <Limited Liability Partnership> or <other body corporate registered, established, constituted or incorporated by or under law>(whichever is applicable)

[3]<registered> or <established> or <constituted> or <incorporated> (whichever is applicable)

[4]Full name and full designation

[5]Full particulars, such as resolution/letter number.ate, etc

[6]<the Board of Director> or the name of other governing authority of the Second Party (whichever is applicable)

INDEX

provided by UIDAI and is desirous of entering into this Agreement that sets out the terms and conditions for use by Second Party as an ASA to UIDAI's Authentication facilities:

OR

AND WHEREAS the Parties hereto had last entered into an Authentication Service Agency Agreement, dated _____[7] (hereinafter referred to as "previous Agreement") for the use by Second Party as an ASA to UIDAI's authentication facilities and the Second Party has applied to UIDAI for the continuation of its appointment as an ASA beyond the period stipulated thereunder for the use for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility provided by UIDAI and is desirous of entering into this Agreement that sets out the terms and conditions for use by the Second Party as an ASA to UIDAI's Authentication facilities:[8]

AND WHEREAS the Second Party understands and acknowledges that the terms and conditions set out herein are in addition to and not in derogation of the powers of UIDAI and the obligations and liabilities of ASA under the Act and the regulations made thereunder:

NOW, THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

1. Definitions and Interpretation

1.1 *Definitions*

1.1.1 In this Agreement, unless the context otherwise requires, the following words and expressions shall have the meanings set out below:

(a) **"Act"** means the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and includes the rules and regulations made thereunder and such clarifications, notifications, circulars, guidelines, policies, orders, processes, standards, specifications and other documents as the UIDAI has issued or may issue, from time to time;

(b) **"Agreement"** means this Agreement and includes—

(i) The following documents submitted by the Second Party *vide* _____[9] number _____[10], dated _____[11]:

(1) Application form for appointment as ASA submitted by the Second Party ("applicant"), duly filled in, along with the correspondence in this regard with UIDAI [**Annex 1**];

---

[7] Date of previous/last agreement
[8] This does not applicable for new applicant entity
[9] <letter> or <email> (whichever is applicable)
[10] Letter number or <nil> (whichever is applicable)
[11] Date of letter/email

INDEX

(ii) The letter conveying in-principle approval to appoint the Second Party as an ASA **[Annex 2]** and checklist for—

(I) Verification of the information furnished by the Second Party, including in respect of documents, infrastructure and technological support that the applicant is required to have, done by an independent audit agency appointed by UIDAI;

(II) Other controls that the ASA is required to have in place, certifying compliance from an audit agency empanelled by the Indian Computer Emergency Response Team (CERT-In);

(iii) The report of verification of the information as per the checklist referred to in item (I) of sub-clause (ii) of clause (b) **[Annex 3]**;

(iv) The Financial Disincentives to be imposed on Authentication Service Agency under the provisions of regulation 25 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021 applicable on the Second Party, set out in **Annex 4**; and

(v) The instruments, if any, supplementing, amending, modifying or confirming this Agreement;

(c) **"Applicable Law"** means and includes the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, the rules and regulations framed thereunder and all other Acts, ordinances, rules, regulations, other laws, judgments, orders, decrees, bye-laws, notifications, circulars, guidelines, policies, protocols, codes, directives, requirements and other governmental restrictions or similar form of decision applicable to the relevant Party, as are in effect on the date of the execution of this Agreement or as may subsequently come into effect during the subsistence thereof;

(d) **"Cause"** means and includes, a determination made by the Authority regarding the occurrence of any of the following in respect of ASA:

(i) There has been a breach on the part of ASA in complying the terms of this Agreement or Applicable Law;

(ii) The ASA has been convicted of, pleading guilty to or *nolo contendere* with respect to any offence—

(I) That involves moral turpitude; or

(II) That was committed in connection with the duties to be performed by the ASA under this Agreement;

(iii) The management of the affairs of the ASA has been entrusted to a receiver; and

(iv) Any representation or warranty as given in section 8 of this Agreement is found to be materially incorrect or false.

(e) **"Confidential Information"** means all information, whether in written, oral, electronic or other form, that relates to the technical or financial data, trade, secrets, design rights, knowhow, plans, budgets and personnel of either party or their affiliates, which is disclosed to or otherwise learned by the ASA in the

INDEX

course of or in the connection with this Agreement, including but not limited to such information received during negotiations, location visits and meetings in connection with this Agreement;

(f) **"Control"** in relation to an ASA, shall, *mutatis mutandis*, have the same meaning as is assigned to it under the Companies Act, 2013;

(g) **"fees"** means and includes such fees and charges as UIDAI may, from time to time, determine as payable by ASA during its appointment, including—
(i) any application fees or subscription fees or both, as UIDAI may specify by any policy, order, process or other document issued by it under regulations made by it in respect of the procedure for authentication of the Aadhaar number and the provision thereunder for the issuance of such policy, order, process or other document, for which provision is necessary for the purpose of giving effect to such regulations;

(h) **"Financial Disincentives"** means such disincentives as UIDAI may impose on ASA under section 7 of this Agreement;

(i) **"Performance Bank Guarantee"** means the guarantee issued by a Public Sector Bank or a Private Sector Bank, categorized as such by the Reserve Bank of India, for such period as is provided for under this Agreement;

(j) **"period of the Agreement"** means the period of subsistence of this Agreement, in accordance with section 2 of this Agreement; and

(k) **"third party"** means any party who is not a Party to this Agreement.

1.1.2 Words and expressions not defined in paragraph 1.1.1 but defined in the Act and the rules and regulations made thereunder shall have the meanings respectively assigned to them therein.

1.2 *Interpretation*

1.2.1 In this Agreement, unless otherwise specified,—
(a) reference to an Annex is to be construed as reference to such annex to this Agreement;
(b) reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re-enacted;
(c) reference to any other document referred to in this Agreement, including any clarifications, notifications, circular, guideline, policy, order, process, standard, specification or checklist issued or referred to by UIDAI, is a reference, to that other document as amended, varied, novated or supplemented at any time; and
(d) all headings and titles are only for convenience and are not to be used to interpret any provision of this Agreement.

INDEX

2. Period of the Agreement

2.1 This Agreement shall be effective from the date of its execution by both the Parties and shall continue till the expiry of a period of three years from such date, unless terminated earlier.

2.2 The Agreement may be renewed for such further period or periods and upon such terms and conditions as the Parties may, by mutual consent in writing, agree upon.

3. Intellectual property

3.1 ASA is aware that UIDAI holds the copyright for the Aadhaar logo and understands that any unauthorised reproduction of the same constitutes infringement of UIDAI's rights therein and may render the person so unauthorisedly reproducing it liable under civil and criminal laws.

3.2 It is hereby mutually agreed between the Parties that all rights (including intellectual property rights), title and interests in the use of the Aadhaar logo shall, at any time, during the period of the Agreement and thereafter, vests in UIDAI and that the ASA shall only have a non-exclusive right to use the same during such period.

3.3 The ASA hereby unequivocally agrees that—

(a) It shall use the Aadhaar logo without modifying it in any manner;

(b) It shall use the Aadhaar logo only during this period of the Agreement and for promotional, educational and informational purposes related to the use of UIDAI's authentication facilities;

(c) It shall not authorize any other entity or person to use the Aadhaar logo, except with their prior permission in writing from UIDAI and in accordance with such terms and conditions as UIDAI may specify;

(d) On becoming aware of any unauthorised use, copy, infringement or misuse of the Aadhaar logo, it shall forthwith inform UIDAI, in writing, of the same and, in case UIDAI so requires, the ASA shall itself initiate legal action or proceedings, or join in or cooperate in such action or proceedings, and execute such documents and do such things as may reasonably be necessary to protect the rights, title and interests of UIDAI; and

(e) Any breach in adherence to the preceeding sub-clauses shall constitute a material breach of this Agreement.

4. Use of Aadhaar authentication facilities by ASA

4.1 Within a period of 30 days from the date of execution of this Agreement or such longer period as UIDAI may permit in writing, the ASA shall—

(a) using the license key provided by UIDAI for this purpose, carry out at least such minimum number of authentication transactions for each mode of authentication specified in **Annex 2**, in the testing environment of such Aadhaar authentication

INDEX

facility (hereinafter referred to as the "Pre-production Environment") as is specified in the said Annex.

(b) Submit a certificate from an audit agency empanelled by the Indian Computer Emergency Response Team (CERT-In), certifying compliance with the controls listed in the checklist communicated *vide* the letter placed at **Annex 2**, as referred to in item (II) of sub-clause (ii) of clause (b) of paragraph 1.1.1.

4.2 After fulfilling the obligations under paragraph 4.1 to the satisfaction of UIDAI, the ASA shall make payment of the full amount of the fees payable by the ASA to UIDAI within 15 days from the date of expiry of the period referred to in the said paragraph or such longer period as UIDAI may permit in writing, the ASA shall be allowed regular use of the said Aadhaar authentication facility in its environment intended for such use (hereinafter referred to as "Production Environment"), using a fresh license key provided by UIDAI.

4.3 If the ASA defaults in meeting any of the requirements under paragraph 4.1 or paragraph 4.2, within such period as is referred to therein,—

(a) the Agreement shall cease on expiry of that period, unless UIDAI permits otherwise in writing;

(b) the fees paid and the Performance Bank Guarantee shall be forfeited in favour of UIDAI; and

(c) no liability shall lie against UIDAI, in any manner whatsoever, in this regard.

4.4 UIDAI hereby grants the ASA a non-exclusive and revocable right to use Aadhaar authentication facilities in accordance with the terms and conditions set out in this Agreement and the provisions of Applicable Law, on the clear understanding between the Parties and that the same are in addition to and not in derogation of the powers of UIDAI and the obligations and liabilities of ASAs under the Act and the regulations made thereunder.

4.5 The ASA understands and agrees that—

(a) it shall be responsible to UIDAI for adherence to all the terms and conditions set out herein and under Applicable Law for the use of Aadhaar authentication facilities in providing necessary infrastructure for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication;

(b) if it engages any other entity for carrying out any activity connected with the use of Aadhaar authentication facilities, in the carrying out of such activity,—

(i) the responsibility for adherence as referred to in clause (a) shall continue to rest entirely with the ASA;

(ii) it shall ensure that such entity is contractually under obligations equivalent to those imposed on the ASA under the Agreement and Applicable Law and that the same are enforceable against that entity;

(iii) it shall ensure that such entity is contractually required to act only on the instructions of the ASA;

(iv) it shall ensure that the transmission to CIDR of an authentication request from a requesting entity, shall be done only by the ASA, and not directly by any such entity;

(v) it shall ensure to engage only with the requesting entities approved by UIDAI and UIDAI informed of the list of requesting entities that it serves;

(vi) it shall send the data received from UIDAI to requesting entity without any modification. If the response packet received from UIDAI is corrupted or time out occurred, ASA will send the error codes as defined by ASA to the requesting entity;

(vii) it shall ensure uptime of minimum 99.99% for its authentication facilities as well as connectivity with CIDR and requesting entity;

(viii) the ASA shall implement a Business Continuity Plan (BCP) for the Aadhaar Authentication services provided to the Res; and

(viii) it shall ensure that the operations and systems if such entity are audited in accordance with the requirements of audit as applicable to the audit of operations and systems of the ASA under the Agreement and Applicable Law.

4.6 The rights and obligations of the ASA under this Agreement are non-transferable and non-assignable, whether by sale, merger or operation of law, save and except with the concurrence or no objection of UIDAI conveyed in writing.

4.7 The ASA is aware of and understands that UIDAI's operation of the Aadhaar Authentication facilities is subject to limitations posed by technology and by changes over time in law, rules, regulations, orders of courts of competent jurisdiction, etc., and UIDAI does not represent and warrant the same to be defect-free.

4.8 The ASA is aware of and understands that the Aadhaar authentication facilities are provided on an "as is" basis, without any express or implied warranties in respect thereof, and that UIDAI does not assume any responsibility or liability for any damage, whether direct, indirect, incidental or consequential, arising as a result of the use of the said facilities.

4.9 The ASA shall 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 UIDAI may lay down from time to time.

4.10 The ASA shall not engage in any activity detrimental to the interests of UIDAI or against the interests of the sovereignty and integrity of India, the security of the State and friendly relations with foreign States,and shall exercise due diligence to prevent the engagement in such activities by any of its entity.

4.11 The ASA shall offer its Authentication services to any AUA/KUA, without discrimination, who approaches them for Authentication services.

INDEX

4.12 The ASA shall publish their pricing policy including rates of Authentication/e-KYC transactions it charges from AUA/KUA and share the same with UIDAI which may also be published by UIDAI on its website.

5. Indemnity and limitation of liability

5.1 The ASA understands that the use of authentication facilities by the ASA or any of its entity does not result in incurring of any liability by UIDAI whatsoever. The ASAalone is responsibleforthepropерandjudicioususe ofthe AadhaarAuthentication facilities. UIDAIshallnot, inanycase, be heldresponsible for damage and/orharm, directorindirect, materialor immaterial, orofany nature whatsoever,arisingfromanyunavailabilityofthe AadhaarAuthentication facilities oritsuseby any of its entity and shall remain harmless and indemnified from and against all claims, liabilities, losses and incurred costs, fines, penalties, expenses, taxes, assessments, punitive damages, fees (including advocate's fee), liabilities (including any investigative, legal and other expenses incurred in connection with, and any amounts paid in settlement of, any pending or threatened legal action or proceedings), judgments, awards, assessments, obligations, damages, etc., which UIDAI may suffer or incur arising out of, or in connection with the said use under this Agreement or under Applicable Law. The ASA shall solely be responsible to defend such claims or actions, either in a legal proceeding or otherwise, at its own cost without incurring any liability to UIDAI whatsoever.

5.2 All settlement of claims, subject to indemnification under section 5 of this Agreement, shall be entered into only with the prior consent of UIDAI, which consent shall not unreasonably be withheld. The Parties to the settlement shall be obliged to keep the terms of the settlement confidential and shall be prohibited from making any disclosure in relation to the same, unless otherwise obliged to disclose under the Applicable Law.

5.3 It is hereby mutually agreed that the said section shall survive the expiry or termination of this Agreement indefinitely.

6. Confidentiality, data protection, security and use of information

6.1 The ASA shall itself treat, and shall ensure that any of its entity are contractually bound to treat, every information disclosed to it as a result of the operation of this Agreement, and especially information about Aadhaar authentication facilities, including the related systems and operations, management and maintenance thereof, as Confidential Information, and shall maintain the confidentiality thereof. The ASA shall not, and shall ensure that all its entities are contractually bound to not, at any time, divulge such Confidential Information or any part thereof to any third party, except on being required to so by any court of competent jurisdiction in India, or as otherwise required by law for the time being in force in India, and shall also ensure that the same is not disclosed to any person voluntarily, accidentally or otherwise.

6.2 The ASA hereby unequivocally agrees to undertake all measures, including security safeguards, to ensure that the information in the possession or control of the ASA or any of its entity, as a result of operation of this Agreement, is secured and protected against any loss

INDEX

or unauthorised access or use or unauthorised disclosure thereof and that all obligations relating to the protection of such information under Applicable Law are duly fulfilled at all times by itself and that by its entity that are contractually bound, if any, to ensure such fulfillment. The ASA shall maintain the highest level of security, confidentiality and secrecy in relation to the information of the Aadhaar number holders and authentication records relating thereto.

6.3 UIDAI reserves all rights to prevent, stop and, if required, take action against the ASA for any breach of its obligations under section 6 of this Agreement.

6.4 It is hereby mutually agreed that the provision of section 6 of this Agreement shall survive the expiry or termination or cessation of this Agreement.

6.5 For the removal of doubts, it is hereby clarified that the provisions of section 6 of this Agreement shall not apply if—

(a) the information that is made or caused to be made publicly available by the person to whom it relates or by any other person who is under an obligation under any law for the time being in force in India to make the same publicly available;

(b) information which has been received from a third party who had the right to disclose the aforesaid information; or

(c) the information is required to be shared or disclosed pursuant to an order of a court of competent jurisdiction.

6.6 Any handover of Confidential Information needs to be maintained in a list, both by UIDAI and ASA, containing, at the minimum, the name of provider, recipient, date of generation of the data, date of handing over of data, form of information and signatures of both the Parties.

7. Financial Disincentives

7.1 UIDAI shall have the right to levy Financial Disincentives on the ASA as per Annex 4 subject to an annual cap of—

(a) ₹1 crore for Central/State Government/Ministry/Department and their attached or sub-ordinate offices; and

(b) ₹1 crore or 1% of Worldwide Gross Annual Turnover from all businesses whichever is more.

7.2 Such Financial Disincentives may be recoverable by UIDAI by, *inter alia*, invoking the Performance Bank Guarantee, in case of any breach of this Agreement. The Financial Disincentives, if and when imposed upon ASA, shall be an admitted liability and the ASA shall not raise any defence against the claim of UIDAI for recovery of such Financial Disincentives. The levying of Financial Disincentives shall be without prejudice to UIDAI's right to terminate this Agreement.

7.3 UIDAI shall designate an officer not below the rank of a Deputy Director General in UIDAI to determine and levy Financial Disincentives, which shall be final and binding upon the ASA.

8. Representations and warranties of the ASA

8.1 The ASA represents and warrants to UIDAI that—

(a) It is duly established and validly exists under the Applicable Law and has full power and authority to execute and perform its obligations under this Agreement and to processed the transactions contemplated hereby;

(b) It is competent to act as an ASA under the Applicable Law;

(c) It shall, from the date of execution of this Agreement, have the financial standing and capacity to act as the ASA in accordance with the terms of this Agreement;

(d) In carrying out all activities under this Agreement, it shall make reasonable endeavour not to cause any unnecessary disruption to Aadhaar authentication facilities;

(e) This agreement has been duly executed by it and constitutes a legal, valid and binding obligation, enforceable against it in accordance with the terms hereof and its obligations under this Agreement shall be legally valid, binding and enforceable against it in accordance with the terms hereof;

(f) the information furnished and any subsequent clarification furnished on or before the date of this Agreement is to the best of its knowledge and belief true and accurate in all material respects as on the date of this Agreement;

(g) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, or constitute a default of any of the terms of its Memorandum of Association and Articles of Association, or Applicable Law, or any covenant, contract, Agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;

(h) there are no material actions, suits, proceedings or investigations pending or to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the breach of this Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform any of its obligations under this Agreement;

(i) it has no knowledge of any violation or default with respect to any order, writ, injunction or decree of any court or any legally binding order of any government instrumentality which may result in any adverse effect on its ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that shall adversely affect the performance of its obligations under this Agreement;

(j) it has complied with Applicable Law in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal

INDEX

liabilities which in the aggregate have or may have an adverse effect on its ability to perform its obligations under this Agreement;

(k) no representation or warranty made by it contained herein or in any other document furnished by it to UIDAI, contains or shall contain any untrue or misleading statement of material fact or make any omission to state a material fact necessary to make such a representation or warranty not misleading; and

(l) no sums, in cash or kind, have been paid or shall be paid, by it or on its behalf, to any person by way of bribes, commission or otherwise for entering into this Agreement or for influencing or attempting to influence any officer or employee of UIDAI in connection therewith.

9. Payment of fees and taxes

9.1 The ASA shall be liable to pay the fees and applicable taxes, if any, to the Authority in terms of sub-clause (g) of paragraph 1.1.1 of this Agreement. The terms of payment shall be such as UIDAI may stipulate from time to time, and payments made shall be non-refundable.

10. Suspension of provision of Aadhaar authentication facility to ASA

10.1 UIDAI shall provide the ASA the use of Aadhaar Authentication facilities for providing necessary infrastructure for ensuring secure network connectivity and related services for enabling requesting entity to perform authentication at its sole discretion and reserves the right to add to, to revise or to suspend in whole or in part such provision at any time, without prior notice, at its sole discretion, in the interests of protection of the information of Aadhaar number holders or the Aadhaar ecosystem, or in public interest, or in any of the interests referred to in clause (e) of paragraph 10.2.

10.2 All or any part of the provision of Aadhaar Authentication facilities made to the ASA may be suspended by UIDAI on the occurrence of any of the following events:

(a) if the ASA defaults in complying with, or acts in contravention of, any requirement of this Agreement or Applicable Law;

(b) if the ASA is in liquidation;

(c) if the business or a class of the business of the ASA has been transferred to any person or has been transferred to or amalgamated with the business of any other person without the approval of the Authority;

(d) if the ASA is convicted for an offence of moral turpitude, serious crime, criminal breach of trust, forgery or acting fraudulently, or a finding of grave misconduct under any law for the time being in force, whether in relation to the present Agreement or otherwise; or

(e) if the conduct of the ASA is found to be detrimental to the interests of UIDAI or held to be against the interests of sovereignty and integrity of India, the security of the State and friendly relations with foreign States:

Provided that no order under section 10 of this Agreement shall be made unless the ASA has been given a reasonable opportunity of being heard.

INDEX

10.3 UIDAI may, at its discretion, revoke any such order of suspension if the ASA satisfies UIDAI that the grounds for such suspension have either ceased to exist or been remedied by the ASA to the satisfaction of UIDAI.

11. Termination

11.1 *Termination by notice*

11.1.1 UIDAI may terminate this Agreement, without any protest or demur from the ASA, upon serving a written notice of 15 days to the ASA. The date of termination shall be effective from the end of the notice period calculated from the date of receipt of such notice.

11.1.2 The ASA may terminate this Agreement by giving 180 days' notice in writing to UIDAI. The said termination by the ASA shall be subject to clearance from UIDAI under the provisions of regulation 23 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021, including any Financial Disincentives levied under this Agreement. Further, during this period the ASA shall take all steps to issue notices of termination to all its AUAs/KUAs with which it has entered into an agreement and shall terminate the services as may be mutually agreed upon in their respective agreements and shall inform UIDAI of the same.

11.2 *Termination by UIDAI due to ASA showing cause*

11.2.1 Notwithstanding anything contained hereinabove, UIDAI may terminate the Agreement with ASA, in the event of it showing cause.

11.2.2 In such an event, UIDAI may give a 30 days notice to the ASA, giving it a reasonable opportunity to explain the circumstances resulting in the cause and to cure the same. If, however, UIDAI is satisfied that the explanation given by ASA is insufficient or despite the time given, the cause was not cured or UIDAI deems it necessary or expedient so to do, it may terminate this Agreement.

11.2.3 In the event that the cause is such that it cannot be cured, for reasons of conviction of the ASA or any such similar circumstances, UIDAI shall have the right to terminate the Agreement forthwith.

11.3 *Termination for change of Control of ASA*

11.3.1 UIDAI may, by giving 30 days written notice, terminate this Agreement, if a change of Control of the ASA has taken place.

11.3.2 In the event that the ASA undergoes such a change of Control, UIDAI may, at its discretion, as an alternative to termination, require a full Performance Bank Guarantee for the obligations of ASA by a guarantor on behalf of such person to whom the Control of the ASA has been transferred, subject to the approval of UIDAI. If such a Performance Bank Guarantee is not furnished within 30 days of UIDAI's demand, UIDAI reserves the right to terminate this Agreement by giving 15 days notice in writing to the ASA.

INDEX

11.3.3 In no event the rights and obligations of the ASA under this Agreement should be assigned or transferred. The rights and obligations of the ASA, under this Agreement, are non-transferable and non-assignable whether by sale, merger, or by operation of law, except with the express written consent of UIDAI.

11.3.4 In the event that the ASA ceases to be a legal entity, either on operation of such change of Control or under provisions of Applicable Law, or it is in liquidation, UIDAI shall have the right to take such measures as it may consider necessary to maintain and preserve the Authentication logs and records and other documents as the ASA may have created pursuant to the provisions of this Agreement and the Act and the regulations made thereunder.

11.4 *Effects of termination*

11.4.1 Without prejudice to any other action which may be taken under this Agreement or the Act and the regulations made thereunder, the following consequences of termination shall follow against the ASA:

(a) The termination of this Agreement by UIDAI shall result in automatic cancellation of the appointment of the Second Party as ASA;
(b) The Performance Bank Guarantee furnished by ASA may be encashed by the Authority without demur and forfeited;
(c) The ASA shall have no right to seek compensation for termination of this Agreement from UIDAI; and
(d) The ASA shall, forthwith, cease to use the Aadhaar logo and authentication software for any purposes and in any form whatsoever.

11.4.2 In case the ASA is also an Authentication User Agency/e-KYC User Agency, termination of the Authentication User Agency Agreement with UIDAI shall automatically result in termination of this Agreement.

12. Performance Bank Guarantee

12.1 The irrevocable and unconditional Performance Bank Guarantee submitted by the ASA shall remain valid for a period of 10 years. In case of renewal of this Agreement for one or more extended periods, the ASA shall submit an extended Performance Bank Guarantee for like period.

12.2 The ASA shall initiate the renewal process at least 90 days prior to the due date for renewal of this Agreement.

12.3 Any failure of the ASA to submit the renewed Performance Bank Guarantee within such period as UIDAI may specify in writing for such submission shall result in automatic cessation of this Agreement, unless otherwise agreed to between the Parties.

13. Force Majeure

13.1 ***"Force Majeure"* means the occurrence of an event which is** beyond the reasonable control of a Party and which makes a Party's performance of its obligations hereunder

INDEX

impossible or so impractical as reasonably to be considered impossible in the circumstances and includes, but is not limited to, the following:

(a) war, or warlike operations (whether a state of war be declared or not), invasion act of foreign enemy, and civil war;
(b) strike, sabotage, lockout, embargo, import restriction, port congestion, lack of usual means of public transportation and communication, industrial dispute, shipwreck, shortage or restriction of power supply, epidemics, quarantine, and plague;
(c) earthquake, landslide, volcanic activity, fire, flood or inundation, tidal wave, typhoon or cyclone, hurricane, storm, lighting, or other inclement weather condition, nuclear and pressure waves, or other natural or physical disaster; and
(d) enactment of any legislation, ordinance, notification, etc., which prohibits either of the Party to perform its obligation(s) for a period of exceeding 14 days.

13.2 If ASA is prevented, hindered, or delayed from or in performing any of itsobligationsunder the Agreement by an event of *Force Majeure*, then it shall notify UIDAI in writing of the occurrence of such event and the circumstances of the event of *Force Majeure*within fourteen days after the occurrence of such event. Issuance of such notice within the specified time frame, unless waived by the Authority for reasons, is a mandatory pre-requisite for seeking the enforcement under section 13 of this Agreement.

13.3 ASA upon issuing the notice shall be excused from the performance or punctual performance of its obligations under the Agreement for so long as the relevant event of *Force Majeure* continues and to the extent that ASA's performance is prevented, hindered, or delayed. The time for achieving final acceptance shall be extended.

13.4 ASA affected by the event of *Force Majeure* shall make reasonable efforts to mitigate the effect of the event of *Force Majeure* upon its performance of the Agreement and fulfill its obligations under the Agreement without prejudice to UIDAI's right to terminate the Agreement.

13.5 No delay or non-performance by ASA to this Agreement caused by the occurrenceof any event of *Force Majeure* shall:

(a) constitute a cause or material breach of the Agreement;
(b) give rise to any claim for damages or additional cost or expense occasioned by the delay or non-performance, if, and to the extent that, such delay or non-performance is caused by the occurrence of an event of *Force Majeure*.

13.6 If the performance of the Agreement is substantially prevented, hindered, or delayed for a single period of more than sixty days on account of one or more events of *Force Majeure* during the time period of the Agreement, the Parties shall attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Agreement by giving a notice to the other.

13.7 Notwithstanding anything contained above in section 13 of this Agreement,*Force Majeure* shall not apply to any obligation of the ASA to discharge any liability that has accrued or may accrue under this Agreement.

14. Miscellaneous

14.1 *Personnel*

14.1 The personnel employed or otherwise engaged by the ASA or any of its entity which is contractually bound by ASA to provide secured connectivity to the CIDR shall, under no circumstances, be considered as employees of UIDAI. The ASA shall have the sole responsibility for the supervision and control of the personnel and for payment of such personnel's compensation, including salary, withholding of income taxes and social security taxes, worker's compensation, employee and disability benefits and the like, subject to Applicable Law.

14.1.2 The ASA shall make its best efforts to ensure that sufficient human resources are deployed to provide secured connectivity to the CIDR and that such resources have appropriate qualifications and skill-sets to undertake the same. UIDAI, after discussion with the ASA, shall have the right to require the removal or replacement of any such human resource in respect of whom UIDAI is satisfied that such removal or replacement is necessary in the interests of the Aadhaar number holders and the proper functioning of the Aadhaar ecosystem.

14.2 *Independent Contractor*

14.2.1 Nothing in this Agreement shall be construed as establishing or implying any partnership or joint venture between the Parties to this Agreement and, except as expressly stated in this Agreement, nothing in this Agreement shall be deemed to constitute any Parties as the agent of the other Party or authorises either Party to—

(a) incur any expenses on behalf of the other Party;
(b) enter into any engagement or make any representation or warranty on behalf of the other Party;
(c) pledge the credit of or otherwise bind or oblige the other Party; and
(d) commit the other Party in any way whatsoever, without in each case obtaining the other Party's prior written consent.

14.3 *Grievance redressal*

14.3.1 The ASA shall set up a grievance handling mechanism to receive and address thecomplaints from the requesting entity with regard to authentication services facilitated by it.

14.3.2 The ASA shall ensure that similar grievance mechanism is set up by its requesting entities.

INDEX

14.3.3 The ASA shall provide various channels to its requesting entities to lodge their grievance, such as through phone, email, website, SMS, etc. Information in this regard shall be displayed at all touch points.

14.3.4 UIDAI may require from the ASA the details of any complaint and its redressal by the ASA.

14.3.5 The ASA shall provide a report of all the grievances handled by it to UIDAI, in such form and in such manner as UIDAI may require.

14.3.6 The ASA understands and agrees that the failure to comply with the grievance redressal mechanism in such manner as UIDAI may stipulate from time to time shall constitute a material breach of this Agreement.

14.4 *Notices*

14.4.1 Any notice or other document that maybe given by either Party to the other Party under this Agreementshall be inwritingand shall be delivered either in person or by Speed Post or at such email address as the Party may specify in writing.

14.4.2 In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below, and shall specify the contact person for purpose of communication:

Unique Identification Authority of India,
Head Office
(Authentication and Verification Division),
Bangla Sahib Road,
Gole Market, New Delhi – 110 001
Contact person: Deputy Director (Authentication and Verification)

_____[12]
_____[13]
Contact person: _____[14]

14.4.3 Any such notice or other document shall be deemed to have been given to the other Party—

(a) if given in person between the hours of 10:00 a.m. and 5:00 p.m. at the address of the other Party as set out above;
(b) if sent by email, provided the same fulfils the requirements under Chapter III of the Information Technology Act, 2000; or
(c) if sent by Speed Post, then from the date on which the same was delivered or was returned by India Post despite the same being sent at the address set out above.

[12] Name of the Second Party
[13] Address of the Second Party
[14] Full name and full designation of the contact person of the Second Party

INDEX

14.4.4 Either Party to this Agreement may change its address and contact person for communication purposes by giving the other reasonable prior written notice of the new information and its effective date.

14.4.5 Notwithstanding the contact person specified by UIDAI, UIDAI reserves the right to have any communication sent by any of its other officers.

14.4.6 Notwithstanding anything contained in Section 14 of this Agreement, the requirement of giving of a notice to the ASA by UIDAI shall be fulfilled if the same is given on the online portal of UIDAI through a dedicated user account of the ASA.

14.5 *Variations and further assurance*

14.5.1 No amendment, variation or other changes to this Agreement shall be valid unless such amendment is made in writing and signed by the duly authorised representatives of the Parties to this Agreement.

14.5.2 Each Party to this Agreement agrees to enter into or execute, without limitation, whatever other Agreement, document, consent and waiver and to do all other things which shall or may be reasonably required completing and delivering the authentication facility in this Agreement.

14.6 *Severability and waiver*

14.6.1 If any provision of this Agreement, or any part thereof, is found by any court or administrative body of competent jurisdiction to be illegal, invalid or unenforceable, such illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this Agreement or the remainder of the provisions in question, which shall remain in full force and effect. The Parties shall negotiate in good faith in order to agree to substitute for any illegal, invalid or unenforceable provision a valid and enforceable provision which achieves to the greatest extent possible the economic, legal and commercial objectives of the illegal, invalid or unenforceable provision or part provision.

14.6.2 No failure to exercise or enforce and no delay in exercising or enforcing on the part of either Party to this Agreement of any right, remedy or provision of this Agreement shall operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of such right, remedy or provision or the exercise or enforcement of any other right, remedy or provision.

14.7 *Compliance with Applicable Law*

14.7.1 Each Party to this Agreement accepts that it shall at all times comply with the Applicable Law.

14.8 *Ethics*

INDEX

14.8.1 The ASA represents, warrants and covenants that it has given no commitments, payments, gifts, kickbacks, lavish or expensive entertainment, or other things of value to any employee of UIDAI in connection with this Agreement and acknowledges that the giving of any such payment, gifts, entertainment, or other things of value is strictly in violation of UIDAI's standard policies and may result in immediate termination/cancellation of this Agreement.

14.9 *Entire Agreement*

14.9.1 This Agreement, along with all annexes hereto, constitutes the entire Agreement between the Parties with respect to their subject matter and as to all other representations, understandings or agreements that are not fully expressed herein, provided that nothing in section 14 of this Agreement shall be interpreted so as to exclude any liability in respect of fraudulent misrepresentation.

15. Governing law and dispute resolution

15.1 This Agreement shall be governed by and construed in accordance with the laws of India, without giving effect to conflict of law rules in relation to any legal action or proceedings to enforce this Agreement.

15.2 The Parties irrevocably submit to the exclusive jurisdiction of the courts situated at New Delhi and waive any objection to such proceedings on grounds of venue or on the grounds that the proceedings have been brought in an inconvenient forum.

15.3 *Good Faith*

15.3.1 The Parties undertake to act in good faith with respect to each other's rights and to adopt all reasonable measures to ensure the realization of the objectives of this Agreement. The Parties recognize that it is impractical in this Agreement to provide for every contingency which may arise during the life of the Agreement, and the Parties hereby agree that it is their intention that this Agreement shall operate fairly as between them, and without detriment to the interest of either of them, and that, if during the term of this Agreement either Party believes that this Agreement is operating unfairly, the Parties shall use their best efforts to remove the cause or causes of such unfairness, but failure to agree on any action pursuant to this paragraph shall not give rise to a dispute, subject to arbitration in accordance with paragraph 15.5.

15.4 *Amicable Settlement*

15.4.1 The performance of this Agreement is governed by the terms and conditions of the Agreement. In case of any dispute or differences arising out of or in relation to this Agreement, the Parties shall use their best efforts to settle all such disputes amicably; failing which, either Party of the Agreement may send a written notice of dispute to the other Party. The Party receiving the notice shall respond to the same in writing, within 30 days from the date of receipt thereof. Failure to respond to the notice within 30 days, or failure to make best efforts to amicably settle the dispute within 60 days following the receipt of the reply to the

INDEX

notice, shall bring into operation the provisions of paragraph 15.5 or paragraph 15.6, as the case may be.

15.5 *Mediation and conciliation*

15.5.1 In the event of any dispute arising out of or in connection with this Agreement, the Parties shall, in the first instance, refer the dispute to Pre-litigation Mediation and Conciliation at the Delhi High Court Mediation and Conciliation Centre. Such reference shall be by way of a notice in writing and shall be a notice for the purposes of commencement of conciliation.

15.5.2 The commencement or pendency of conciliation shall not prevent either Party from seeking interim relief or reliefs for the purposes of preserving their rights.

15.5.3 If the dispute is not settled through conciliation within 60 days following the commencement of conciliation, or within such other period as the Parties may agree to in writing, such dispute shall, thereafter, be finally resolved through arbitration.

15.6 *Arbitration*

15.6.1 Any dispute or differences arising between the Parties out of or in connection with this Agreement or in respect of any defined legal relationship associated therewith or derived there from, shall be referred to arbitration in accordance with the Arbitration and Conciliation Act, 1996. The dispute shall be referred to and decided by a sole arbitrator.

15.6.2 The arbitration proceedings shall be held at the Delhi International Arbitration Centre and conducted in accordance with the rules made by the said Centre regarding such proceedings, the administrative cost thereof and the arbitrator's fees.

15.6.3 The Parties agree to have their dispute and differences resolved in accordance with the provisions of section 29B of the Arbitration and Conciliation Act, 1996.

15.6.4 The language of the arbitration proceedings shall be English.

15.6.5 The decision of the sole arbitrator shall be accepted by the Parties as final and binding.

15.6.5 The Parties shall continue to discharge their respective obligations under thisAgreement during the pendency of the arbitration proceedings.

IN WITNESS WHEREOF, the Parties, through their duly authorised representatives, hereby sign and execute this Agreement, on the ___day of _____, 20__.

Signed and delivered for and on behalf of the Unique Identification Authority of India, acting through _____[15]

Signature:

---

[15] Name and designation

Signed and delivered for and on behalf of _____[16] by _____[17]

_____[18]

Witnesses:

(1) _____[19] (2) _____[20]

(_____)[21] (_____)[22]

_____ _____

_____[23] _____[24]

[16] Name of the Second Party
[17] Designation
[18] Signature with seal / stamp of office
[19] Signature of witness 1
[20] Signature of witness 2
[21] Name of witness 1
[22] Name of witness 2
[23] Address of witness 1
[24] Address of witness 2

Annex 1[25]

[25] Application form for Appointment as ASA, submitted by the applicant, duly filled in, along with the correspondence in this regard with UIDAI, to be added as Annex 1 [*see* item (1) of sub-clause (i) of clause (b) pf paragraph 1.1.1 of the Agreement]

Annex 2[26]

[26] Letter conveying in-principle approval to appoint the applicant as an ASA, to be added as Annex 2 [*see* sub-clause (ii) of clause (b) of paragraph 1.1.1 of the Agreement]

Annex 3[27]

[27]Report of verification done by UIDAI appointed independent audit agency, of the information furnished by the applicant (including in respect of documents, infrastructure and technological support that the applicant is required to have) as per the checklist for such verification, to be added as Annex 3 [*see* sub-clause (iii) of clause (b) of paragraph 1.1.1 of the Agreement, read with item (I) of sub-clause (ii) *ibid.*]

Annex 4

Financial Disincentives to be imposed on Authentication Service Agency under the provisions of regulation 25 of Aadhaar (Authentication and Offline Verification) Regulations, 2021

S. No.	Non-compliance	First contravention	Second contravention	Third contravention
1	Non-compliance of regulations number 8(1), 19, 20, 21(3), 22(1), 22(2), 22(3) and 22(4) of the Aadhaar (Authentication and Offline Verification) Regulations, 2021	Disincentives upto Rs. 1 lakh per day for each day of non-compliance from the date of actual commission of violation regardless of the date of discovery of the same.	If the regulation is not complied within 15 days of issuance of notice by UIDAI on first contravention, disincentives upto Rs. 2 lakh per day for each day of non-compliance.	If the regulation is not complied within 15 days of issuance of notice by UIDAI on second contravention, disincentives up to Rs. 3 lakh per day for each day of non-compliance.
2	Non-compliance of the sections number 2, 4, 5, 6, 8 and 9 and paragraphs 11.1.2, 13.2, 13.4 and 14.3 of the Authentication Service Agency Agreement	Disincentives upto Rs. 1 lakh per day for each day of non-compliance from the date of actual commission of violation, irrespective of the date of discovery of the same.	If the regulation is not complied within 15 days of issuance of notice by UIDAI on first contravention, disincentives up to Rs. 2 lakh per day for each day of non-compliance.	If the regulation is not complied within 15 days of issuance of notice by UIDAI on second contravention, disincentives up to Rs. 3 lakh per day for each day of non-compliance.

Note: It may be noted that the disincentives mentioned above are in addition to, and not in derogation of, any other remedy available to UIDAI under the Applicable Law.

Annex III

Compliance checklist for certifying compliance with controls that the ASA is required to have in place (Pre Onboarding)
Version 1.0

Important note: Wherever a control description requires ASA to ensure or do anything, the same shall be reported as compliant if and only if the auditor finds that the same is being complied with and, further, that appropriate policies, procedures, mechanisms, resources and technical enablements are in place to secure compliance with the same on an ongoing basis.

Control No.	Short Title	Control Description	Compliance Status (Compliant / Non Compliant / Not Applicable)	Auditor's Observation	Comments of ASA management
A.	**Information Security Governance**				
1	Security organisation and CISO function	ASA should ensure that it has a designated Chief Information Security Officer (CISO) or equivalent function that oversees information security governance and compliances. The CISO should have independent reporting to its Board or other governing body or chief executive.			
2	Appointment of management and technical single point of contact	ASA should appoint a Management Single Point of Contact (MPOC) and Technical Single Point of Contact (TPOC) that should oversee the management of the authentication application and Aadhaar related activities. MPOC/TPOC should ensure consistent communication with UIDAI on Aadhaar related requirements and			

INDEX

Annex III

		compliances. Any change in MPOC/TPOC should be communicated to UIDAI in a timely manner.			
3	Information security policy and procedure	ASA should have an information security policy and information security procedures in accordance with industry leading standards, such as ISO27001 (ISMS), NIST Cyber Security Framework, CSA Framework and ISO27701 (PIMS). The entity's information security policy should also address the security aspects of Aadhaar, as provided under the Aadhaar Act, regulations and specifications.			
4	Aadhaar authentication application design	ASA should ensure that the authentication application design architecture is documented and validated by UIDAI and covers Aadhaar security requirements.			
5	Aadhaar authentication data flow diagram	ASA should ensure that the Aadhaar data flow is properly documented for its ASA applications.			
6	Risk Assessment	ASA should implement process and procedure to perform periodic (at least annual) information security risk assessment of its ICT infrastructure supporting the authentication processes. Further, entity should also perform risk assessment of its third party suppliers / vendors having access to the Aadhaar systems, processes and other relevant infrastructure. Security risks should be documented and reviewed periodically by Security Officers / CISO / those in charge of the security governance of the ASA.			

INDEX

Annex III

7	Third party information security policy	ASA should ensure that it has a third party information security policy that lays down the security controls and compliances that its third party vendors, suppliers, ICT service providers and ICT support vendors (e.g., third party / outsource application developers, infrastructure support vendors, data centre hosting agency, cloud service providers etc.) are obligated to adhere to.			
B	**Compliance Requirement**				
8	Annual information security audit by CERT-In-empanelled auditor	ASA should ensure that its operations and systems are audited by an information systems auditor certified by a recognised body on an annual basis and on need basis to ensure compliance with Information Security Standards and Specifications. The audit report should be shared with UIDAI. If any non-compliance is found as a result of the audit, ASA should— (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 actions; and (d) review the corrective actions taken.			
C.	**Data Privacy**				
9	Data protection policy	ASA should establish a data protection policy addressing, inter alia, data protection related aspects under— (a) the Aadhaar Act, the regulations made thereunder and the standards and specifications issued by UIDAI from time to time; (b) the Information Technology Act, 2000 ("IT Act"); and			

INDEX

Annex III

		(c) till the coming into force of the Digital Personal Data Protection Act, 2023 ("DPDP Act"), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") and, on and from the date of coming into force of the DPDP Act, the said Act and the rules made thereunder. Such policy should be published on the website of ASA and the URL for the same should be mentioned.			
10	Data Classification and Labelling Policy	Does ASA have data classification and labelling policy in place? What is the data classification level applied to Aadhaar and correlated data? Please share data labelling and classification policy.			

INDEX

Annex III

D.	Asset Management				
11	Asset inventory maintenance	Does ASA maintain inventory of assets consisting of informational assets and hardware assets? Are these assets labelled, classified, and monitored/ reviewed periodically? Does the asset register have well defined owners and custodians and reflect correct classification scheme for each and every asset? Are the asset registers updated and reviewed periodically?			
12	Security hardening of assets	Does all the assets (e.g., desktop, laptop, servers, databases etc.) used by ASA and their sub-contractors for Aadhaar Authentication are used only after their hardening as per the ASA hardening baseline document.			
13	Maintenance of software inventory	ASA should ensure that it uses only licensed software for Aadhaar authentication related infrastructure environment. Record of all software licenses should be kept and updated regularly.			
14	Asset disposal procedure	ASA should define a procedure for disposal of the information assets being used for authentication operations. Information systems and documents containing Aadhaar related information should be disposed of securely.			

INDEX

Annex III

15	Asset repair procedure and asset movement logs	ASA should, before consigning any asset for repair, sanitise the same to ensure that it does not contain any Aadhaar related data. A register to log the movement of all the assets consigned outside should be maintained. ASA should, in case of in-house repair of assets, document the details of the original equipment manufacturer (OEM) and maintain the logs of the assets being repaired.			
E.	**Human Resource Security**				
16	Background verification and signing of confidentiality agreement with third-party contractors	ASA should take an undertaking from third party contractors regarding NDAs and BGVs conducted successfully for their personnel handling Aadhaar related data.			
17	Training and awareness	Do all employees of the Authentication Service Agency and relevant third party contractors receive information security awareness education and training and regular updates in ASA policies and procedures, as relevant to job function. Are new hire required to undergo mandatory information security and awareness training? Does, the training provided include all relevant security and privacy guidelines laid down by the Authority.			

INDEX

Annex III

18	Specialised Training	Are specific and specialised training conducted for various functional roles involved in authentication ecosystem.			
19	Training Periodicity	Are the trainings conducted half yearly and as and when changes are made in the authentication ecosystem. ASA shall maintain records of such trainings conducted.			
20	Employee's / Third Party Qualification	Does ASA ensure employees / third parties employed for maintaining necessary authentication system and infrastructure, and process'(s) requisite qualification for undertaking such works.			
F.	**Incident Management**				
21	Incident management procedure and RCA procedure	ASA should ensure that incident management framework, including forensic investigation, is implemented in accordance with the requirements under UIDAI's Information Security Policy and circulars. ASA should perform Root Cause Analysis (RCA) for major incidents identified in its ecosystem as well as that of its sub-contractors ecosystem, if any.			
G.	**Access Control**				

INDEX

Annex III

22	Access Control Policy and Procedure	Does ASA have user access right provisioning and deprovisioning process in place? How does ASA manage and monitor individuals access information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing Aadhaar related information.			
23	Access provisioning mechanism	ASA should ensure that only authorised individuals are able to access information facilities such as the authentication application, audit logs, authentication servers, application, source code, information security infrastructure, etc., and Aadhaar processing related information. Access Control List (ACL) shall be maintained by the ASA.			
24	Privilege user access management	ASA should ensure that systems and procedures are in place for privilege user access management (PAM). Privilege user access should be limited to authorised users only.			
25	Privilege accounts	ASA should ensure through the PAM tool that privileged accounts, such as NT Authority, Administrator and root accounts, are accessible only to a limited set of users, and that access to privileged account is not allowed to normal users.			
26	Periodic access review	ASA should ensure that access is provided based on least privilege and that access is reviewed periodically (at least half-yearly).			

INDEX

Annex III

27	Access revocation mechanism	Within 24 hours of exit of any personnel, ASA should revoke the rights and privileges to access or process Aadhaar related information. Upon such revocation, user IDs should be deleted forthwith if not in use.			
28	Segregation of duties	ASA should ensure that personnel involved in operational, development or testing functions should not be given additional responsibilities in system administration processes, audit log maintenance, security review of system or processes that may compromise data security. Where segregation of duties is not possible or practicable, the process should include compensating controls, such as monitoring of activities, maintenance and review of audit trails and management supervision.			
29	Initial password allocation	ASA should ensure that the allocation of initial passwords is done in a secure manner and that such passwords are changed on first log in.			

INDEX

Annex III

30	Password management guidelines	What is the password construction policy used for creating of password? Does user require to change its password after first login? What is frequency of password? Does the password policy meet's following requirement, if No please share brief comment- 1. Minimum password length of 8 characters 2. are not based on anything somebody else may easily guess or obtain using person related information, e.g., name, telephone number and date of birth; 3. is free of consecutive identical characters or all-numeric or all-alphabetical groups; 4. contain at least one numeric, one uppercase letter, one lowercase letter and one special character; 5. are required to be changed at regular intervals (passwords for privileged accounts should be changed more frequently than normal passwords); 6. do not allow the use of the last five passwords; 7. do not allow the username and password to be the same for a particular user; and 8. do not use the same password for various UIDAI access needs of a particular user.			
31	User account lockout	ASA should ensure that three successive log-in failures result in the user account being locked. End users / operators should not be able to log in until their account is unlocked and the password is reset.			
32	Restriction usage of generic IDs	ASA should ensure that common or generic or group user IDs are not used. Exceptions shall be approved by ASA's senior management and documented where there is no alternative.			

INDEX

Annex III

33	Local Admin Access Rights	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.			
34	Password Hardcoded & Auto Log - On	Passwords shall not be hardcoded in codes, login scripts, any executable program or files. Additionally, passwords shall not be included in any automated log-on process, e.g. stored in a macro or function key.			
35	Password Security	If the passwords are being stored in the database or any other form, they should be stored in an encrypted / hashed form. Further, Password should not be stored or transmitted in applications in clear text or in any reversible form.			
H.	**Physical Security**				
36	Physical security of ASA data centre	ASA data centre should be secured fully and should have access control.			
37	Physical security of ASA data centre	ASA data centre should be under 24X7 protection of security guards and CCTV surveillance.			

INDEX

Annex III

38	Physical security of ASA data centre	ASA should ensure that access to the data centre is restricted only to authorised individuals and appropriate logs of entry of individuals should be maintained. ASA should ensure that physical access to the data centre and other restricted areas is pre-approved and recorded, along with the date, time and purpose of entry. ASA should ensure that the movement of all incoming and outgoing assets in the ASA data centre is documented.			
39	Preventive maintenance activity at data centre	ASA should ensure that preventive maintenance activities, such as audit of fire extinguishers and CCTV, are carried out on a quarterly basis.			
40	Emergency Evacuation Plans	Controls such as intrusion detection and evaluation plans shall be implemented in case of an emergency.			
41	Clear Desk and Clear Screen	A clear desk and clear screen policy for shall be adopted to reduce risks of unauthorized access, loss and damage to information related to Aadhaar. Screen saver or related technological controls shall be implemented to lock the screen of the information systems when unattended beyond a specified duration.			
42	Physical location of ASA servers	ASA should ensure that their data centers are within India.			
I.	**Data Security**				
43	HSM	ASA shall procure a dedicated, on-premise, HSM set up for the management of security/encryption keys, and should not share the same with any other entity. The HSM used shall be FIPS 140-2 compliant.			

INDEX

Annex III

44	End-point security	ASA should ensure that USB access on the servers and endpoints is, in the default, restricted for all, and the same is allowed only on approval basis.			
45	End-point security — antivirus / anti-malware	ASA should use licensed malware and antivirus solution (preferably Next-Generation antivirus) to protect against malware. The malware/antivirus installed should be configured to update in real time.			
46	End-point security	ASA should ensure that end-point devices used for developing, processing, handling Aadhaar data and application timeout after a session is idle is not more than 30 to 15 minutes, based on the criticality.			
47	Patch management	ASA should ensure that the patch management process is implemented for applying patches to information systems. Patches should be updated at both the application and the server and network levels. ASA should ensure that either N or N-1 patches are maintained.			
48	Data Leakage Prevention	Are sufficient security measures implemented to detect and prevent data leakage? Please provide detail of data leakage prevention solution or the alternative control implemented.			
J.	**Network Security**				

INDEX

Annex III

49	IPS/IDS/WAF implementation	ASA should ensure that Network Intrusion and Prevention Systems (NIPS), Intrusion Detection System (IDS), Web Application Firewall (WAF) are implemented to safeguard the network from external attacks / DDoS attacks. ASA should ensure that Internet access on systems are restricted to necessary or work-related websites and that access to web portals known for pirated software, gambling etc. are restricted.			
50	Vulnerability Assessment	ASA should plan organisation information security policy, inclusive of vulnerability assessment and penetration testing on its network, infrastructure and applications.			
K.	**Operations Security**				
51	Segregation of testing and production environments	The Test and Production facilities / environments must be physically and logically separated.			
52	Service Continuity & Service Availability	ASA shall ensure operational continuity and high availability of service? ASA should ensure DC and DR is available with them. ASA shall maintain BCP and DR policy document, BCP DR test detail and Crisis Management detail.			
53	Audit Program	Does ASA has planned, established, implemented and maintained an audit program(s), including the frequency, methods, responsibilities, planning requirements and reporting. Does the audit program(s) take into consideration the importance of the processes concerned and the results of previous audits?			
54	Grievance Handling	Please provide detail on grievance handling mechanism set (by ASA), and detail on channel's they can be			

INDEX

Annex III

		approached via. Please share supporting evidence or link.			

INDEX

Annex III

L.	**Application Security**				
55	Secure software development	ASA should implement system and processes to ensure secure software development practices. Periodic training of developers should be conducted on secure software development practices. Records of such trainings should be maintained.			
56	Compliance to API specifications and application security	The client applications i.e. software used by ASA 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.			
57	Configuration reviews and system walkthrough	ASA should ensure that authentication applications as well as infrastructure are integrated with IDAM, PIM/PAM and SIEM.			
M.	**Logging and Monitoring**				
58	Logs recording	ASA should ensure that the event/security logs recording critical user-activities, exceptions and security events are enabled and stored to assist any future investigation and enable access control monitoring.			
59	Logs monitoring	ASA should ensure that regular monitoring of event/security logs takes place to detect unauthorised use of information systems and that results of the same are recorded. Further, access to audit trails and event logs should be provided to authorised personnel only.			

INDEX

Annex III

60	Clock synchronisation through use of Network Time Protocol (NTP)	ASA should connect to the Network Time Protocol (NTP) server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL), or with NTP servers traceable to the said NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC; however, it should be ensured that such time source does not deviate from NPL and NIC.			

INDEX

Annex IV

Compliance checklist for certifying compliance with controls that the ASA is required to have in place Version 1.0 **Important note:** Wherever a control description requires ASA to ensure or do anything, the same shall be reported as compliant if and only if the auditor finds that the same is being complied with and, further, that appropriate policies, procedures, mechanisms, resources and technical enablement's are in place to secure compliance with the same on an ongoing basis.					
Control No.	**Short Title**	**Control Description**	**Compliance Status (Compliant / Non Compliant / Not Applicable)**	**Auditor's Observation**	**Comments of ASA management**
A.	**Information Security Governance**				
1	Security organisation and CISO function	ASA should ensure that it has a designated Chief Information Security Officer (CISO) or equivalent function that oversees information security governance and compliances. The CISO should have independent reporting to its Board or other governing body or chief executive.			
2	Appointment of management and technical single point of contact	ASA should appoint a Management Single Point of Contact (MPOC) and Technical Single Point of Contact (TPOC) that should oversee the management of the authentication application and Aadhaar related activities. MPOC/TPOC should ensure consistent communication with UIDAI on Aadhaar related requirements and compliances. Any change in MPOC/TPOC should be communicated to UIDAI in a timely manner.			

INDEX

3	Information security policy and procedure	ASA should have an information security policy and information security procedures in accordance with industry leading standards, such as ISO27001 (ISMS), NIST Cyber Security Framework, CSA Framework and ISO27701 (PIMS). The entity's information security policy should also address the security aspects of Aadhaar, as provided under the Aadhaar Act, regulations and specifications.			
4	Aadhaar authentication network design	ASA should ensure that the authentication network design architecture is documented and covers Aadhaar security requirements, and it will be reviewed by Tech centre			
5	Aadhaar authentication data flow diagram	ASA should ensure that the Aadhaar data flow is properly documented, and it will be reviewed by Tech centre			
6	Risk Assessment	ASA should implement process and procedure to perform periodic (at least annual) information security risk assessment of its ICT infrastructure supporting the authentication processes. Further, entity should also perform risk assessment of its third party suppliers / vendors having access to the Aadhaar systems, processes and other relevant infrastructure. Security risks should be documented and reviewed periodically by Security Officers / CISO / those in charge of the security governance of the ASA.			
7	Third party information security policy	ASA should ensure that it has a third party information security policy that lays down the security controls and compliances that its third party vendors, suppliers, ICT service providers and ICT support vendors (e.g., third party / outsource application developers, infrastructure support vendors, data centre hosting agency, cloud service providers etc.) are obligated to adhere to.			

INDEX

8	Standard Operating Procedures (SOPs)	Standard Operating Procedure (SOP) shall be developed for all information systems and services related to Aadhaar 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.			
B.	**Compliance Requirement**				
9	IPR provisions contained in UIDAI's ASA Agreement (latest version)	The ASA should be in compliance with the intellectual property provisions contained in UIDAI's Authentication Service Agency Agreement (latest version).			
10	Annual information security audit by CERT-In-empanelled auditor	ASA should ensure that its operations and systems are audited by CERT - In Empanelled information systems auditor on an annual basis and on need basis to ensure compliance with UIDAI's standards and specifications. The audit report should be shared with UIDAI. If any non-compliance is found as a result of the audit, ASA should— (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 actions; and (d) review the corrective actions taken. The annual audit should cover all security controls applicable under the Aadhaar (Data Security) Regulations, 2016.			

INDEX

11	Onboarding of AUA/KUA	ASA should only engage with the AUA / KUA approved by the Authority and keep the Authority informed of the list of requesting entities that it serves along with all relevant details of its agreements with the AUAs. In case of disengagement with an AUA / KUA, the ASA shall inform UIDAI within a period of 7 days from the date of disengagement.			
12	Compliance to UIDAI Requirements	ASA shall ensure 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. ASA shall adhere to all regulations, information security policies, processes, standards, specifications and guidelines issued by UIDAI from time to time.			
13	Integrity of Data to AUA/KUA	The Authentication Service Agency will send the data received from UIDAI to Authentication User Agency / e-KYC User Agency without any modification. If response packet received from UIDAI is corrupted or time out occurred, Authentication Service Agency will send the error codes as defined by Authentication Service Agency to the Authentication User Agency / e-KYC User Agency.			

INDEX

14	Compliance with ASA agreement	The requesting ASA should comply with provisions of ASA Agreement with UIDAI at all times.			
15	Cryptography & Key Management	The authentication request shall be digitally signed by the requesting AUA/KUA and Authentication Service Agency (using FIPS 140-2 compliant HSM), as per the mutual agreement between them and forwarded to CIDR.			
16	Cryptography & Key Management	ASA shall not decrypt the e-KYC response data received from UIDAI for e-KYC request.			
17	Digital Signing	ASA should ensure private key used for digitally signing the authentication request and the license keys are kept secure and access controlled. The private key should meet below parameter specified by the authority and documented in SPI Specification document (latest):- a) Digital signature certificate used/ procured should be of class II or class III certificate			
18	Use of secure communication protocols	ASA should ensure message security and integrity between their server's, and AUA server.			
19	Compliance and Completeness Check	ASA shall perform basic compliance and completeness checks on the authentication data packet such as checking structural validity of the packet received from AUA/KUA and check its signature to ensure no unwanted, malicious requests are sent through.			
C.	**Data Privacy**				

INDEX

20	Data protection policy	ASA should establish a data protection policy addressing, inter alia, data protection related aspects under— (a) the Aadhaar Act, the regulations made thereunder and the standards and specifications issued by UIDAI from time to time; (b) the Information Technology Act, 2000 ("IT Act"); and (c) till the coming into force of the Digital Personal Data Protection Act, 2023 ("DPDP Act"), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") and, on and from the date of coming into force of the DPDP Act, the said Act and the rules made thereunder. Such policy should be published on the website of ASA and the URL for the same should be mentioned.			
21	Data Classification and Labelling Policy	ASA should have data classification and labelling policy in place. Further, ASA shall ensure data classification level is applied to Aadhaar and its correlated data.			
22	Reporting and Cooperating in case of privacy incident(s)	ASA shall: a. report promptly to UIDAI (within 24 hours) (email id: authsupport@uidai.net.in) any privacy incidents affecting the personal data of the residents; and b. extend full cooperation to UIDAI, or any agency appointed or authorised by UIDAI to cooperate while inquiries, incidents, claims and complaints are being handled in case of any security and privacy breach.			
D.	**Asset Management**				

INDEX

23	Asset inventory maintenance	ASA shall maintain inventory of assets consisting of informational assets and hardware assets. These assets must be labelled and classified alongwith well defined owners and custodians with correct classification scheme for each and every asset. Further, the same shall be updated and reviewed periodically.			
24	Security hardening of assets	All the assets (e.g., desktop, laptop, servers, databases etc.) used by ASA and their sub-contractors for Aadhaar Authentication shall be used only after their hardening as per the ASA hardening baseline document.			
25	Maintenance of software inventory	ASA should ensure that it uses only licensed software for Aadhaar authentication related infrastructure environment. Record of all software licenses should be kept and updated regularly.			
26	Asset disposal procedure	ASA should define a procedure for disposal of the information assets being used for authentication operations. Information systems and documents containing Aadhaar related information should be disposed off securely.			

INDEX

27	Asset repair procedure and asset movement logs	ASA should, before consigning any asset for repair, sanitise the same to ensure that it does not contain any Aadhaar related data. A register to log the movement of all the assets consigned outside should be maintained. ASA should, in case of in-house repair of assets, document the details of the original equipment manufacturer (OEM) and maintain the logs of the assets being repaired.			
E.	**Human Resource Security**				
28	Background verification and signing of confidentiality agreement	ASA should conduct a background check and sign a confidentiality agreement / non-disclosure agreement (NDA) with all personnel/agency handling Aadhaar related information. Access to authentication infrastructure should not be granted before signing NDA and completion of background verification (BGV) for personnel.			
29	Background verification and signing of confidentiality agreement with third-party contractors	ASA should take an undertaking from third party contractors regarding NDAs and BGVs conducted successfully for their personnel handling Aadhaar related data.			

INDEX

30	Training and awareness	All employees of the Authentication Service Agency and relevant third party contractors shall receive information security awareness education, training and regular updates in ASA policies and procedures, as relevant to job function. The training provided shall include all relevant security and privacy guidelines laid down by the Authority.			
31	Specialised Training	Are specific and specialised training conducted for various functional roles involved in authentication ecosystem.			
32	Training Periodicity	Trainings shall be conducted half yearly and as and when changes are made in the authentication ecosystem. ASA shall maintain records of such trainings conducted.			
33	Employee's / Third Party Qualification	Does ASA ensure employees / third parties employed for maintaining necessary authentication system and infrastructure, and process'(s) requisite qualification for undertaking such works.			
F.	**Incident Management**				

INDEX

34	Incident management procedure and RCA procedure	ASA should ensure that incident management framework, including forensic investigation, is implemented in accordance with the requirements under UIDAI's Information Security Policy and circulars. ASA should perform Root Cause Analysis (RCA) for major incidents identified in its ecosystem as well as that of its sub-contractors ecosystem, if any.			
35	Reporting of incidents to UIDAI and CERT-In	ASA should— (a) inform UIDAI (email id: authsupport@uidai.net.in) misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or systems within its network, and report any confidentiality security breach of Aadhaar related information to UIDAI within 24 hours; (b) report cyber incidents as mentioned in Annexure I to the directions dated 28.4.2022 of CERT-In, bearing no. 20(3)/2022-CERT-In, within 6 hours of noticing such incidents or the same being brought to their notice; and (c) on and from the date of coming into force of sub-section (6) of section 8 of the DPDP Act, intimation of personal data breach to the Board and each affected Data Principal, within such time as may be prescribed by rules made under the said Act.			
G.	**Access Control**				

INDEX

36	Access Control Policy and Procedure	ASA shall have user access right provisioning and deprovisioning process in place. ASA shall manage and monitor individuals accessing information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing Aadhaar related information.			
37	Single Sign On (SSO)	ASA should implement secure authentication mechanism such as Multi Factor Authentication / Single sign etc. to access UIDAI applications.			
38	Access provisioning mechanism	ASA should ensure that only authorised individuals are able to access information facilities such as the authentication application, audit logs, authentication servers, application, source code, information security infrastructure, etc., and Aadhaar processing related information. Access Control List (ACL) shall be maintained by the ASA.			
39	Privilege user access management	ASA should ensure that systems and procedures are in place for privilege user access management (PAM). Privilege user access should be limited to authorised users only.			
40	Privilege accounts	ASA should ensure through the PAM tool that privileged accounts, such as NT Authority, Administrator and root accounts, are accessible only to a limited set of users, and that access to privileged account is not allowed to normal users.			

INDEX

41	Periodic access review	ASA should ensure that access is provided based on least privilege and that access is reviewed periodically (at least half-yearly).			
42	Access revocation mechanism	Within 24 hours of exit of any personnel, ASA should revoke the rights and privileges to access or process Aadhaar related information. Upon such revocation, user IDs should be deleted forthwith if not in use.			
43	Segregation of duties	ASA should ensure that personnel involved in operational, development or testing functions should not be given additional responsibilities in system administration processes, audit log maintenance, security review of system or processes that may compromise data security. Where segregation of duties is not possible or practicable, the process should include compensating controls, such as monitoring of activities, maintenance and review of audit trails and management supervision.			
44	Initial password allocation	ASA should ensure that the allocation of initial passwords is done in a secure manner and that such passwords are changed on first log in.			

INDEX

48	Local Admin Access Rights	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 suitable action as per the HR policy of ASA .			
49	Password Hardcoded & Auto Log - On	Passwords shall not be hardcoded in codes, login scripts, any executable program or files. Additionally, passwords shall not be included in any automated log-on process, e.g. stored in a macro or function key.			
50	Password Security	If the passwords are being stored in the database or any other form, they should be stored in an encrypted / hashed form. Further, Password should not be stored or transmitted in applications in clear text or in any reversible form.			
H.	**Change Management**				
51	Change logs management	ASA should document all changes to Aadhaar authentication applications, infrastructure, processes and information processing facilities, and maintain change log/register.			
I.	**Physical Security**				

INDEX

52	Physical security of ASA data centre	ASA data centre hosting Aadhaar related information should be secured fully and should have access control.			
53	Security of ASA servers	ASA should ensure that their servers are placed in an isolated, secure cabinet in the data centre.			
54	Physical security of ASA data centre	ASA data centre and servers should be under 24X7 protection of security guards and CCTV surveillance.			
55	Physical security of ASA data centre	ASA should ensure that access to the data centre is restricted only to authorised individuals and appropriate logs of entry of individuals should be maintained.			

INDEX

56	Physical security of ASA data centre	ASA should ensure that physical access to the data centre and other restricted areas hosting critical Aadhaar related equipment/information is pre-approved and recorded, along with the date, time and purpose of entry.			
57	Physical security of ASA data centre	ASA should ensure that the movement of all incoming and outgoing assets related to Aadhaar in the ASA data centre is documented.			
58	Physical security of ASA data centre	ASA should ensure that visible and clearly readable signs/notices notifying areas designated as restricted areas and provisions restricting entry to the same are posted at all points leading to entry to such areas.			
59	Physical security of ASA data centre	ASA should provide lockable cabinets or safes in the data centre and information processing facilities for housing servers containing critical Aadhaar related information. ASA should deploy label, monitor and test regularly the operation of fire exit doors and fire extinguishing systems.			
60	CCTV Coverage and Recording	CCTV surveillance shall cover the ASA servers. ASA shall retain the recordings of CCTV for at least 30 days. Access to CCTV logs and recordings shall be provided to authorized individuals. CCTV recordings shall be securely stored.			

INDEX

61	Protection of power and network cables	Controls shall be designed and implemented to protect power and network cables from unauthorized interception or damage.			
62	Preventive maintenance activity at data centre	ASA should ensure that preventive maintenance activities, such as audit of fire extinguishers and CCTV, are carried out on a quarterly basis.			
63	Emergency Evacuation Plans	Controls such as intrusion detection and evaluation plans shall be implemented in case of an emergency.			
64	Clear Desk and Clear Screen	A clear desk and clear screen policy for shall be adopted to reduce risks of unauthorized access, loss and damage to information related to Aadhaar. Screen saver or related technological controls shall be implemented to lock the screen of the information systems when unattended beyond a specified duration.			
65	Physical location of ASA servers	ASA should ensure that the data centers hosting servers on which Aadhaar related information is stored are within India.			
J.	**Data Security**				

INDEX

66	Storage of PID block and license keys	Encrypted PID blocks and license keys, that came as part of authentication must not be stored anywhere in its system.			
67	Session Key Security	The ASA should ensure that Session key must not be stored anywhere except in memory and should not be reused across transactions. Only re-use of session key is allowed when its use as seed key when using synchronized session key scheme.			
68	Use of HSM	The key(s) used for digitally signing of authentication request shall be stored in HSM only. The HSM used shall be FIPS 140-2 compliant. ASA should have a dedicated, on-premise, HSM set up for the management of security/encryption keys, and should not share the same with any other entity.			
69	License Key Security	ASA should ensure the license keys are kept secured and access controlled.			
70	Storage of Aadhaar Number, VID and UID Token	ASA in any case shall not store Aadhaar number, UID Token or VID in their transaction logs.			
71	End-point security	ASA should ensure that USB access on the servers and endpoints is, in the default, restricted for all, and the same is allowed only on approval basis.			

INDEX

72	End-point security — antivirus / anti-malware	ASA should use licensed malware and antivirus solution (preferably Next-Generation antivirus) to protect against malware. The malware/antivirus installed should be configured to update in real time.			
73	End-point security	ASA should ensure that end-point devices used for developing, processing, handling Aadhaar data and application timeout after a session is idle is not more than 30 to 15 minutes, based on the criticality.			
74	Patch management	ASA should ensure that the patch management process is implemented for applying patches to information systems. Patches should be updated at both the application and the server and network levels. ASA should ensure that either N or N-1 patches are maintained.			
75	Data Leakage Prevention	ASA shall implement a data leakage prevention solution to detect and prevent data leakage.			

INDEX

76	Restriction on Aadhaar or AUA/KUA information	ASA and other sub-contractors providing Aadhaar authentication service to AUA/KUA shall ensure AUA/KUA information is not displayed or disclosed to external agencies or unauthorized persons. Also, Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate or any other document/service shall not be published or displayed at any platform.			
K.	**Network Security**				
77	Network connectivity with UIDAI	ASA shall establish dual redundant, secured leased lines or MPLS connectivity with the data centers of UIDAI, in accordance with the procedure and security processes as may be specified by UIDAI for this purpose			
78	Network connectivity with AUA/KUA	The network between AUA / KUA and ASA shall be secure. ASA shall connect with AUAs/KUAs through leased lines or MPLS connectivity. If a public network is used, a secure channel such as SSL/TLS or site to site VPN shall be used.			

INDEX

79	Segregation of ASA servers	The ASA server host shall reside in a segregated network segment that is isolated from the rest of the network of the ASA organization. The ASA server host shall be dedicated for the Aadhaar Authentication purposes and shall not be used for any purpose other than those specified in the application for appointment as ASA.			
80	Firewall access of network	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.			
81	IPS/IDS/WAF implementation	ASA should ensure that Network Intrusion and Prevention Systems (NIPS), Intrusion Detection System (IDS), Web Application Firewall (WAF) are implemented to safeguard the network from external attacks / DDoS attacks. ASA should ensure that Internet access on systems are restricted to necessary or work-related websites and that access to web portals known for pirated software, gambling etc. are restricted.			
82	Vulnerability Assessment	Vulnerability assessment exercise should be conducted on a bi-annual basis for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.			
L.	**Operations Security**				

INDEX

83	Segregation of testing and production environments	The Test and Production facilities / environments must be physically and logically separated.			
84	Service Continuity & Service Availability	The Authentication Service Agency shall ensure uptime of minimum 99.99% for its authentication services as well as connectivity with CIDR and Authentication User Agencies / e-KYC User Agencies. ASA shall ensure operational continuity and high availability of service? ASA shall maintain BCP and DR policy document, BCP DR test detail and Crisis Management detail.			
85	Audit Program	ASA shall plan, establish, implement and maintain an audit program(s), including the frequency, methods, responsibilities, planning requirements and reporting. Additionally, the audit program(s) shall take into consideration the importance of the processes concerned and the results of previous audits.			
86	Grievance Handling	Please provide detail on grievance handling mechanism set (by ASA), and detail on channel's they can be approached via. Please share supporting evidence or link.			
87	Redundancy	ASA should maintain redundancy of infrastructure to ensure seamless provision of authentication delivery of services.			

INDEX

88	Usage of Test Data	ASA should utilize test data or non-production data for testing of application or software during testing phase.			
M.	**Application Security**				
89	Secure software development	ASA should implement system and processes to ensure secure software development practices. Periodic training of developers should be conducted on secure software development practices. Records of such trainings should be maintained.			
90	Restrictions on designing/ compiling malicious code	ASA personnel 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 Aadhaar information.			
91	Source code review by CERT-In-empanelled auditor	ASA shall perform Source Code review of the modules and applications used for establishing connectivity with CIDR and undergo audit by a certified auditor. ASA shall ensure that there is no sensitive business logic, secret keys or other proprietary information in the code of the modules and applications used for authentication			
92	SAST/DAST application audit	ASA should ensure that authentication application security assessment {including static application security testing (SAST) and dynamic application security testing (DAST)} is performed at least annually or at the time of major changes to the authentication application, and that all vulnerabilities are addressed for remediation and no vulnerable third party components are used by the authentication application.			

INDEX

93	Vulnerability assessment	ASA should plan organisation information security policy, inclusive of vulnerability assessment and penetration testing on its network, infrastructure and applications.			
94	Configuration reviews and system walkthrough	ASA should ensure that authentication applications as well as infrastructure are integrated with IDAM, PIM/PAM and SIEM.			
N.	**Logging and Monitoring**				
95	Authentication log maintenance	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, device identity related data and e-KYC response data, where applicable shall not be retained.			

INDEX

96	Authentication log retention	ASA should ensure that the logs of authentication transactions are stored online for audit purposes for two years and, thereafter, archived for another five years.			
97	Logs recording	ASA should ensure that the event/security logs recording critical user-activities, exceptions and security events are enabled and stored (at least for 6 months) to assist any future investigation and enable access control monitoring.			
98	Logs monitoring	ASA should ensure that regular monitoring of event/security logs takes place to detect unauthorised use of information systems and that results of the same are recorded. Further, access to audit trails and event logs should be provided to authorised personnel only.			
99	Compliance on storage and maintenance of logs	The ASA shall comply with all applicable laws in respect of storage and maintenance of these logs, including the Aadhaar Act 2016 and its regulations, Information Technology Act, 2000.			

INDEX

100	Clock synchronisation through use of Network Time Protocol (NTP)	ASA should connect to the Network Time Protocol (NTP) server of the National Informatics Centre (NIC) or National Physical Laboratory (NPL), or with NTP servers traceable to the said NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC; however, it should be ensured that such time source does not deviate from NPL and NIC.			
O.	**Fraud and Forensics**				
101	Fraud analytics module	ASA shall deploy as part of its systems, a Fraud Analytics module that is capable of analysing authentication related transactions to identify fraud.			
102	Fraud Notification	In case if ASA 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 UIDAI			

INDEX

Annex V

(Letter head of the Applicant)

To:

Chief Executive Officer
Unique Identification Authority of India
Bangla Sahib Road, Behind Kali Mandir
Gole Market, New Delhi – 110 001

Subject: Statement and Undertaking regarding ASA transaction volume

Reference: UIDAI Circular No. 5 dated …..5.2025

Sir/Madam,

In terms of the directions issued *vide* above referred UIDAI Circular, it is informed that the estimated number of authentication transactions per annum for _____ *(Name of ASA)* is as under:

(a) Up to 10 crore transactions per year* ☐

(b) More than 10 crore and up to 20 crore transactions per year* ☐

(c) More than 20 crore transactions per year* ☐

(**tick as applicable*)

2. We hereby undertake to pay applicable fee of ₹ _____ (excluding GST), valid for two years from the date of start of pre-production. In case the actual number of ASA transactions exceeds the estimated number of ASA transactions given above, we undertake to pay to UIDAI the difference of the amount of applicable fees reckoned on the basis of the actual such number and that reckoned on the basis of the estimated number, along with the interest @ 18% per annum.

Yours sincerely,

Name of the Authorised Signatory: _____
Designation: _____

Date:
Place:

F. no. HQ-13029/1/2022-AUTH-I HQ (Comp. No. 18084)
Unique Identification Authority of India
(Authentication and Verification Division)

3rd floor, UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110 001
Dated: 9th June 2025

Circular No. 07 of 2025

Subject: Changes in eKYC response (PDF and XML format) for Foreigner enrolled Aadhaar number holders

At the time of enrollment and updation, UIDAI records various demographics details of Aadhaar number holder like name, dob, gender, address, mobile and email on the basis of document submitted by them as per Aadhaar act and regulations. Authentication services offered by UIDAI are as Auth (Y/N) and eKYC. As part of the eKYC process, the Aadhaar Number Holder authorizes UIDAI (through Aadhaar authentication) to provide their basic demographic data for PoI and PoA along with their photograph (digitally signed) to AUA/KUAs using our latest eKYC API 2.5. Presently, eKYC response fields are same for all residents enrolled as an Aadhaar number holder.

2. UIDAI has made following changes in the eKYC response (PDF and XML format) for Foreigner enrolled Aadhaar number holders:

(i) The **aadhaarExpiryDate** and **isResidentForeigner** tags in case of foreigner enrolled as an Aadhaar number holder will be sent in the eKYC response.

(ii) If the Aadhaar for foreigner has expired, then an appropriate error code (993 - Foreigner Aadhaar Expired) will be sent in the eKYC response.

(iii) Foreigner enrolled as an Aadhaar number holder will have DOB as "YYYY" only in the eKYC response.

Accordingly, response fields of eKYC API 2.5 will be changed in eKYC response (PDF and XML format).

3. Revisions in the eKYC response for Foreigner enrolled as an Aadhaar number holder for clearer communication regarding aspects relevant to informed use of Aadhaar are as under:

(i) Below are the old and revised eKYC response fields of eKYC API 2.5:

UIDAI F. no.: HQ-13029/1/2022-AUTH-I HQ/C-18084, dated 9.6.2025

Old eKYC response	Revised eKYC response
1) UidData a) Full Aadhaar (Full KYC) *or* Masked Aadhaar (Limited KYC) 2) PoI b) Name of the Aadhaar Holder c) Date of Birth d) Gender 3) PoA e) Full Address 4) LData (Local Language data) - *Optional* f) Name and full address in local language 5) Pht (Photo) g) base64 encoded JPEG photo of the Aadhaar Number Holder 6) Prn (pdf) - *Optional* h) base64 Encoded e-Aadhaar PDF of Aadhaar Number Holder	1) UidData i) Full Aadhaar (Full KYC) or j) Masked Aadhaar (Limited KYC) 2) PoI k) Name of the Aadhaar Holder l) Date of Birth m) Gender **n) isResidentForeigner** **o) aadhaarExpiryDate** 3) PoA p) Full Address 4) LData (Local Language data) - *Optional* q) Name and full address in local language 5) Pht (Photo) r) base64 encoded JPEG photo of the Aadhaar Number Holder 6) Prn (pdf) - *Optional* s) Base64 encoded e-Aadhaar PDF of Aadhaar Number Holder

(ii) Below are the old and revised eKYC response XML format:

Old eKYC response XML format	Revised eKYC response XML format
<KycRes ret="" code="" txn="" ts="" ttl="" actn="" err=""> <Rar>base64 encoded fully valid Auth response XML for Aadhaar Number Holder</Rar> <UidData uid="" tkn=""> <Poi name="" dob="" gender=""/> <Poa co="" house="" street="" lm="" loc="" vtc="" subdist="" dist="" state="" country="" pc="" po=""/> <LData lang="" name="" co="" house="" street="" lm="" loc="" vtc="" subdist="" dist="" state="" country="" pc="" po=""/> <Pht>base64 encoded JPEG photo of the Aadhaar Number Holder</Pht> <Prn type="pdf">base64 encoded signed Aadhaar letter for printing</Prn> </UidData> <Signature/> </KycRes>	<KycRes ret="" code="" txn="" ts="" ttl="" actn="" err=""> <Rar>base64 encoded fully valid Auth response XML for Aadhaar Number Holder</Rar> <UidData uid="" tkn=""> <Poi name="" **dob="YYYY"** gender="" **isResidentForeigner="" aadhaarExpiryDate=""**/> <Poa co="" house="" street="" lm="" loc="" vtc="" subdist="" dist="" state="" country="" pc="" po=""/> <LData lang="" name="" co="" house="" street="" lm="" loc="" vtc="" subdist="" dist="" state="" country="" pc="" po=""/> <Pht>base64 encoded JPEG photo of the Aadhaar Number Holder</Pht> <Prn type="pdf">base64 encoded signed Aadhaar letter for printing</Prn> </UidData> <Signature/> </KycRes>

INDEX

F. no. HQ-13064/1/2024-AUTH-I HQ/C-15014
Unique Identification Authority of India
(Authentication and Verification Division)

3rd floor, UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110001
Dated 31 July 2025

Circular 9 of 2025

To:

All Requesting entities (AUAs, KUAs, Sub-AUAs and Sub-KUAs) and ASAs

Subject: Aadhaar Status Notification Framework Documentation

Reference is invited to UIDAI Circular 1 of 2025 dated 1.1.2025 subjected "Execution of Supplementary Agreement or Agreement to supplement AUA Agreement under sub-regulation (3A) of regulation 9 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021".

2. For availing the Aadhaar status verification service, requesting entities are directed to use the UIDAI's provided API framework for the same. Technical specification document for Aadhaar status verification is attached in Annexure I.

3. This issues with approval of competent authority.

(Sanjeev Yadav)
Director
Tel.: 011-23478609
Email: dir2.auth-hq@uidai.net.in

Copy to:

1. All UIDAI Regional Offices
2. Technology Centre, Bangalore

INDEX

UIDAI F. no.: HQ-13029/1/2022-AUTH-1 HQ/C-18084, dated 9.6.2025

(iii) Below are the old and revised eKYC PDF response format:

Old eKYC PDF response	Revised eKYC PDF response
	
	

4. In view of the aforesaid, it is directed that the KUAs/Sub-KUAs may incorporate the above changes in their eKYC application by 30.6.2025. For entities requesting eKYC response in PDF format, the above changes will be executed from the UIDAI backend. For entities consuming eKYC response in XML and then generating PDF at their end may implement the above changes at their back end. These changes will come into effect from 1.7.2025.

5. All transaction requests received from entities without incorporating the changes as mentioned in letter will be rejected w.e.f. 1.7.2025. Detail of nodal officer is to facilitate successful completion of these changes in eKYC, will be Mr RBS Sandhu, Director (Auth), UIDAI Technology Centre, Bangalore (tel.: 080-23099441-444; email: authsupport@uidai.net.in.).

6. This issues with the approval of competent authority.

(Pratik Choudhary)
Deputy Director
Tel.: 011-23478608
Email: dd1.auth-hq@uidai.net.in

To,

1. All AUAs/KUAs/ASAs

Copy to:

1. All UIDAI Regional Offices
2. Technology Centre, Bangalore

INDEX

F. no. HQ-13023/1/2023-AUTH-I HQ (C-13862)
Unique Identification Authority of India
(Authentication and Verification Division)
3rd floor, UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110 001
Dated: 9th June 2025

To:

All registered device vendors

Subject: Customization of RD Service for UIDAI Sandbox Environment

Sir/Madam,

We are pleased to inform you that the UIDAI Sandbox was officially launched on April 8, 2025. This secure and innovative platform enables developers, businesses and non-AUA entities to test and integrate Aadhaar-based services in a controlled environment. The Sandbox supports strategic objectives to empower developers, drive innovation, accelerate adoption, enhance security, and foster collaboration.

2. The UIDAI Sandbox operates with its own certificate architecture. Unlike staging or production, where devices use environment-specific certificates to encrypt the PID block via AES, Sandbox testing requires production-registered devices to employ the staging certificate for PID encryption. To facilitate realistic end-to-end testing without impacting live systems, your RD Service implementation must be updated accordingly.

3. In view of the above, the undersigned is directed Device providers to implement the following changes and make the updated RD Service package available on your portal:

(a) **RD Service Customization Validation**

(i) Modify your RD Service so that production-registered Fingerprint and Iris devices, when operating in the Sandbox, use the staging certificate (Sandbox) for PID block encryption instead of the production certificate.

(ii) Ensure that the service logic cleanly detects the Sandbox environment (e.g. via endpoint URL or configuration flag) and switches certificates automatically.

(b) **Testing & Validation**

(i) After customization, register a subset of your devices in the production environment.

(ii) Perform comprehensive testing within the Sandbox to verify that PID encryption and overall authentication flows function correctly with the staging certificate.

(c) **Deployment & Distribution**

(i) Package and publish the updated RD Service (including any updated libraries, sample configurations and release notes) on your device provider portal.

(ii) Notify your integrator and partner network of the availability of the new Sandbox-compatible RD Service package.

4. In view of the aforesaid, all registered device vendors are directed to complete development, validation and publication of the updated RD Service package by **June 30, 2025**, to ensure smooth on-boarding of Sandbox participants.

5. Your cooperation is critical to the success of the UIDAI Sandbox ecosystem. If you have any questions or require technical assistance in this regards, please contact us at "support-sandbox@uidai.net.in".

6. This issues with the approval of the competent authority.

(Pratik Choudhary)
Deputy Director
Tel.: 011-23478608
Email: dd1.auth-hq@uidai.net.in

Copy to:

1. Technology Centre, Bangalore

INDEX

Annex

HQ-13028/2/2024-AUTH-I HQ-Part (1)
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road
Behind Kali Mandir, Gole Market
New Delhi-110 001
Dated: 15 Jul 2025

CIRCULAR NO 2 of 2018

Subject: Revised Clarification on Face Authentication Implementation

UIDAI Circular No. 2 of 2018 (Ref: No. K-11020/231/2018/UIDAI Auth-I) dated 15th January 2018 introduced Face Authentication, which was in-house developed authentication modality, as an additional biometric modality to augment the Aadhaar authentication ecosystem *vide* UIDAI Circular No. 13028/1/UIDAI(AUTH-I) dated 03.06.2022. In view of developments and current authentication trends, the clarifications are issued to supersede and update earlier references in the circular. Reference is also invited to UIDAI Circulars No. 07 of 2023, issued *vide* HQ-13083/6/2021-AUTH-II HQ (E-3605) 6754 dated 11.07.2023.

2. It is clarified that Face Authentication can be used as an alternative mode of biometric authentication in addition to fingerprint and iris based biometric authentication. It is further emphasised that the adoption of face authentication as an alternative modality is aimed at enhancing the inclusivity and flexibility of the Aadhaar authentication process. This step is particularly significant for individuals who may encounter difficulties with fingerprint or iris authentication due to various reasons such as age, occupation, or health conditions. By formally recognising Face Authentication, UIDAI seeks to ensure that all Aadhaar Number Holders (ANH) have equitable access to authentication services.

3. All concerned departments, agencies, and stakeholders are requested to take note of this clarification. The intent is to facilitate a seamless transition towards a more robust and user-friendly authentication framework, in line with evolving technological advancements and user needs.

4. This circular is issued with approval of the Competent Authority.

(Sanjeev Yadav)
Director
Tel: 011-23478609
Email: dir.tech@uidai.gov.in

To:
All AUAs/KUAs

Copy to:
DDG ROs: For kind information
DDG Technology Centre: For kind information

INDEX

HQ-13028/2/2024-AUTH-I HQ-Part (1)
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road
Behind Kali Mandir, Gole Market
New Delhi-110 001
Dated: 15 Jul 2025

CIRCULAR NO 2 of 2018

Subject: Partial Modification on Face Authentication Implementation

In partial modification of UIDAI Circular No. 2 of 2018 (Ref: No. K-11020/231/2018/UIDAI Auth-I) dated 15th January 2018, on the above subject, in the said circular—

(a) Para 1,2,3,4,6,7,8,9 and 10 are deleted as these are inconsistent with current developments and trends.

(b) Point 5 to be read as:

5. Face Authentication can be used as an alternative biometric mode of Authentication in addition to Fingerprint and Iris. It is further emphasized that the adoption of Face Authentication as an alternative modality is aimed at enhancing the inclusivity and flexibility of the Aadhaar authentication process. This step is particularly significant for individuals who may encounter difficulties with fingerprint or iris authentication due to various reasons such as age, occupation, or health conditions. By formally recognising Face Authentication, UIDAI seeks to ensure that all residents have equitable access to authentication services without facing undue hardship.

(c) Point 11 is newly added to intimate the stakeholders about the recent developments.

2. A copy of the said modified circular, it attached as Annex.

3. This issues with the approval of Chief Executive Officer, UIDAI.

(Sanjeev Yadav)
Director
Tel: 011-23478609
Email: dir[redacted]

To:
All AUAs/KUAs

Copy to:
DDG ROs: For kind information
DDG Technology Centre: For kind information

INDEX

F. no.: HQ-13031/1/2022-AUTH-I HQ (Comp No. 13927)
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road,
Gole Market, New Delhi – 110001
Dated: 18.07.2025

Circular No. 8 of 2025

Subject: Revised guidelines for hosting Aadhaar Data Vault (ADV), Hardware Security Module (HSM) and authentication application on premises and cloud infrastructure for Aadhaar Authentication Ecosystem.

This circular shall be read in continuation of UIDAI circular no. 11020/205/2017-UIDAI (Auth-I) dated 25.07.2017 on ADV implementation and circular no. 11020/204/2017-UIDAI (Auth-I) dated 22.06.2017 on HSM implementation.

2. All requesting entities (REs) storing Aadhaar numbers, UID Tokens and any connected Aadhaar data (e.g. eKYC XML containing Aadhaar number and demographic data) are directed to mandatorily implement the ADV.

3. Storage of Aadhaar number, UID Token or any Aadhaar demographic data received after successful Authentication or eKYC shall only be permitted within the ADV. Requesting entities are strictly prohibited for storing Aadhaar number or related data from the requested inputs by the Aadhaar number holder in Authentication/eKYC request.

4. The ADV implemented by a requesting entity must be hosted on either of the following:
   (a) on-premises (within the secure premises of the requesting entity);
   (b) on a Government Community Cloud (GCC) platform-based cloud, empaneled by MeitY (Ministry of Electronics and IT), Govt. of India; and
   (c) ADV as-a-service provided by an entity.

5. In case of GCC platform-based cloud implementation or ADV as-a-service based implementation, annual System and Organization Controls (SOC 2) Type II audit of the cloud infrastructure must be ensured by the concerned requesting entity.

6. Requesting entities must ensure the following for ADV implementation:
   (a) The GCC provider or the entity providing ADV as-a-service must be compliant with UIDAI security and privacy standards and ensure complete logical segregation of ADV for each requesting entity.
   (b) The data in ADV shall be stored in a single logical instance for each entity with the corresponding reference key which must be generated and used.
   (c) Aadhaar data must be stored in an encrypted format using strong algorithms like AES-256 or above.
   (d) High Availability and Disaster Recovery (HA/DR) shall be in place for the ADV with the same level of security along with dual redundant connectivity to the ASAs. It should have sufficient bandwidth based on respective anticipated transaction volume.
   (e) Only trusted communication channels, and secure APIs/microservices, shall be used for data access in vault.

INDEX

(f) All access must be routed through authenticated applications with appropriate user authentication, authorization and logging mechanisms.

(g) Robust access control, monitoring and alerting systems must be implemented to detect and prevent unauthorized access to ADV. Ensure strict implementation of Identity and Access Management (IAM) so that only authorized personnel and systems can access the vault. All access must be logged and monitored.

7. Requesting entities and Authentication Service Agencies (ASA) must mandatorily implement the Hardware Security Module (HSM) for cryptographic operations (such as signing of authentication request, encryption/decryption of ADV data, decryption of eKYC response data or any other operation as mandated by UIDAI time to time). The HSM must be hosted as either of the following:

(a) on-premises (within the secure premises of the requesting entity),

(b) on a Government Community Cloud (GCC) platform-based cloud, empanelled by MeitY (Ministry of Electronics and IT), Govt. of India,

(c) as HSM services provided along with ADV as-a-service by any entity.

8. Requesting entities and ASAs must ensure the following for HSM implementation:

(a) It must be FIPS 140-2 Level 3 certified or higher,

(b) It must be logically isolated for each requesting entity/ASA independently,

(c) It must support:

(i) Key Generation

(ii) Secure Key Storage

(iii) Multifactor, Multirole Access Control and Audit Logging

9. The application should rotate the key, and the requesting entity/ASA must have a mechanism in place for the prevention of unauthorized substitution of keys.

10. Aadhaar authentication applications or any module handling authentication data shall only be hosted on-premises (within the secure premises of the requesting entity) *or* on a MeitY-empanelled platform.

11. Requesting Entities and ASAs are advised to refer the latest list of MeitY-empanelled GCC services provider, available at: *https://www.ambud.meity.gov.in*. This list is maintained and updated by MeitY.

12. This issues with the approval of competent authority.

(Pratik Choudhary)
Deputy Director
Tel.: 011-23478608
Email: dd1.auth-hq@uidai.net.in

To:

1. All requesting entities and Authentication Service Agencies in Aadhaar Authentication Ecosystem

Copy to:

1. Technology Centre, UIDAI, Bangalore
2. Regional Offices, UIDAI.

INDEX

F. no. HQ-13064/1/2024-AUTH-I HQ/C-15014
Unique Identification Authority of India
(Authentication and Verification Division)

3rd floor, UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110001
Dated 31 July 2025

Circular 9 of 2025

To:

All Requesting entities (AUAs, KUAs, Sub-AUAs and Sub-KUAs) and ASAs

Subject: Aadhaar Status Notification Framework Documentation

Reference is invited to UIDAI Circular 1 of 2025 dated 1.1.2025 subjected "Execution of Supplementary Agreement or Agreement to supplement AUA Agreement under sub-regulation (3A) of regulation 9 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021".

2. For availing the Aadhaar status verification service, requesting entities are directed to use the UIDAI's provided API framework for the same. Technical specification document for Aadhaar status verification is attached in Annexure I.

3. This issues with approval of competent authority.

(Sanjeev Yadav)
Director
Tel.: 011-23478609
Email: dir2.auth-hq@uidai.net.in

Copy to:
1. All UIDAI Regional Offices
2. Technology Centre, Bangalore

INDEX

Annexure I

Unique Identification Authority of India (UIDAI)

Aadhaar Status Notification Framework

Documentation Version 1.0.0

July-2025

INDEX

Framework Overview

- **Title:** UIDAI Aadhaar Status Notification Framework
- **Description:** This API handles the subscription, notification and interrogation exchange for Aadhaar status.
- **Version:** 1.0.0

Description

1.1 UIDAI status notification framework is backed by Para 9 (3A) of the Aadhaar (Authentication and Offline Verification) Regulation, 2021 issued by UIDAI. This framework enables the requesting entities who desirous of ensuring update of status regarding an Aadhaar number previously submitted *has been subsequently omitted or deactivated or reactivated, the Authority shall send a subsequent digitally signed appropriate response, along with related technical details* may enter into this supplementary agreement with UIDAI.

1.2 The framework would be operationalised through the implementation of the following API interactions between AUA/Sub-AUA and UIDAI.

- **Subscription:** AUA/Sub-AUA to subscribe to the notification service of UIDAI. AUA/subAUA will call the UIDAI subscription endpoint to register the schedule to get the notification. *Refer to Section **2.1** for details on the subscription.*
- **Polling:** AUA/subSub-AUA AUA to poll UIDAI and get the list status change records at the scheduled interval.
- **Verification:** This API endpoint would be hosted by UIDAI to provide a mechanism to interrogate the status code and obtain the reason for rejection. *Refer to Section **3.1** for details on the interrogation.*

1.3 **Billing.** UIDAI will record the transaction for billing purposes on successful notification push to AUA/Sub-AUA . Billing would be recorded for every successful push. Cost of the transaction and invoicing is beyond the scope of the document.

API Overview

2.1 The API requests and responses are structured with three primary components:

- **Signature:** A cryptographic signature generated using HMAC (Hash-based Message Authentication Code) to ensure message integrity and authenticity.
- **Header:** Contains metadata about the message, including the version of the protocol, message identifiers, timestamps, action types, and other key details necessary to process the request and respond accordingly.
- **Message:** The core content, which includes subscription details.

INDEX

Subscription API Overview

3.1 **Summary:** This endpoint subscribes to an AUA or ASA to receive Aadhaar status notifications. The service will notify the registered endpoint whenever there is a status change related to Aadhaar.

HTTP Method: POST

```
{
  "signature": "HMAC of the {header}+{message}", "header": {
    "ver": "1.0.0",
    "msgId": "12345",
    "msgTs": "2024-12-29T10:00:00Z", "ac":
    "AUA123",
    "sa": "SubAUA001",
    "action": "subscribe",
    "isMessageEncrypted": false, "lk":
    "LICENSEKEY123"
  },
  "msg": {
    "notifyEndpoint": "https://example.com/notify", "startDate":
    "2024-12-30",
    "schedule": "0 0 * * *"
  }
}
```

Parameters:

- signature: Base 64 of HMAC signature of {header}+{message}.
- header: Contains metadata about the request.
  - ver: Version of the API (e.g., "1.0.0").
  - msgId: Unique identifier for the message.
  - msgTs: Timestamp when the message was created.
  - ac: AUA code assigned by UIDAI.
  - sa: Sub-AUA code assigned by UIDAI.
  - action: Action to be taken, set to "subscribe".
  - isMessageEncrypted: Boolean flag for encrypted message.
- msg: Contains the subscription details.
  - notifyEndpoint: The endpoint where notifications will be sent.
  - startDate: The date after which notifications should start.

INDEX

- schedule: Cron expression for scheduling the notification.

Header Parameters:

- X-Request-ID
  - **Type**: string
  - **Format**: uuid(36-byte UUID)
  - **Required**: Yes
  - **Description**: A unique identifier for the request. The value must be a 36-character UUID
- **Content-Type**: application/json

Responses:

- **200 OK**: Request was successfully processed.
- **400 Bad Request**: There was an issue with the input (e.g., invalid format, missing fields).
- **500 Internal Server Error**: There was an unexpected issue while processing the request.

Example Response


```
{
  "signature": "HMAC of the {header}+{message}", "header": {
    "ver": "1.0.0",
    "msgId": "12345",
    "msgTs": "2024-12-29T10:05:00Z", "ac":
    "AUA123",
    "sa": "SubAUA001",
    "action": "subscribe",
    "isMessageEncrypted": false
  },
  "msg": {
    "status": "success",
    "message": "Subscription successful"
  }
}
```


400 Bad Request


```
{
  "status": "failure", "error": {
    "code": "STS-GEN-001",
    "message": "Generic error: Invalid input format"
  }
```


INDEX

```
}
```

500 Internal Server Error

```
{
  "status": "failure", "error": {
    "code": "STS-GEN-001",
    "message": "Generic error occurred while processing the request."
  }
}
```

4.1 Polling API

UIDAI will host an endpoint which will be polled by the AUA/ASAs to fetch status change notification.

HTTP Method: POST

https://<<IP Address>>/uidstatus/ver/poll

4.1 Request in Encrypted Form

```
{
  "signature": "HMAC of {header}+{message}", "header": {
    "ver": "1.0",
    "msgId": "string",
    "msgTs": "ISO-8601 Timestamp", "lk": "ASA
    license key",
    "ac": "AUA Code",
    "sa": "Sub-AUA Code",
    "action": "notify", "isMessageEncrypted":
    true | false
  },
  "msg": {
    "txnId": "Unique transaction ID", "header":
    {
      "alg": "AES-256-GCM",
      "enc": "RSA-OAEP",
      "requestSessionKey": "...",
      "thumbprint": "...",
      "iv": "..."
```

INDEX

```
    },
    "data": "<Base64Url-encoded ciphertext>", "requestHMAC":
    "encrypted hash of "msg" block"
  }
}
```

4.2 Preparation of the datafield.

```
{
    "ac": "AUA license key", "sa": "Sub-
    AUA license key",
    "lastPolledDate": "ISO 8601 date"
}
```

Steps to prepare the cipher datafield as follows:-

- ASA/AUA is required to prepare the above JSON object.
- In the next step, the JSON object is required to be marshalled to a byte array.
- Post marshalling to a byte array, the hash of the byte array is to be calculated. This hash is to be used to populate the value portion of the requestHMAC key.
- Then the byte array is encrypted using a symmetric key algorithm. The key to be generated to be preserved to encrypt in the subsequent stage. **AES-256-GCM** algorithm is to be used for symmetric key encryption.
- Encrypted data is encoded as base64 string and used as value for the data field.
- The symmetric key is encrypted using the public certificate of the UIDAI and then encoded using Base64 to get the value portion of requestSessionKey.

4.3 Response in Encrypted Form

```
{
  "signature": "HMAC of {header}+{message}", "header": {
    "ver": "1.0",
    "msgId": "string",
    "msgTs": "ISO-8601 timestamp", "lk": "ASA
    license key",
    "ac": "AUA Code",
    "sa": "Sub-AUA Code",
    "action": "notify",
```

INDEX

```
        "isMessageEncrypted": false
      },
      "msg": {
        "header": {
          "alg": "AES-256-GCM",
          "enc": "RSA-OAEP",
          "requestSessionKey":
"VGhpcyBpcyBhIHNhbXBsZSBlbmNyeXB0ZWQgc2Vzc2lvbiBrZXk=",
          "thumbprint": "abcdef1234567890abcdef1234567890abcdef12", "iv":
          "MTIzNDU2Nzg5MGFiY2RlZg==" // base64url-encoded IV
        },
        "txnId": "Unique transaction ID"

"recordPending": "Total number of records pending for sync up",

"data":
      "U2FtcGxlIGVuY3J5cHRlZCBkYXRhIGJsb2lgd2l0aCB1aWQgc3RhdHVzIHJlc3 BvbnNl",
          "requestHMAC": "YWFhYmJiY2NjZGRkZWVlZmZmZ2dnZ2dn"
      }
    }
```

4.4 Decoding of the datafield

```
[
    {
      "referenceId": "Unique Reference ID", "uidToken":
      "Tokenized UID", "timestamp": "Status change
      timestamp", "status": "actv | susp | inactv"
    }
]
```

Steps to decode the datafield as follows:-

- The Base64 encoded encrypted symmetric key is decoded into byte array.
- The symmetric key is to be extracted from the value portion of the requestSessionKey. AUA/ASA to use their private key to decrypt the

INDEX

session key.

- Decode the data field, which is in base64 string into a byte array.
- The Byte array is decrypted using the **AES-256-GCM** algorithm and the symmetric key.
- The hash of the byte array is computed and then compared with the requestHMAC.
- Decrypted Byte array is then marshalled into a JSON object as represented above.

4.5 Attribute Definition

The following attributes are used in status notification request - response.

- signature: HMAC signature of {header}+{message}.
- header: Contains metadata about the notification.
  - ver: API version.
  - msgId: Message ID.
  - msgTs: Timestamp when the message was created.
  - ac: AUA code.
  - sa: Sub-AUA code.
  - action: Set to "notify".
  - isMessageEncrypted: Boolean flag indicating whether the message is encrypted.
- msg: Contains the notification data:
  - txnId: Transaction ID for the notification event.
  - recordPending : Number of records pending for notification.
  - data: List of status change UIDs in tokenized form.
  - requestHMAC : HMAC of the cleartext byte array
  - header:
    i. alg: Defines the symmetric encryption algorithm used to encrypt the message. For example, AES (Advanced Encryption Standard) can be used in modes such as CBC (Cipher Block Chaining) or GCM (Galois/Counter Mode). **UIDAI at present supports only AES-256-GCM.**
    ii. enc: Specifies the asymmetric encryption algorithm used to encrypt the session key (e.g., RSA). Asymmetric encryption allows the session key to be securely shared between the sender and the receiver. **UIDAI at present supports only RSA-OAEP.**
    iii. requestSessionKey: The actual session key used to encrypt the message. The session key is encrypted with an asymmetric encryption algorithm (like RSA) and then Base64Url-encoded to ensure it's safely transmitted.
    iv. thumbprint: The thumbprint of the public key that was used to

INDEX

encrypt the session key. This thumbprint ensures that the correct public key is being used and allows the recipient to verify the key used for encryption.

v. IV: The Initialization Vector used in encryption. The IV ensures that even if the same plaintext is encrypted multiple times, it will produce different ciphertexts each time. The IV is typically a random bit string used in modes like AES-CBC.

5.1 UID Status Verification API

The UID Status Verification API allows Authentication User Agencies (AUAs) and Sub-AUAs (Sub-Authentication User Agencies) to check the status of a UID (Unique Identification Number) or a list of UIDs after receiving status modification intimations from UIDAI. This API is designed to facilitate secure, real-time access to the status of UIDs to ensure accurate and up-to-date identity information for services requiring Aadhaar-based authentication.

The API request and response are structured with three primary components:

- **Signature**: A cryptographic signature generated using HMAC (Hash-based Message Authentication Code) to ensure message integrity and authenticity.
- **Header**: Contains metadata about the message, including the version of the protocol, message identifiers, timestamps, action types, and other key details necessary to process the request and respond accordingly.
- **Message**: The core content, which includes encrypted data, encryption details (such as algorithm and keys), and a session key to securely communicate the UID status check.

This specification outlines the message format, the cryptographic methods used, and the endpoint details, ensuring secure, efficient, and standard-compliant communication between parties using the UID Status Verification API. The API supports both encrypted and non-encrypted message exchanges, with the flexibility to accommodate varying use cases for UID status verification.

5.1.1 Sample Request

```
{
  "signature": "HMAC of the {header}+{message}", "header": {
```

INDEX

```
    "ver": "1.0.0",
    "msgId": "12345",
    "msgTs": "2024-12-29T10:00:00Z",
    "action": "search",
    "tid": "registered",
    "ac": "AUA123",
    "sa": "SubAUA001", "lk":
    "LICENSEKEY123",
    "totalCount": 100,
    "isMsgEncrypted": false
  },
  "msg": {
    "header": {
      "alg": "AES-256-GCM",
      "enc": "RSA-OAEP",
      "requestSessionKey": "encrypted_session_key",
      "thumbprint": "thumbprint_string",
      "iv": "initialization_vector"
    },
    "data": "Base64Url-encoded encrypted payload",
    "requestHMAC": "HMAC of the encrypted message"
  }
}
```

Data Block before encryption:

```
[
  {
    "type": "uid",
    "uidToken": "123456789012"
  },
  {
    "type": "uid",
    "uidToken": "987654321098"
  },
  {
    "type": "token", "uidToken":
    "abcdef123456"
```

INDEX

```
        ]
    ]
```

5.1.2 Sample Response

```
{
  "signature": "HMAC of the {header}+{message}", "header": {
    "version": "1.0.0",
    "msgId": "12345",
    "msgTs": "2024-12-29T10:05:002",
    "action": "search",
    "ac": "AUA123",
    "sa": "SubAUA001",
    "totalCount": 100,
    "isMsgEncrypted": false
  },
  "msg": {
    "header": {
      "alg": "AES with GCM",
      "enc": "RSA",
      "requestSessionKey": "encrypted_session_key",
      "thumbprint": "thumbprint_string",
      "iv": "initialization_vector"
    },
    "data": "Base64Url-encoded encrypted payload",
    "requestHMAC": "HMAC of the encrypted response"
  }
}
```

Data Block post decryption

```
[
  {
    "uidToken": "abcdef123456",
    "uidStatus": "ACTIVE",
    "errorCode": "0", "errorMsg":
    "No error"
  },
```

INDEX

```
    {
      "uidToken": "987654abcdef123456321098", "uidStatus":
      "INACTIVE",
      "errorCode": "0",
      "errorMsg": "No error"
    },
    {
      "token":"abcdef123456656",
      "uidStatus": "",
      "errorCode": "STV-VER-001",
      "errorMsg": "UID status processing failed"
    }
  ]
```


5.2 Attribute Definition

The following attributes are defined within the UID Status Verification API for both the request and response. These attributes describe the structure and purpose of each part of the message for clarity and standardization.

- signature: HMAC signature of {header}+{message}.
- header: Contains metadata about the notification.
  - version: The version of the messaging protocol being used (e.g., "0.1.0").
  - msgId: A unique identifier for the message, used for tracking and correlation.
  - msgTs: Timestamp when the message was created, represented in ISO 8601 format.
  - action: The action to be performed (e.g., "search" for UID status check).
  - ac: Unique code identifying the AUA (Authentication User Agency).
  - sa: Code identifying the Sub-AUA (if applicable).
  - lk: The license key for the AUA or Sub-AUA.
  - totalCount: Number of records in the batch being processed.
  - isMsgEncrypted: Boolean flag indicating whether the message body is encrypted.
- msg:
  - header: Metadata for the encrypted message, including encryption settings and keys.
    - alg: The encryption algorithm used (e.g., "AES with GCM").
    - enc: Encryption method or mode used.
    - requestSessionKey: The session key used for the encryption.
    - thumbprint: A fingerprint of the public key used for encryption.

INDEX

- iv: The initialization vector for the encryption.
- data: The encrypted and base64-encoded payload containing the UID status check request.
  - uidToken: The UID token whose status is being returned (e.g., "123456789012" or a token value).
  - uidStatus: The current status of the UID (e.g., "ACTIVE", "INACTIVE", etc.).
  - errorFlag: An optional flag indicating if there was an error in processing the UID status. This could be used to return error details.
- requestHMAC: The HMAC used to validate the integrity of the request message.

6. Analytics Events

On successful notification of status change information to the AUA, an event would be generated, which will serve dual purpose i.e. invoicing with AUA/subAUA and business monitoring of the process. Event would comprise of following attributes:

- Event Metadata
  - _eventId : UUID value to uniquely identify the event
  - _eventType : "AADHAAR_STATUS_NOFICATION_PUSH"
  - _eventTimestamp: Event Timestamp in ISO Format
  - _version : Version of the Event Structure
- Payload
  - requestId : x-request-id of the transaction
  - msgId: message ID of the UIDAI Event
  - msgTs : Timestamp
  - refId : ReferenceId of ANH
  - ac : AUA Code
  - sa : subAUA Code
  - responseStatus : Response Status from AUA/subAUA

INDEX

F. No. HQ-13084/7/2025-AUTH-II HQ/C-18590
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated: 01 Aug 2025

Circular 10 of 2025

Subject: UIDAI framework for onboarding of State Co-operative Banks (StCBs) and District Central Co-operative Banks (DCCBs) in Aadhaar Authentication Ecosystem

Based on the requests received from National Bank for Agriculture and Rural Development (NABARD) and from various co-operative banks, Ministry of Cooperation and NPCI, a committee was constituted *vide* Order no. HQ-13018/1/2025-AUTH-II HQ/C-17855, dated 23.5.2025, to discuss on framework for onboarding of co-operative banks under chairmanship of Director (A&V) UIDAI.

2. On the basis of recommendation of the committee, a policy framework has been designed to onboard the (StCBs) and their associated DCCBs with ease on UIDAI Aadhaar authentication ecosystem. The policy framework document, along-with the form (comprising details of their respective DCCBs) to be submitted by the State Co-operative Banks is attached as **Annexure**.

3. This issues with the approval of the competent authority.

(Sanjeev Yadav)
Director
Tel: 011-23478609
Email: dir2.auth-hq@uidai.net.in

Copy to:

1. Secretary, Ministry of Cooperation, Government of India, New Delhi
2. Managing Director and CEO (NPCI)
3. Chairman (NABARD), with request to circulate to all (StCBs) and DCCBs
4. All State Co-operative Banks

Copy to for information:

1. All Regional Offices, UIDAI
2. Technology Centre, Bangalore
3. Sh. Kumar Ram Krishna, Director, Ministry of Cooperation
4. Sh. Ajay Pal, Head AePS, NPCI
5. Sh. James P George, DGM, NABARD
6. Sh. Pankaj Pandey, Chief Technical Officer, Uttar Pradesh Co-operative Bank.

Annexure-I

UIDAI framework for onboarding of Co-operative Bank

for inclusion of Co-operative Banks in Aadhar Ecosystem

1. Objective

This policy framework will be named as "UIDAI framework for onboarding of Co-operative Bank" (hereinafter new framework) and it aims to institutionalize the process for the inclusion of co-operative Banks in the Aadhaar ecosystem. The objective is to enable these co-operative banks to leverage Aadhaar-based authentication services for customer onboarding and Aadhar Enabled payment System (AePS) for the secure, efficient and transparent delivery of financial service especially to rural and underserved populations. The integration of co-operative banks into AePS is aligned with the Government of India's goal of achieving universal financial inclusion. A comprehensive, coordinated strategy comprising financial assistance, technical facilitation, and policy-level interventions is proposed to realize this vision.

2. Background

(a) The Unique Identification Authority of India (UIDAI) plays a crucial role in enabling real-time online authentication for delivery of service, facilitating de-duplication, and streamlining customer onboarding through various modes and biometric modalities, including face authentication.

(b) New framework is in alignment with the objectives outlined in the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016. The Act empowers the UIDAI to provide a digital identity platform, enabling the authentication of individuals' identity for the delivery of services and benefits.

(c) The AePS system developed by the National Payments Corporation of India (NPCI) is a key digital public infrastructure designed to promote financial inclusion. It facilitates interoperable Aadhaar-based transactions that includes both financial and non-financial services via Micro-ATMs deployed at Customer Service Points (CSPs). AePS plays a pivotal role in expanding banking access to India's remotest regions and supports the overarching objectives of the Digital India initiative.

(d) By recognizing the indispensable role of co-operative banks in serving agrarian and rural population in the country, it is imperative to onboard these banks to AePS ecosystem to ensure last-mile delivery of financial services.

(e) Ministry of Cooperation (MoC) has also issued directions to facilitate faster onboarding of all co-operative banks in Aadhaar ecosystem.

3. Key Stakeholders

(a) Unique Identification Authority of India (UIDAI)

(b) National Payments Corporation of India (NPCI)

(c) State and District Central Co-operative banks ((StCBs) and DCCBs)

(d) National Bank for Agriculture and Rural Development (NABARD)

4. **Facilitation and Support**

(a) A new identification is proposed to be given to DCCBs called as "DCB-ID". This DCB-ID will act as internal identifier for the StCBs.

(b) **Extension of DCB-ID**: All DCCBs will be onboarded by StCB through an internal identifier. List of all such DCB-ID will be shared with UIDAI and after approval of UIDAI, onboarding of DCCBs will be done. Any addition or deletion for onboarding/deboarding of DCCBs will be after approval of UIDAI only.

(c) **Simplified compliance requirement:** Addressing of the regulatory obligation by respective State or Apex co-operative banks.

(d) **Capacity Building Initiatives**: Joint training programmes are recommended to be conducted by UIDAI's regional offices, NABARD and NPCI to enhance awareness and ensuring technical readiness.

5. **Way Forward –Terms of the Policy**

To support smooth onboarding of co-operative banks in Aadhaar ecosystem for enablement of AePS, the following policy measures are proposed:

a) **Financial Support by NABARD:**
   (i) As committed by NABARD, infrastructure setup costs (e.g., ADV, HSM) for the same shall be borne by NABARD.
   (ii) All miscellaneous onboarding-related expenses will be borne by NABARD.

b) **Technical handholding by NPCI:**
   (i) NPCI will provide comprehensive technical support and guidance for onboarding eligible member banks on AePS.
   (ii) NPCI will facilitate prioritised test slots and faster integration cycles.
   (iii) Joint training sessions will be conducted by NPCI with other stakeholders.
   Note: Banks to follow NPCI guidelines, procedures and process for onboarding on AePS.

c) **Regulatory easing by UIDAI:**
   (i) UIDAI will provide advisory support during the onboarding process.
   (ii) UIDAI will do the technical handholding in ensuring compliance requirements.
   (iii) Consideration of all DCCBs and the respective State/Apex Co-operative bank as a single entity for the purposes of licensing and regulatory compliances.

6. **Onboarding Process Flow for co-operative Banks:**

This framework outlines a streamlined approach for onboarding of State and District Co-operative banks as a requesting entity in Aadhaar ecosystem. It aligns with the approach of "One State One Apex Co-operative Bank" to ensure centralized compliance and enhance operational efficiency.

(a) UIDAI will onboard State Co-operative Bank as a master Authentication User Agency (AUA) and e-KYC User Agency (KUA), subject to official recognition and submission of the requisite onboarding documents.

(b) The State Co-operative Bank shall make an application to UIDAI to get onboarded as an AUA/KUA.

(c) UIDAI will grant in-principal approval based on the evaluation of submitted documents by the respective bank subject to execution of the agreement, deposit of prescribed license fee as applicable for AUA and KUA, transaction validation and submission complied IS audit report conducted by a CERT-In empanelled auditor.

(d) After meeting all pre-production requirements, the co-operative bank will be onboarded in production post approval of the Competent Authority.

(e) Once State Co-operative Bank is onboarded as an AUA/KUA in production, a request letter on the letter head of State Co-operative bank addressing to the CEO UIDAI along with onboarding documents, shall be submitted on behalf of its District Central Co-operative Bank (DCCBs) for issuance of "DCB-ID".

(f) DCCBs will only use the DCB-ID code issued by UIDAI, based on the recommendation of the State Co-operative bank. The State Co-operative bank cannot onboard any DCCBs independently without notifying and obtaining formal approval from UIDAI.

(g) UIDAI will raise invoice to the StCB for all authentication transaction charges pertaining to the onboarded DCCBs. There shall be no separate license fee charged to the DCCBs owing to StCBs and its DCCBs being considered as one single entity and DCCBs like branches of respective StCBs.

(h) State Co-operative bank shall ensure that all its DCCBs comply with the provisions of the Aadhaar Act, 2016 and its associated regulations, directions, processes, standards, guidelines, notifications, specifications and protocols, as issued by UIDAI.

7. Policy for existing onboarded co-operative banks

(a) All new onboarding of StCBs and DCCBs will be as per the "UIDAI framework for onboarding of Co-operative Banks".

(b) Should any co-operative bank desire, they may choose to be onboarded as per existing policy of AUA/KUA and Sub-AUA/Sub-KUA.

(c) Existing co-operative banks may choose to continue with the existing structure as AUA/KUA and Sub-AUA/Sub-KUA or these co-operative banks may choose to adopt new framework.

(d) The license fee once paid by co-operative banks already in production or in pre-production till issue of the new framework will not be refunded. After the current license fee cycle, the co-operative banks may make payment of license fee as per new framework.

Encl: Application form for onboarding DCCBs

****

Annexure

Application for appointment as a DCCBs under (StCBs) as per the framework of onboarding of co-operative Bank

Details of the DCCBs						Details of Key Managerial Person of (StCBs)				
State	Name of DCCBs	Registration/Incorporation No.	RBI License No. (Pls attach copy of the document)	Registered Office address	GSTN registration number	Name	Email	Full Designation	Mobile Number	Alternate office telephone number
1	2	3	4	5	6	7	8	9	10	11

Page 4 of 4

INDEX

F. no. HQ-13043/1/2025-AUTH-I HQ (Comp:18668)
Unique Identification Authority of India
(Authentication and Verification Division)

3rd floor, UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110 001
Dated: 15th Sep 2025

To

All AUA/KUAs, ASAs, Biometric Device Vendors in Aadhaar Authentication Ecosystem

Subject: Introduction of L1 Compliant Iris Authentication Registered Devices in Aadhaar Authentication Ecosystem

Unique Identification Authority of India (UIDAI), in collaboration with biometric device vendors, STQC, and C-DAC, is improving the Aadhaar Authentication Ecosystem's security and efficiency. They are upgrading from L0 compliant Iris Authentication Registered Devices to L1 compliant devices, reaffirming UIDAI's commitment to providing strong and secure authentication processes.

Key Features of L1 Compliant Iris Authentication Registered Devices:

1. Device Security with Level 1 Compliance: Signing and encryption of biometric data are performed within a Trusted Execution Environment (TEE), ensuring that host OS processes or users cannot access the private key or inject biometrics. Private key management is fully contained within the TEE.
2. Secure System Design: Aligned with the key objectives of the UIDAI RD Service Specification (latest version).
3. Implementation of RD Service and Management Client: Compliant with the latest RD Service Specification.
4. Iris Liveness Check: Implementation of liveness detection with Fake Iris Detection (FID)
5. Standardized and Certified Device Driver: Provided by biometric device vendors, this driver (exposed via SDK/Service) encapsulates biometric capture, user experience (e.g., preview), and signing and encryption within the TEE. The driver forms the encrypted PID block before returning to the host application.

INDEX

6 Detailed Specifications: Refer to the document "Aadhaar Registered Devices - Technical Specification Version 2.0 (Revision 7) January 2022" (attached as annexure) and latest API Specifications

Action Required:

1 Transitioning from L0 to L1 registered devices: L0 iris authentication devices will gradually be phased out. Once L1 iris registered devices are available, all future purchases of iris authentication devices must comply with L1 specifications. While L0 devices will remain operational for now, any deployed L0 devices with expired or non-renewed STQC certificates must be removed. A separate notification will be released to announce the sunset date for L0 Iris registered devices.
2 Application Modifications: AUAs and KUAs need to update their authentication applications and backend servers to accommodate L1 compliant iris-registered devices and the latest Aadhaar Authentication API specifications. Technical teams should be made aware of these updates and carry out thorough testing to ensure seamless compatibility.
3 Phase-Out of Expired Devices: AUAs/KUAs need to identify and remove L0 iris devices with expired STQC certificates by December 31, 2025, as authentication services on these devices will no longer be supported after this date.

UIDAI encourages all partners to actively adopt L1-compliant iris devices to enhance the security of the Aadhaar Authentication Ecosystem.

This issues with the approval of the competent authority.

(Pratik Choudhary)
Deputy Director
Tel.: 011-23478608
Email: dd1.auth-hq@uidai.net.in

Copy for information to:

1 DG, STQC
2 DDG (Tech Centre, UIDAI)

INDEX

F. No. HQ-13079/5/2023-AUTH-II HQ/C-10846
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110 001
Dated 14 October 2025

Circular No.11 of 2025

Subject: Extension of Authentication Service Agency facilities to other requesting entities

Ref: UIDAI Circular No. 5 of 2025, dated 29.5.2025 issued *vide* letter of even no. and regulation 19(i) of the Aadhaar (Authentication and Offline Verification) Regulations, 2021.

As per the *ibid* regulation and circular, all Authentication Service Agency (ASA) are required to comply with directions, specifications, etc. issued by the Authority, in terms of network and other Information Technology infrastructure, processes, procedures, etc.

2. To bring in more resilience in their authentication framework, certain requesting entities' may use services of more than one ASA or may approach co-located ASA. Hence, in terms of clause 2(d) and (e) of the said circular, it is reiterated that:

(a) ASAs shall extend ASA services to other requesting entities for optimum utilisation of infrastructure and wider accessibility of Aadhaar authentication facilities; and
(b) ASAs shall maintain dual redundant connectivity with sufficient MPLS bandwidth to ensure high availability, failover support and uninterrupted services.

4. All ASAs shall submit an undertaking on their letterhead, in the form and substance of **Annexure I**, conforming with the compliance above, to be received by UIDAI by 10.11.2025.

5. This issues with the approval of competent authority.

(Arpit Agrawal)
Deputy Director
Tel. 011-23478641
Email: dd2.auth-hq@uidai.net.in

IN REF.
INDEX

Annexure I

[To be printed on letter head of ASA]

Undertaking by Authentication Service Agency (ASA) to extend existing ASA connectivity services to other Authentication User Agency (AUA)/eKYC User Agency (KUA)

We, _____ [1] in compliance with UIDAI Circular 5 of 2025, dated 29.5.2025, clause 2(d) & (e), and regulation 19(i) of the Aadhaar (Authentication and Offline Verification) Regulations, 2021, hereby undertake that—

(a) extend ASA connectivity services to any other requesting entities as and when the request is received from in a fair and non-discriminatory manner, ensuring optimal utilization of ASAs existing infrastructure;

(b) to maintain dual redundant connectivity, which is essential for ensuring high availability and failover support with sufficient MPLS bandwidth in proportion to existing load for ensuring of uninterrupted services towards existing and newly onboarded AUA/KUAs;

(c) to increase the bandwidth by developing required infrastructure, to be able to cater upcoming demands from any requesting entity of UIDAI for performing Aadhaar Authentication;

(d) to comply with UIDAI directions, specifications, and instructions in respect of network, IT infrastructure, processes and procedures, etc; and

(e) submit to UIDAI, as required, the summary with details of requesting entities availing connectivity services through us.

(Signature with stamp/seal of authorised signatory)

Name: _____

Full designation: _____

Date: _____

Place: _____

_____

[1] Name of ASA

INDEX

F. No. HQ-13064/1/2024-AUTH-I HQ/C. 15014
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated: 24th October, 2025

Circular 12 of 2025

Subject: Execution of Supplementary Agreement or Agreement to supplement AUA Agreement under sub-regulation (3A) of regulation 9 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021

With the Aadhaar (Authentication and Offline Verification) Amendment Regulations, 2024 dated 31.1.2024, UIDAI has introduced a provision, for sharing of update of status of Aadhaar number upon entering Supplementary Agreement or Agreement to supplement AUA Agreement ("agreement") by requesting entity ("RE") with UIDAI, as sub-regulation (3A) under regulation 9 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021. The said provision is as below—

"(3A) Where the requesting entity has entered into a Memorandum of Understanding or agreement with the Authority for the performance of authentication with update of status regarding whether an Aadhaar number previously submitted has been subsequently omitted or deactivated or reactivated, in the event of such Aadhaar number being omitted or deactivated or such a deactivated Aadhaar number being reactivated, the Authority shall send a subsequent digitally signed appropriate response, along with related technical details."

2. The purpose of the agreement is to set out the terms and conditions for RE for performance of authentication with update of status of Aadhaar numbers previously submitted, in the event of such an Aadhaar number being subsequently omitted or deactivated Aadhaar number being re-activated. This sharing of data will be helpful for RE for their data cleansing and preventing any misuse of facilities and services being offered by it.

3. Eligibility for signing agreements and responsibilities of entities: -

(a) The entity which is already appointed as RE (**AUA/KUA/Sub-AUA/Sub-KUA**) with UIDAI are eligible to make request for such update of status of Aadhaar number upon entering the agreement with UIDAI. The said agreement shall be executed on non-judicial stamp paper of value as applicable.

(b) AUAs/KUAs shall keep UIDAI informed of such agreements executed with their Sub-AUAs/Sub-KUAs and maintain updated records for audit and compliance purposes.

INDEX

(c) Hence, any Sub-AUA and Sub-KUA desirous to avail this Aadhaar authentication facility for performance of authentication with update of status of Aadhaar numbers may enter into a separate agreement with its concerned AUA/KUA, in the form and substance of the template provided at 'Annexure A' of the Supplementary Agreement attached as **Annexure-I**.

4. Two copies of the agreement (original and duplicate) duly signed by the authorized representative of the RE shall be sent to UIDAI for signature. The original signed copy shall be retained by UIDAI for record purposes and duplicate signed copy will be sent to RE by UIDAI.

5. The RE (AUA/KUA/Sub-AUA/Sub-KUA), for the performance of authentication under the said agreement, shall be charged to pay such fees, including applicable taxes, as UIDAI may specify in **sub-regulation 2A of regulation 3 of The Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2021 (as amended).**

6. Enclosers with this letter are templet for supplementary agreement with AUA/KUA and template of separate agreement between AUA/KUA and their Sub-AUA/Sub-KUA.

7. *For any queries regarding the agreement, you are requested to mail to UIDAI at onboarding@uidai.net.in*

8. This circular will be superseding the existing circular no. 1 of 2025, dated 01.01.2025.

9. This issues with the approval of competent authority.

Encl: as above

(Sanjeev Yadav)
Director
Tel.: 011-23478609
Email: dir2.auth-hq@uidai.net.in

To:

1. Secretaries in charge of Ministries and Departments in Government of India (as per list attached)
2. Chairperson and Chief Executive Officer, Railway Board
3. Chief Secretaries of State Governments (as per list attached)
4. Chief Secretary, Government of Jammu and Kashmir / National Capital Territory of Delhi / Puducherry / Andaman and Nicobar Islands Administration
5. Advisor to Administrator, Chandigarh Administration
6. Advisor to Lieutenant Governor, Ladakh Administration
7. Administrator, Dadra and Nagar Haveli and Daman and Diu Administration / Lakshadweep Administration

INDEX

Copy, for information, to:

1. Advisor to Prime Minister, Prime Minister's Office
2. Chief Executive Officer, NITI Aayog
3. Secretary (Coordination), Cabinet Secretariat
4. All Deputy Directors General, UIDAI
5. All Authentication User Agency and e-KYC User Agency

INDEX

List of addressee Secretaries

1. Secretary, Department for Promotion of Industry and Internal Trade, Vanijya Bhawan, New Delhi – 110 011
2. Secretary, Department of Administrative Reforms and Public Grievances, 513, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001
3. Secretary, Department of Agricultural Research and Education, First floor, Krishi Bhawan, New Delhi – 110 001
4. Secretary, Department of Agriculture and Farmers Welfare, Krishi Bhavan, Dr Rajendra Prasad Road, New Delhi – 110 001
5. Secretary, Department of Animal Husbandry and Dairying, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
6. Secretary, Department of Atomic Energy, E Block, Raisina Hill, New Delhi – 110 011
7. Secretary, Department of Biotechnology, 7th floor, Block-2, CGO Complex, Lodhi Road, New Delhi – 110 003
8. Secretary, Department of Chemicals and Petrochemicals, 236A, A Wing, 2nd floor, Shastri Bhawan, New Delhi – 110 001
9. Secretary, Department of Commerce, Udyog Bhawan, New Delhi – 110 011
10. Secretary, Department of Consumer Affairs, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
11. Secretary, Department of Drinking Water and Sanitation, C Wing, 4th floor, Paryavaran Bhawan, CGO Complex, Lodhi Road, New Delhi – 110 003
12. Secretary, Department of Economic Affairs, North Block, New Delhi - 110 001
13. Secretary, Department of Empowerment of Persons with Disabilities, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
14. Secretary, Department of Ex-servicemen Welfare, South Block, New Delhi – 110 011
15. Secretary, Department of Fertilizers, A Wing, Shastri Bhawan, New Delhi – 110 001
16. Secretary, Department of Financial Services, 3rd floor, Jeevan Deep Building, Parliament Street, New Delhi – 110 001
17. Secretary, Department of Fisheries, Krishi Bhawan, New Delhi – 110 001
18. Secretary, Department of Food and Public Distribution, H Wing, Krishi Bhawan, New Delhi – 110 001
19. Secretary, Department of Health and Family Welfare, A Wing, Nirman Bhavan, New Delhi – 110 011
20. Secretary, Department of Health Research, 1, Red Cross Road, Gokul Nagar, New Delhi – 110 001
21. Secretary, Department of Higher Education, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
22. Secretary, Department of Investment and Public Asset Management, 4th floor, Block No. 11 CGO Complex, Lodhi Road New Delhi – 110 003
23. Secretary, Department of Land Resources, NBO Building, G Wing, Nirman Bhawan, Dr Maulana Azad Road, New Delhi – 110 011
24. Secretary, Department of Official Language, NDCC-II Bhawan, A Wing, 3rd floor, Jai Singh Marg, New Delhi – 110 001

INDEX

25. Secretary, Department of Pension and Pensioners' Welfare, 514, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001
26. Secretary, Department of Personnel and Training, North Block, New Delhi – 110 001
27. Secretary, Department of Pharmaceuticals, A Wing, Shastri Bhawan, New Delhi – 110 001
28. Secretary, Department of Posts, Dak Bhawan, Patel Chowk, New Delhi – 110 001
29. Secretary, Department of Public Enterprises, Block-14, CGO Complex, Lodhi Road, New Delhi – 110 003
30. Secretary, Department of Rural Development, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
31. Secretary, Department of School Education and Literacy, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
32. Secretary, Department of Science and Technology, Technology Bhawan, New Mehrauli Road, New Delhi – 110 016
33. Secretary, Department of Scientific and Industrial Research, Technology Bhawan, New Mehrauli Road, New Delhi – 110 016
34. Secretary, Department of Social Justice and Empowerment, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
35. Secretary, Department of Space, Antariksh Bhavan, New BEL Road, Bangalore – 560 231
36. Secretary, Department of Sports, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
37. Secretary, Department of Telecommunications, Sanchar Bhawan, 20, Ashoka Road, New Delhi – 110 001
38. Secretary, Department of Water Resources, River Development and Ganga Rejuvenation, Shram Shakti Bhawan, Rafi Marg, New Delhi – 110 001
39. Secretary, Department of Youth Affairs, Room No. 1, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
40. Secretary, Legislative Department, A Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
41. Secretary, Ministry of AYUSH, Ayush Bhawan, B Block, GPO Complex, Barapullah Road, INA Colony, New Delhi – 110 023
42. Secretary, Ministry of Civil Aviation, Rajiv Gandhi Bhawan, Block B, Jor Bagh, Safdarjung Airport Area, New Delhi – 110 003
43. Secretary, Ministry of Coal, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
44. Secretary, Ministry of Cooperation, 2nd floor, Atal Akshya Urja Bhawan, Pragati Vihar, New Delhi – 110 003
45. Secretary, Ministry of Corporate Affairs, A Wing, Shastri Bhawan, Rajendra Prasad Road, New Delhi – 110 001
46. Secretary, Ministry of Culture, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
47. Secretary, Ministry of Development of North Eastern Region, Vigyan Bhawan Annexe, Maulana Azad Road, New Delhi – 110 011

INDEX

48. Secretary, Ministry of Earth Sciences, Mahasagar Bhawan, Block - 12, C.G.O Complex, Lodhi Road, New Delhi – 110 003
49. Secretary, Ministry of Electronics and Information Technology, 6, CGO Complex, Lodhi Road, New Delhi - 110 003
50. Secretary, Ministry of Environment, Forest and Climate Change, Indira Paryavaran Bhawan, Jor Bagh Road, New Delhi - 110 003
51. Secretary, Ministry of Food Processing Industries, Panchsheel Bhawan, August Kranti Marg, New Delhi – 110 049
52. Secretary, Ministry of Heavy Industries, Udyog Bhawan, New Delhi - 110 001
53. Home Secretary, Ministry of Home Affairs, North Block, New Delhi – 110 001
54. Secretary, Ministry of Housing and Urban Affairs, Nirman Bhawan, C Wing, Dr Maulana Azad Road, New Delhi - 110 011
55. Secretary, Ministry of Information and Broadcasting, Dr Rajendra Prasad Road, Shastri Bhawan, New Delhi – 110 001
56. Secretary, Ministry of Labour and Employment, Shram Shakti Bhawan, Rafi Marg, New Delhi - 110 001
57. Secretary, Ministry of Micro, Small and Medium Enterprises, Udyog Bhawan, Rafi Marg, New Delhi – 110 011
58. Secretary, Ministry of Mines, A Wing, 3rd floor, Shastri Bhawan, New Delhi - 110 001
59. Secretary, Ministry of Minority Affairs, 11th floor, Paryavaran Bhawan, CGO Complex, Lodhi Road, New Delhi - 110 003
60. Secretary, Ministry of New and Renewable Energy, Block no. 14, CGO Complex, Lodhi Road, New Delhi - 110 003
61. Secretary, Ministry of Panchayati Raj, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi - 110 001
62. Secretary, Ministry of Parliamentary Affairs, Parliament House, Sansad Marg, New Delhi – 110 001
63. Secretary, Ministry of Petroleum and Natural Gas, Shastri Bhawan, Rajendra Prasad Road, New Delhi - 110 001
64. Secretary, Ministry of Ports,Shipping and Waterways, Transport Bhavan, 1, Parliament Street, New Delhi – 110 001
65. Secretary, Ministry of Power, 2nd floor, Shram Shakti Bhawan, New Delhi – 110 001
66. Secretary, Ministry of Road Transport and Highways, Transport Bhavan, 1, Parliament Street, New Delhi – 110 001
67. Secretary, Ministry of Skill Development and Entrepreneurship, 2nd floor, Shivaji Stadium Annexe, Shaheed Bhagat Singh Marg, New Delhi – 110 001
68. Secretary, Ministry of Statistics and Programme Implementation, 418, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001
69. Secretary, Ministry of Steel, Udyog Bhawan, New Delhi – 110 001
70. Secretary, Ministry of Textiles, Udyog Bhawan, New Delhi - 110 001
71. Secretary, Ministry of Tourism, Transport Bhavan, 1, Parliament Street, New Delhi - 110 001
72. Secretary, Ministry of Tribal Affairs, B Wing, Shastri Bhawan, New Delhi – 110 001
73. Secretary, Ministry of Women and Child Development, Shastri Bhawan, A Wing, Dr Rajendra Prasad Road, New Delhi – 110 001

INDEX

List of Chief Secretaries to State Governments

1. Chief Secretary, Government of Kerala, Secretariat, Thiruvananthapuram – 695 001, Email: chiefsecy@kerala.gov.in
2. Chief Secretary, Government of Jharkhand, 1st floor, Project Bhawan, Mantralaya, Dhurwa, Ranchi – 834 004, Email: cs-jharkhand@nic.in
3. Chief Secretary, Government of West Bengal, Nabanna, 13th floor, 325, Sarat Chatterjee Road, Shibpur, Howrah - 711 102, Email: cs-westbengal@nic.in
4. Chief Secretary, Government of Odisha, Odisha State Secretariat, Sachivalaya Marg, Unit-2, Bhubaneswar, Email: csori@nic.in
5. Chief Secretary, Government of Manipur, Babupara, Imphal West, Manipur – 795 001, Email: cs-manipur@nic.in
6. Chief Secretary, Government of Uttar Pradesh, 1st floor, Room no. 110, Lal Bahadur Shastri Bhawan, Lucknow – 226 001, Email: csup@nic.in
7. Chief Secretary, Government of Chhattisgarh, Mantralaya, Naya Raipur, Chhattisgarh - 492 002, Email: csoffice.cg@gov.in
8. Chief Secretary, Government of Karnataka, Room no. 320, 3rd floor, Vidhana Soudha, Bengaluru – 560 001, Email: cs@karnataka.gov.in
9. Chief Secretary, Government of Uttarakhand, 4 Subhash Road, Uttarakhand Secretariat, Dehradun - 248 001, Email: cs-uttarakhand@nic.in
10. Chief Secretary, Government of Madhya Pradesh, 4th floor, Mantralaya, Vallabh Bhavan-I, Bhopal – 462 004, Email: cs@mp.nic.in
11. Chief Secretary, Government of Punjab, 6th floor, Punjab Civil Secretariat-1, Sector 1, Chandigarh – 160 001, Email: cs@punjab.gov.in
12. Chief Secretary, Government of Telangana, Telangana Secretariat, 5th floor, Burgula Rama Krishna Rao Bhavan NH 44, Hill Fort, Adarsh Nagar, Hyderabad - 500 063, Email: cs@telangana.gov.in
13. Chief Secretary, Government of Andhra Pradesh, 1st Block, 1st floor, Andhra Pradesh Secretariat Office, Velagapudi – 522 023, Email: cs@ap.gov.in
14. Chief Secretary, Government of Arunachal Pradesh, Block-II, 5th floor, Civil Secretariat, Itanagar – 791 111, Email: cs-arunachal@nic.in
15. Chief Secretary, Government of Assam, Assam Secretariat, CM Block, Second Floor Dispur, Guwahati - 781 006, Email: cs-assam@nic.in
16. Chief Secretary, Government of Bihar, Main Secretariat, Patna – 800 015, Email: cs-bihar@nic.in
17. Chief Secretary, Government of Goa, Secretariat, Porvroim, Bardez – 403 521, Email: cs-goa@nic.in
18. Chief Secretary, Government of Gujarat, 1st Block, 5th floor, Sachivalaya, Gandhinagar, Email: chiefsecretary@gujarat.gov.in
19. Chief Secretary, Government of Haryana, 47, 9th floor, Haryana Civil Secretariat, Sector-1, Chandigarh - 160 001, Email: cs@hry.nic.in
20. Chief Secretary, Government of Himachal Pradesh, Himachal Pradesh Secretariat, Shimla - 171 002, Email: cs-hp@nic.in
21. Chief Secretary, Government of Maharashtra, Main Building, Mantralaya, 6th floor, Madam Cama Road, Mumbai – 400 032, Email: chiefsecretary@maharashtra.gov.in

INDEX

22. Chief Secretary, Government of Meghalaya, Main Secretariat Building, Rilang Building Meghalaya Secretariat, Shillong - 793 001. Email: cso-meg@nic.in
23. Chief Secretary, Government of Nagaland, Civil Secretariat, Kohima – 797 004, Email: csngl@nic.in
24. Chief Secretary, Government of Sikkim, New Secretariat, Gangtok – 737 101, Email: cs-skm@nic.in
25. Chief Secretary, Government of Tamil Nadu, Secretariat, Chennai – 600 009, Email: cs@tn.gov.in
26. Chief Secretary, Government of Tripura, New Secretariat Complex, Secretariat Agartala, West Tripura – 799 010, Email: cs-tripura@nic.in
27. Chief Secretary, Government of Mizoram, New Secretariat Complex, Aizwal – 796 001, Email: cs-mizoram@nic.in
28. Chief Secretary, Government of Rajasthan, Main Building, Secretariat, Jaipur – 302 005, Email: csraj@rajasthan.gov.in

INDEX

Annexure I

[On non-judicial stamp paper of value as applicable]

AGREEMENT

This Agreement (hereinafter referred to as "Supplementary Agreement" or "Agreement to supplement AUA Agreement") is entered into by and between:

THE UNIQUE IDENTIFICATION AUTHORITY OF INDIA, a statutory authority established under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ["Act"], having its Head Office at New Delhi (current address: Aadhaar Building, Bangla Sahib Road, Gole Market, New Delhi – 110 001) (hereinafter referred to as "UIDAI" or "Authority" or "First Party", which expression shall, unless the context otherwise requires, include its authorized representatives and successors), of the First Part;

AND

_____[1] (hereinafter referred to as "Second Party"), acting through its authorised representative, _____[2], which expression shall, unless the context otherwise requires, include its authorised representatives and such successors of the Second Part.

The said parties are collectively referred to hereinafter as 'Parties' and individually as 'Party'.

WHEREAS the Second Party is a requesting entity appointed by the First Party as an _____[3] for the purpose of use of the Aadhaar Authentication facilities of the First Party;

AND WHEREAS the Second Party has, under the Aadhaar (Authentication and Offline Verification) Regulations, 2021, entered into an AUA agreement with the First Party for the use of the Aadhaar Authentication facilities of the First Party ("AUA Agreement") and is desirous of entering into this Supplementary Agreement that sets out the terms and conditions for use of the said facilities for performance of authentication with update of status of Aadhaar numbers previously submitted, in the event of such an Aadhaar number being subsequently omitted or deactivated Aadhaar number being re-activated;

AND WHEREAS the Second Party understands and acknowledges that the terms and conditions set out herein are in addition to and not in derogation of the powers of the First Party and the obligations and liabilities of requesting entities under the Act, the regulations made thereunder and the obligations and liabilities of the Second Party under the AUA Agreement;

NOW THEREFORE, this Supplementary Agreement witnesses as under:

1. The Supplementary Agreement shall come into force from the date it is signed and shall remain in effect until it is replaced by another Supplementary Agreement or is terminated in writing with the mutual consent of both Parties.

[1] Name of the Second Party
[2] Full name and full designation
[3] <Authentication User Agency (AUA)>or<Authentication User Agency (AUA) and an e-KYC User Agency (KUA)> (whichever is applicable)

INDEX

1.1 The Parties may, by mutual agreement, amend the terms and conditions of the Supplementary Agreement.

1.2 The Supplementary Agreement may be terminated by either Party by giving notice, in writing, to the other Party on this behalf.

1.3 The Second Party acknowledges that it shall be obligated to pay such fees, including applicable taxes, as the First Party may specify in the Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023 made by it in exercise of its powers under sub-sections (1) and (2) of section 54 read with sub-section (1) of section 8 of the Act, and on such terms as to payment thereof as the First Party may stipulate from time to time.

1.4 The First Party shall provide the Second Party the use of Aadhaar Authentication facilities at its sole discretion and reserves the right to add to, to revise or to suspend in whole or in part such provision at any time, without prior notice, at its sole discretion, in the interest of protection of the information of Aadhaar number holders or the Aadhaar ecosystem, or in public interest, or in public interest, or in any of the interests referred to as per the terms of the AUA Agreement.

2. Principles

2.1 This Supplementary Agreement sets forth a statement of intent of the Parties to this Supplementary Agreement to establish a framework—

(a) to facilitate the use of Authentication facility including any subsequent appropriate response returned by the First Party regarding the status as to whether any Aadhaar number previously submitted has been subsequently omitted or deactivated or re-activated in the event of any omission or deactivation of such Aadhaar number or re-activation of such a deactivated Aadhaar number; and

(b) to facilitate sharing of Aadhaar-seeded information of deceased individuals with the First Party by the Second Party.

2.2 The Parties to Supplementary Agreement shall use their best endeavors to meet the terms of this Supplementary Agreement.

3. Safeguards and Confidentiality

3.1 The Parties to Supplementary Agreement undertake to implement and maintain security procedures and measures in order to ensure the protection against the risks of unauthorised access, alteration, delay, destruction or loss of information regarding status update.

3.2 The Parties to Supplementary Agreement agree that the status update response provided shall be subject to the confidentiality rules and other safeguards to ensure the necessary level of confidentiality.

3.3 The Second Party further agrees that any Sub-Authentication User Agency (Sub-AUA) and Sub-e-KYC User Agency (Sub-KUA) is desirous to avail facility for performance of authentication with update of status of Aadhaar numbers previously submitted, in the event of such an Aadhaar number being subsequently omitted or deactivated Aadhaar number being re-activated, shall enter into a separate agreement with the Second Party, in the form and substance of the template provided under **Annexure-A** of this agreement.

3.4 The Second Party shall keep First Party duly informed of any such separate agreement executed with its Sub-AUA and Sub-KUA. Copies or summaries of such agreements, along with details of the Sub-AUA and Sub-KUA, shall be furnished to the First Party as and when executed, and the Second Party shall maintain updated records for inspection or audit by the First Party.

4. Consultation

4.1 The Parties may consult one another informally at any time about a new request or proposed request.

4.2 The Parties may consult and revise terms of the Supplementary Agreement in the event of a substantial change in the laws, practices, market or business conditions affecting the operation of this Supplementary Agreement.

4.3 Any dispute arising out of the interpretation and implementation or application of this Supplementary Agreement shall be settled amicably by consultation between the Parties.

5. Nodal Officer

The Parties to Supplementary Agreement shall appoint Nodal Officer and alternate Nodal Officer with the following responsibilities to—

(a) act as point of contact for coordinating in respect of anything relating to this Supplementary Agreement;
(b) accord due priority and resources for timely completion of tasks related to this Supplementary Agreement;
(c) establish a mechanism for resolving status update response quality issue, if any, within a reasonable time-frame; and
(d) establish a mechanism for periodic review of Supplementary Agreement.

IN WITNESS WHEREOF, the Parties hereto have signed this Supplementary Agreement to confirm their approval of, an agreement with, its contents.

Signed at <<PLACE>> on <<DATE>>

FOR AND ON BEHALF OF UIDAI:	FOR AND ON BEHALF OF SECOND PARTY:
Signature:	Signature:
Name:	Name:
Designation:	Designation:
Date:	Date:
IN THE PRESENCE OF:	IN THE PRESENCE OF:

Signature:	Signature:
Name:	Name:
Designation:	Designation:
Date:	Date:

Annexure A

[On non-judicial stamp paper of value as applicable]

AGREEMENT

This Agreement (hereinafter referred to as "Supplementary Agreement" or "Agreement to Joint Undertaking") is entered into by and between:

_____[1] (hereinafter referred to as "First Party"), acting through its authorised representative, _____[2], which expression shall, unless the context otherwise requires, include its authorised representatives and such successors of the First Part.

AND

_____[3] (hereinafter referred to as "Second Party"), appointed by the First Party as its Sub-Authentication User Agency (Sub-AUA) and Sub-e-KYC User Agency (Sub-KUA) to avail its Aadhaar authentication services, acting through its authorised representative, _____[4], which expression shall, unless the context otherwise requires, include its authorised representative and such successors of the Second Part.

The said parties are collectively referred to hereinafter as 'Parties' and individually as 'Party'.

WHEREAS the First Party is a requesting entity appointed by UIDAI as an _____[5] for the purpose of use of the Aadhaar Authentication facilities of UIDAI and has further entered into a supplementary agreement under sub-regulation (3A) of regulation 9 of the Aadhaar (Authentication and Offline Verification) Regulations, 2021 for use of said facilities for performance of authentication with update of status of Aadhaar numbers previously submitted, in the event of such an Aadhaar number being subsequently omitted or deactivated Aadhaar being re-activated:

AND WHEREAS the Second Party is appointed as Sub-AUA and Sub-KUA to the First Party through joint undertaking dated _____[6] for the purpose of use of Aadhaar Authentication facilities of UIDAI through First Party:

AND WHEREAS the Second Party is desirous to enter into this supplementary agreement that sets out the terms and conditions for use of said facilities for performance of authentication with update of status of Aadhaar numbers previously submitted, in the event of such an Aadhaar number being subsequently omitted or deactivated Aadhaar being re-activated:

AND WHEREAS the Parties understands and acknowledges that the terms and conditions set out herein are in addition to and not in derogation of the powers of UIDAI and the Parties shall be jointly and severally liable for non-compliance of the provisions of the Aadhaar Act and its Regulations, specifically the Aadhaar (Authentication and Offline Verification) Regulations 2021,and directions, information security policies, processes, standards, specifications, guidelines and protocols issued by the Authority from time to time:

---

[1] Name of the First Party
[2] Full name and full designation
[3] Name of the Second Party
[4] Full name and full designation
[5] <Authentication User Agency (AUA)>or<Authentication User Agency (AUA) and an e-KYC User Agency (KUA)> (whichever is applicable)
[6] Date of execution of joint undertaking

NOW THEREFORE, this Supplementary Agreement witnesses as under:

1. The Supplementary Agreement shall come into force from the date it is signed and shall remain in effect until it is replaced by another supplementary agreement or is terminated in writing with the mutual consent of the Parties or the Joint undertaking between the Parties is revoked.

1.1 The Parties understands and acknowledges that UIDAI shall provide the AUA the use of Aadhaar Authentication facilities at its sole discretion and reserves the right to add to, to revise or to suspend in whole or in part such provision at any time, without prior notice, in the interest of the of protection of the information of Aadhaar number holders or the Aadhaar ecosystem, or in public interest or in any of the interests referred to as per the terms of the AUA Agreement.

1.2 The Supplementary Agreement may be terminated by either Party by giving notice, in writing, to the other Party on this behalf.

1.3 The Parties acknowledges that it shall be obligated to pay such fees, including applicable taxes, as UIDAI may specify in the Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023 made by it in exercise of its powers under sub-sections (1) and (2) of section 54 read with sub-section (1) of section 8 of the Act, and on such terms as to payment thereof as UIDAI may stipulate from time to time.

1.4 The Second Party shall use the update of status of Aadhaar numbers solely through the First Party.

1.5 The First Party shall remain fully responsible to UIDAI for all the acts of the Second Party.

2. **Principles**

2.1 This Supplementary Agreement sets forth the statement of intent of the Parties to thus Supplementary Agreement to establish a framework to facilitate the Second Party the use of Authentication facility, through the First Party, including any subsequent appropriate response returned by UIDAI regarding the status as to whether any Aadhaar number previously submitted has been subsequently omitted or deactivated or re-activated in the event of any omission or deactivation of such Aadhaar number or re-activation of such a deactivated Aadhaar number.

2.2 The Parties to Supplementary Agreement shall use their best endeavours to meet the terms of this Supplementary Agreement.

3. **Safeguards and Confidentiality**

3.1 The Parties to Supplementary Agreement undertake to implement and maintain security procedures and measures in order to ensure the protection against the risks of unauthorised access, alteration, delay, destruction or loss of information regarding status update.

3.2 The Parties to Supplementary Agreement agree that the status update response provided shall be subject to the confidentiality rules and other safeguards to ensure necessary level of confidentiality.

4. **Consultation**

4.1 The First Party shall keep UIDAI informed of details of the Second Party along with copy of this supplementary agreement as and when executed and shall maintain updated records for inspection or audit by UIDAI.

4.2 Any dispute arising out of the interpretation and implementation or application of this Supplementary Agreement shall be settled amicably by consultation between the parties.

5. **Nodal Officer**

The Parties to Supplementary Agreement shall appoint Nodal Officer and alternate Nodal Officer with the following responsibilities to—

(a) act as point of contact for coordinating in respect of anything relating to this Supplementary Agreement;

(b) accord due priority and resources for timely completion of tasks related to this Supplementary Agreement;

(c) establish a mechanism for resolving status update response quality issue, if any, within a reasonable time-frame; and

(d) establish a mechanism for periodic review of Supplementary Agreement.

IN WITNESS WHEREOF, the Parties hereto have signed this Supplementary Agreement to confirm their approval of, an agreement with, its contents.

Signed at _____[1] on _____[2]

For and on behalf of First Party:	**For and on behalf of Second Party**
Signature:	Signature:
Name: Designation:	Name: Designation:
Date:	Date:
In the presence of:	**In the presence of:**
Signature:	Signature:
Name:	Name:
Designation:	Designation:
Date:	Date:

[1] <<Place>>
[2] <<Date>>

Annexure-IV

F. No. HQ-13079/15/2024-AUTH-II HQ/15213
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road
Behind Kali Mandir, Gole Market
New Delhi – 110 001
Dated 20 December 2024

Circular 3 of 2024

Subject: Guidelines on requiring Aadhaar number for receipt of subsidy, benefit or service under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

Please refer to the following Circulars of UIDAI, a copy each of which is annexed herewith for ready reference, namely:—

(a) Circular no. 23011/Gen/2014/Legal-UIDAI, dated 15.9.2016, on the subject "Notification for use of Aadhaar under Section 7 of Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act") for targeted delivery of financial and other subsidies, benefits and services funded from Consolidated Fund of India" **(Annexure-II)**; and

(b) Circular no. 1-1/2019-UIDAI (DBT), dated 25.11.2019, on the subject "Guidelines on use of Aadhaar under section 7 of the Aadhaar Act 2016 (as amended by the Aadhaar and Other Laws (Amendment) Act, 2019) by the State Governments for the schemes funded out of Consolidated Fund of State" **(Annexure-III)**.

2. On the basis of a review of the existing templates to take into account further evolution of the policies, procedures and systems for the issuing Aadhaar number and performing authentication thereof and with a view to offering greater clarity, in partial modification of the aforesaid Circulars, a revised template that may be used for the issuance of a notification pursuant to requirement of Aadhaar number under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 is attached herewith **(Annexure-I)**.

3. The revised template, among other things, makes clear the following:

(a) The officer designated by the Ministry or Department concerned shall check the documents or information presented by an individual who is desirous of availing of subsidy, benefit or service but to whom Aadhaar number has not been assigned in the manner specified in clause (4) of paragraph 1 of the template. Accordingly, *the Enrolment ID (EID) contained in the enrolment acknowledgement must be used to check the status of the enrolment request by submitting the EID on myAadhaar portal (https://myaadhaar.uidai.gov.in/portal) to confirm that the EID is valid and that the enrolment request does not stand rejected.*

(b) Where the authentication of the Aadhaar number of the beneficiary done through any of the biometric-based modes of authentication (namely, facial image,

INDEX

F. no.: HQ-13031/1/2022-AUTH-I HQ (Comp No. 13927)/3028
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road,
Gole Market, New Delhi – 110001
Dated: 04.11.2025

Circular No. 14 of 2025

Subject: Revised guidelines for hosting Hardware Security Module (HSM), Aadhaar Data Vault (ADV) and authentication application on premises and cloud infrastructure for Aadhaar Authentication Ecosystem.

This circular superseded the UIDAI circular no. 11020/205/2017-UIDAI (Auth-I) dated 25.07.2017, Circular 8 of 2025 dated 18.07.2025 on ADV implementation and shall be read in continuation of UIDAI circular No. 11020/204/2017-UIDAI (Auth-I) dated 22.06.2017 on HSM implementation.

2. All requesting entities (REs) are directed to mandatorily store Aadhaar numbers and any connected Aadhaar data (e.g. eKYC XML containing Aadhaar number and demographic data) on a separate secure database/vault/system. This system will be termed as "Aadhaar Data Vault" and will be the only place where Aadhaar Number and any connected data will be stored.

3. Entities are allowed to securely store UID Tokens or any relevant demographic data and/or photo of the Aadhaar Number Holder in their local database in encrypted manner with Cryptographic Algorithms (Symmetric/Asymmetric Encryption) as long as Aadhaar Number is not stored in those systems.

4. Requesting entities are strictly prohibited for storing Aadhaar number or related data from the requested inputs by the Aadhaar number holder in Authentication/eKYC request.

5. The ADV implemented by a requesting entity must be hosted on either of the following

(a) on-premises (within the secure premises of the requesting entity/technical service provider);
(b) on a Government Community Cloud (GCC) platform-based cloud, empaneled by MeitY (Ministry of Electronics and IT), Govt. of India, list of those Cloud Service Providers (CSP) are available at *https://www.ambud.meity.gov.in* ; and
(c) ADV as-a-service provided by UIDAI Requesting Entities.

6. In case of GCC platform-based cloud implementation or ADV as-a-service based implementation, the annual System and Organization Controls (SOC 2) Type II audit of the cloud infrastructure must be conducted by Cert-IN empanelled auditor agency authorized for cloud security audit and this has to be ensured by the concerned requesting entity.

7. Requesting entities must ensure the following for ADV implementation:

(a) The GCC provider or the entity providing ADV as-a-service must be compliant with UIDAI security and privacy standards and ensure complete logical segregation of ADV for each requesting entity.

(b) 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.

(c) 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 ADV.

(d) The data in ADV shall be stored in a single logical instance for each entity with the corresponding reference key which must be generated and used. Access to Aadhaar Data Vault shall be made secure and accessed through internal systems only.

(e) Aadhaar data must be stored in an encrypted format using strong algorithms like AES-256 (*or* higher) *or* as specified in latest Authentication API.

(f) High Availability and Disaster Recovery (HA/DR) shall be in place for the ADV with the same level of security along with dual redundant connectivity to the ASAs. It should have sufficient bandwidth based on respective anticipated transaction volume.

(g) 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.

(h) Only trusted communication channels and secure APIs/microservices, shall be used for data access in vault. All access must be routed through authenticated applications with appropriate user authentication, authorization and logging mechanisms.

(i) Robust access control, monitoring and alerting systems must be implemented to detect and prevent unauthorized access to ADV. Ensure strict implementation of Identity and Access Management (IAM) so that only authorized personnel and systems can access the vault. All access must be logged and monitored.

(j) 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.

(k) 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. Hashing of Aadhaar numbers is not allowed to be used as Reference keys.

8. Requesting entities and Authentication Service Agencies (ASA) must mandatorily implement the Hardware Security Module (HSM) for cryptographic operations (such as signing of authentication request, encryption/decryption of ADV data, decryption of eKYC response data or any other operation as mandated by UIDAI time to time). The HSM must be hosted as either of the following:

   (a) on-premises (within the secure premises of the requesting entity).
   (b) on a Government Community Cloud (GCC) platform-based cloud, empaneled by MeitY (Ministry of Electronics and IT), Govt. of India.
   (c) as HSM services provided along with ADV as-a-service by any entity.

9. Requesting entities and ASAs must ensure the following for HSM implementation:

   (a) It must be FIPS 140-2 Level 3 certified or higher.
   (b) It must be logically isolated for each requesting entity/ASA independently.
   (c) It must support:
      (i) Key Generation
      (ii) Secure Key Storage
      (iii) Multifactor, Multirole Access Control and Audit Logging

10. Aadhaar authentication applications or any module handling authentication data shall only be hosted on-premises (within the secure premises of the requesting entity) *or* on a GCC platform-based cloud, empaneled by MeitY, Govt. of India.

11. Requesting Entities and ASAs are advised to refer the latest list of MeitY-empaneled GCC services provider, available at: *https://www.ambud.meity.gov.in*. This list is maintained and updated by MeitY.

12. Additional information and clarifications can be found in the Frequently Asked Questions (FAQ) section accessible through below mentioned link
https://uidai.gov.in//images/FAQs_Aadhaar_Data_Vault_03112025_v10.pdf

13. This issues with the approval of competent authority.

(Pratik Choudhary)
Deputy Director
Tel.: 011-23478608
Email: dd1.auth-hq@uidai.net.in

To:

1. All requesting entities and Authentication Service Agencies in Aadhaar Authentication Ecosystem

Copy, for information, to:

1. Secretaries in charge of Ministries and Departments in Government of India (as per list attached)
2. Chief Secretaries of State Governments (as per list attached)
3. Chief Secretary, Government of Jammu and Kashmir / National Capital Territory of Delhi / Puducherry / Andaman and Nicobar Islands Administration
4. Advisor to Administrator, Chandigarh Administration
5. Advisor to Lieutenant Governor, Ladakh Administration
6. Administrator, Dadra and Nagar Haveli and Daman and Diu Administration / Lakshadweep Administration
7. Technology Centre, UIDAI, Bangalore
8. Regional Offices, UIDAI

List of addressee Secretaries

1. Secretary, Department for Promotion of Industry and Internal Trade, Vanijya Bhawan, New Delhi – 110 011
2. Secretary, Department of Administrative Reforms and Public Grievances, 513, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001
3. Secretary, Department of Agricultural Research and Education, First floor, Krishi Bhawan, New Delhi – 110 001
4. Secretary, Department of Agriculture and Farmers Welfare, Krishi Bhavan, Dr Rajendra Prasad Road, New Delhi – 110 001
5. Secretary, Department of Animal Husbandry and Dairying, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
6. Secretary, Department of Atomic Energy, E Block, Raisina Hill, New Delhi – 110 011
7. Secretary, Department of Biotechnology, 7th floor, Block-2, CGO Complex, Lodhi Road, New Delhi – 110 003
8. Secretary, Department of Chemicals and Petrochemicals, 236A, A Wing, 2nd floor, Shastri Bhawan, New Delhi – 110 001
9. Secretary, Department of Commerce, Udyog Bhawan, New Delhi – 110 011
10. Secretary, Department of Consumer Affairs, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
11. Secretary, Department of Drinking Water and Sanitation, C Wing, 4th floor, Paryavaran Bhawan, CGO Complex, Lodhi Road, New Delhi – 110 003
12. Secretary, Department of Economic Affairs, North Block, New Delhi - 110 001
13. Secretary, Department of Empowerment of Persons with Disabilities, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
14. Secretary, Department of Ex-servicemen Welfare, South Block, New Delhi – 110 011
15. Secretary, Department of Fertilizers, A Wing, Shastri Bhawan, New Delhi – 110 001
16. Secretary, Department of Financial Services, 3rd floor, Jeevan Deep Building, Parliament Street, New Delhi – 110 001
17. Secretary, Department of Fisheries, Krishi Bhawan, New Delhi – 110 001
18. Secretary, Department of Food and Public Distribution, H Wing, Krishi Bhawan, New Delhi – 110 001
19. Secretary, Department of Health and Family Welfare, A Wing, Nirman Bhavan, New Delhi – 110 011
20. Secretary, Department of Health Research, 1, Red Cross Road, Gokul Nagar, New Delhi – 110 001
21. Secretary, Department of Higher Education, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
22. Secretary, Department of Investment and Public Asset Management, 4th floor, Block No. 11 CGO Complex, Lodhi Road New Delhi – 110 003
23. Secretary, Department of Land Resources, NBO Building, G Wing, Nirman Bhawan, Dr Maulana Azad Road, New Delhi – 110 011
24. Secretary, Department of Official Language, NDCC-II Bhawan, A Wing, 3rd floor, Jai Singh Marg, New Delhi – 110 001

25. Secretary, Department of Pension and Pensioners' Welfare, 514, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001
26. Secretary, Department of Personnel and Training, North Block, New Delhi – 110 001
27. Secretary, Department of Pharmaceuticals, A Wing, Shastri Bhawan, New Delhi – 110 001
28. Secretary, Department of Posts, Dak Bhawan, Patel Chowk, New Delhi – 110 001
29. Secretary, Department of Public Enterprises, Block-14, CGO Complex, Lodhi Road, New Delhi – 110 003
30. Secretary, Department of Rural Development, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
31. Secretary, Department of School Education and Literacy, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
32. Secretary, Department of Science and Technology, Technology Bhawan, New Mehrauli Road, New Delhi – 110 016
33. Secretary, Department of Scientific and Industrial Research, Technology Bhawan, New Mehrauli Road, New Delhi – 110 016
34. Secretary, Department of Social Justice and Empowerment, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
35. Secretary, Department of Space, Antariksh Bhavan, New BEL Road, Bangalore – 560 231
36. Secretary, Department of Sports, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
37. Secretary, Department of Telecommunications, Sanchar Bhawan, 20, Ashoka Road, New Delhi – 110 001
38. Secretary, Department of Water Resources, River Development and Ganga Rejuvenation, Shram Shakti Bhawan, Rafi Marg, New Delhi – 110 001
39. Secretary, Department of Youth Affairs, Room No. 1, C Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
40. Secretary, Legislative Department, A Wing, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
41. Secretary, Ministry of AYUSH, Ayush Bhawan, B Block, GPO Complex, Barapullah Road, INA Colony, New Delhi – 110 023
42. Secretary, Ministry of Civil Aviation, Rajiv Gandhi Bhawan, Block B, Jor Bagh, Safdarjung Airport Area, New Delhi – 110 003
43. Secretary, Ministry of Coal, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
44. Secretary, Ministry of Cooperation, 2nd floor, Atal Akshya Urja Bhawan, Pragati Vihar, New Delhi – 110 003
45. Secretary, Ministry of Corporate Affairs, A Wing, Shastri Bhawan, Rajendra Prasad Road, New Delhi – 110 001
46. Secretary, Ministry of Culture, Shastri Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
47. Secretary, Ministry of Development of North Eastern Region, Vigyan Bhawan Annexe, Maulana Azad Road, New Delhi – 110 011
48. Secretary, Ministry of Earth Sciences, Mahasagar Bhawan, Block - 12, C.G.O Complex, Lodhi Road, New Delhi – 110 003

49. Secretary, Ministry of Electronics and Information Technology, 6, CGO Complex, Lodhi Road, New Delhi – 110 003
50. Secretary, Ministry of Environment, Forest and Climate Change, Indira Paryavaran Bhawan, Jor Bagh Road, New Delhi – 110 003
51. Secretary, Ministry of Food Processing Industries, Panchsheel Bhawan, August Kranti Marg, New Delhi – 110 049
52. Secretary, Ministry of Heavy Industries, Udyog Bhawan, New Delhi – 110 001
53. Home Secretary, Ministry of Home Affairs, North Block, New Delhi – 110 001
54. Secretary, Ministry of Housing and Urban Affairs, Nirman Bhawan, C Wing, Dr Maulana Azad Road, New Delhi – 110 011
55. Secretary, Ministry of Information and Broadcasting, Dr Rajendra Prasad Road, Shastri Bhawan, New Delhi – 110 001
56. Secretary, Ministry of Labour and Employment, Shram Shakti Bhawan, Rafi Marg, New Delhi – 110 001
57. Secretary, Ministry of Micro, Small and Medium Enterprises, Udyog Bhawan, Rafi Marg, New Delhi – 110 011
58. Secretary, Ministry of Mines, A Wing, 3rd floor, Shastri Bhawan, New Delhi – 110 001
59. Secretary, Ministry of Minority Affairs, 11th floor, Paryavaran Bhawan, CGO Complex, Lodhi Road, New Delhi – 110 003
60. Secretary, Ministry of New and Renewable Energy, Block no. 14, CGO Complex, Lodhi Road, New Delhi – 110 003
61. Secretary, Ministry of Panchayati Raj, Krishi Bhawan, Dr Rajendra Prasad Road, New Delhi – 110 001
62. Secretary, Ministry of Parliamentary Affairs, Parliament House, Sansad Marg, New Delhi – 110 001
63. Secretary, Ministry of Petroleum and Natural Gas, Shastri Bhawan, Rajendra Prasad Road, New Delhi – 110 001
64. Secretary, Ministry of Ports,Shipping and Waterways, Transport Bhavan, 1, Parliament Street, New Delhi – 110 001
65. Secretary, Ministry of Power, 2nd floor, Shram Shakti Bhawan, New Delhi – 110 001
66. Secretary, Ministry of Road Transport and Highways, Transport Bhavan, 1, Parliament Street, New Delhi – 110 001
67. Secretary, Ministry of Skill Development and Entrepreneurship, 2nd floor, Shivaji Stadium Annexe, Shaheed Bhagat Singh Marg, New Delhi – 110 001
68. Secretary, Ministry of Statistics and Programme Implementation, 418, Sardar Patel Bhawan, Sansad Marg, New Delhi – 110 001
69. Secretary, Ministry of Steel, Udyog Bhawan, New Delhi – 110 001
70. Secretary, Ministry of Textiles, Udyog Bhawan, New Delhi – 110 001
71. Secretary, Ministry of Tourism, Transport Bhavan, 1, Parliament Street, New Delhi – 110 001
72. Secretary, Ministry of Tribal Affairs, B Wing, Shastri Bhawan, New Delhi – 110 001
73. Secretary, Ministry of Women and Child Development, Shastri Bhawan, A Wing, Dr Rajendra Prasad Road, New Delhi – 110 001

List of Chief Secretaries to State Governments

1. Chief Secretary, Government of Kerala, Secretariat, Thiruvananthapuram – 695 001, Email: chiefsecy@kerala.gov.in
2. Chief Secretary, Government of Jharkhand, 1st floor, Project Bhawan, Mantralaya, Dhurwa, Ranchi – 834 004, Email: cs-jharkhand@nic.in
3. Chief Secretary, Government of West Bengal, Nabanna, 13th floor, 325, Sarat Chatterjee Road, Shibpur, Howrah - 711 102, Email: cs-westbengal@nic.in
4. Chief Secretary, Government of Odisha, Odisha State Secretariat, Sachivalaya Marg, Unit-2, Bhubaneswar, Email: csori@nic.in
5. Chief Secretary, Government of Manipur, Babupara, Imphal West, Manipur – 795 001, Email: cs-manipur@nic.in
6. Chief Secretary, Government of Uttar Pradesh, 1st floor, Room no. 110, Lal Bahadur Shastri Bhawan, Lucknow – 226 001, Email: csup@nic.in
7. Chief Secretary, Government of Chhattisgarh, Mantralaya, Naya Raipur, Chhattisgarh - 492 002, Email: csoffice.cg@gov.in
8. Chief Secretary, Government of Karnataka, Room no. 320, 3rd floor, Vidhana Soudha, Bengaluru – 560 001, Email: cs@karnataka.gov.in
9. Chief Secretary, Government of Uttarakhand, 4 Subhash Road, Uttarakhand Secretariat, Dehradun - 248 001, Email: cs-uttarakhand@nic.in
10. Chief Secretary, Government of Madhya Pradesh, 4th floor, Mantralaya, Vallabh Bhavan-I, Bhopal – 462 004, Email: cs@mp.nic.in
11. Chief Secretary, Government of Punjab, 6th floor, Punjab Civil Secretariat-1, Sector 1, Chandigarh – 160 001, Email: cs@punjab.gov.in
12. Chief Secretary, Government of Telangana, Telangana Secretariat, 5th floor, Burgula Rama Krishna Rao Bhavan NH 44, Hill Fort, Adarsh Nagar, Hyderabad - 500 063, Email: cs@telangana.gov.in
13. Chief Secretary, Government of Andhra Pradesh, 1st Block, 1st floor, Andhra Pradesh Secretariat Office, Velagapudi – 522 023, Email: cs@ap.gov.in
14. Chief Secretary, Government of Arunachal Pradesh, Block-II, 5th floor, Civil Secretariat, Itanagar – 791 111, Email: cs-arunachal@nic.in
15. Chief Secretary, Government of Assam, Assam Secretariat, CM Block, Second Floor Dispur, Guwahati - 781 006, Email: cs-assam@nic.in
16. Chief Secretary, Government of Bihar, Main Secretariat, Patna – 800 015, Email: cs-bihar@nic.in
17. Chief Secretary, Government of Goa, Secretariat, Porvroim, Bardez – 403 521, Email: cs-goa@nic.in
18. Chief Secretary, Government of Gujarat, 1st Block, 5th floor, Sachivalaya, Gandhinagar, Email: chiefsecretary@gujarat.gov.in
19. Chief Secretary, Government of Haryana, 47, 9th floor, Haryana Civil Secretariat, Sector-1, Chandigarh - 160 001, Email: cs@hry.nic.in
20. Chief Secretary, Government of Himachal Pradesh, Himachal Pradesh Secretariat, Shimla - 171 002, Email: cs-hp@nic.in
21. Chief Secretary, Government of Maharashtra, Main Building, Mantralaya, 6th floor, Madam Cama Road, Mumbai – 400 032, Email: chiefsecretary@maharashtra.gov.in

22. Chief Secretary, Government of Meghalaya, Main Secretariat Building, Rilang Building Meghalaya Secretariat, Shillong - 793 001, Email: cso-meg@nic.in
23. Chief Secretary, Government of Nagaland, Civil Secretariat, Kohima – 797 004, Email: csngl@nic.in
24. Chief Secretary, Government of Sikkim, New Secretariat, Gangtok – 737 101, Email: cs-skm@nic.in
25. Chief Secretary, Government of Tamil Nadu, Secretariat, Chennai – 600 009, Email: cs@tn.gov.in
26. Chief Secretary, Government of Tripura, New Secretariat Complex, Secretariat Agartala, West Tripura – 799 010, Email: cs-tripura@nic.in
27. Chief Secretary, Government of Mizoram, New Secretariat Complex, Aizwal – 796 001, Email: cs-mizoram@nic.in
28. Chief Secretary, Government of Rajasthan, Main Building, Secretariat, Jaipur – 302 005, Email: csraj@rajasthan.gov.in

HQ-13073/3/2023-AUTH-II HQ

I/50064/2025

F.No. HQ-13073/3/2023-AUTH-II HQ/E-12984/3324
Unique Identification Authority of India
(Authentication & Verification Division)

UIDAI Head Office, Bangla Sahib Road
Gole Market, New Delhi – 110 001
Dated: 8th December, 2025

Circular no. 15 of 2025

Subject: Revision of fees for performance of authentication transactions by requesting entities other than Telecom Service Providers.

Reference:

I. The Aadhaar (Payment of Fees for Performance of Authentication) Regulations, 2023 (as amended)
II. UIDAI Circular No. 1 of 2024 (HQ-13062/4/2021-Auth-II HQ/(E-3235)/8271 dated 16.01.2024.

In pursuance to regulation 3(3)(b) of Sr. no. I cited above, as per ratio proportion of Consumer Price Index General (Combined), the transaction charges stand revised upon completion of every period of twenty-four calendar months.

2. The revised transaction charges as per provisions of regulation 3(1)(a) and 3(1)(b) of Sr no. I cited above, shall be effective from 01.11.2025 and are as follows:

Authentication type	Category of requesting entity	Existing rate (₹) (inclusive of taxes) Up to 31.10.2025	Revised rate (₹) (inclusive of taxes) w.e.f. 1.11.2025
Yes/No	All (AUA, sub-AUA, KUA and sub-KUA)	0.60	0.60 (no change)
eKYC	KUA and sub-KUA other than Telecom Service Provider	(a) For successful authentication transaction: 3.40 (b) For failed authentication transaction: 0.60	(a) For successful authentication transaction: 3.60 (b) For failed authentication transaction: 0.60

3. This issues under approval of the Competent Authority.

Digitally signed by Arpit Agrawal
Date: 08-12-2025 13:09:49

(Arpit Agrawal)
Deputy Director
Tel: 011-23478641
Email: dd2.auth-hq@uidai.net.in

INDEX

F no. HQ-13062/3/2020-Auth-II HQ – Part(4)/Comp-20043

Unique Identification Authority of India

(Authentication and Verification Division)

UIDAI Head Office
Bangla Sahib Road, Gole Market
New Delhi – 110 001
Dated: 12th January 2026

Circular 1 of 2026

Subject: Implementation of Unique Identifiers for Aadhaar-based Authentication Transactions.

UIDAI has been approving use of Aadhaar authentication under provisions of sections 4 and 7 of the Aadhaar Act. For ease of implementation, certain government requesting entities have been implementing multiple distinct schemes and departments under single AUA/KUA or Sub-AUA/Sub-KUA code.

Performing Aadhaar authentication transactions by such requesting entities (RE) using single AUA/KUA or Sub-AUA/Sub-KUA code for multiple schemes/services or departments may lead to implementation challenges, which are as following –

a) Difficult to differentiate between transactions for various schemes and departments as they originate using same code;
b) Impedes auditing, fraud detection and prevention, and performance tracking for individual schemes;
c) Technical issue in one scheme can affect all others simultaneously, leading to a lack of service continuity and reliability;
d) Using a single Sub-AUA code for multiple schemes makes it difficult to pinpoint the source of a security or compliance violation; and
e) Lacks transparency for implementation of Aadhaar authentication for approved schemes.

2. In this connection, all Department/Ministry of Centre/State Government entities (*herein after referred as* "Government entity") which are REs in Aadhaar ecosystem are directed to implement the following as the case may be with immediate effect that is to enhance transparency, improving visibility, and streamlining the process of managing transactions:

a) **Unique Transaction Identifiers**: Government entity as RE shall implement a unique identifier within the transaction ID for each scheme/service/use-case of the department or organization conducting transactions using their allotted license and code. Also, respective requesting entity shall formally inform UIDAI with identifiers implemented for each scheme/service/use-case. The schema for implanting unique identifiers is enclosed at **Annexure-I**.

b) **LITE Code Implementation**: Government entity as RE with a one-time use case wherein transactions to be performed are less than one lakh in a year may implement a LITE code using facility and infrastructure of an AUA/KUA under intimation to UIDAI. In this context, UIDAI has issued circular No. 3 of 2023 *vide* letter no. HQ-13073/2/2023-Auth HQ/C-10768 and partial modification to circular No. 3 of 2023 dated 26.12.2024. Further, for implementation of LITE code SoP is enclosed as **Annexure-II**.

INDEX

3. Implementing unique identifiers by AUA/KUA/Sub-AUA/Sub-KUA will incur the following benefits-

a) Provides more insight for benefit analysis of schemes by scheme implementing entity;
b) Ensure schemes benefit being provided as per approval;
c) Provide the necessary administrative and technical segregation to ensure adequate supervision by scheme implementing entity;
d) Identifier will ensure transaction traceability for all approved schemes;
e) Will enhance data analysis on implemented schemes;
f) Improves reliability and traceability for the approved purpose; and
g) Internal security compliance in accordance with the Aadhaar Act, 2016 and its associated regulations.

4. In view of aforesaid, all requesting entities are requested to make technical enablement and provide details internal identifiers to UIDAI within 30 days from issuance of the circular to avoid any disruption in services.

5. Subsequently, UIDAI needs to be under intimation before implementing transaction identifier for any scheme/service/use-case, as per the format enclosed at **Annexure-III.**

6. This circular shall be applicable to Departments/Ministries of Centre/ State Government

7. This issues with the approval of competent authority.

Yours faithfully,

(Arpit Agrawal)
Deputy Director
Tel: 011-23478641
Email: dd2.auth-hq@uidai.net.in

To:

Departments/Ministries of Centre/State Government Entities

Copy to:

1. All Deputy Director General of Regional Offices, UIDAI
2. Technology Centre, UIDAI - Bengaluru

INDEX

F no. HQ-13062/3/2020-Auth-II HQ – Part(4)/Comp-20043 dated 12.1.2026

Annexure – I

Schema for implanting unique identifiers

All user agencies must embed an identifier as per the details/guidelines mentioned below:

Transaction Identifier Format: The transaction identifier should be up to five alphabetic characters, either the scheme name or its prominent initials.

Placement of Identifier: The identifier must be appended at the end of every transaction ID for the respective scheme.

Applicability: This format applies to both demographic (Yes/No) authentication and e-KYC use cases.

Examples:

a) Demographic Authentication (e.g. Pradhan Mantri Awas Yojana, PMAY)

Transaction ID: NIC7716453145432025-10-29T23:35:23**PMAY**

(Here, PMAY, identifies the Pradhan Mantri Awas Yojana scheme)

b) eKYC (e.g., Jeevan Pramaan Portal)

Transaction ID: UKC:46351901192025102923344 9**JPP**

(Here, JPP signifies the Jeevan Pramaan scheme)

F no. HQ-13062/3/2020-Auth-II HQ – Part(4)/Comp-20043 dated 12.1.2026

Annexure-II

SoP for allocation of "Less In Transaction Entity" (LITE Code), is as follows:

Reference:

1) UIDAI circular 3 of 2023 dated 31.3.2023.
2) Partial modification issued dated 26.12.2024 to UIDAI circular 3 of 2023 dated 31.3.2023.
3) UIDAI circular 4 of 2025 dated 18.3.2025.
4) UIDAI circular 13 of 2025 dated 3.11.2025.
5) UIDAI circular 14 of 2025 dated 3.11.2025.

a) The Government entity desirous of using Aadhaar authentication facility of UIDAI and claiming to perform transactions ≤ 1 lakh in a financial year (FY), shall approach its respective Authentication User Agency (AUA) and e-KYC User Agency (KUA) (*hereinafter referred as* AUA/KUA) and submits a formal request to get onboarded with LITE code.

b) Respective AUA/KUA shall submit a formal letter to UIDAI along with gazette notification, issued as per the guidelines issued by UIDAI under relevant provisions of the Aadhaar Act, 2016.

c) Based on the recommendation received from the respective AUA/KUA, LITE code shall be allocated by UIDAI to Entity. In addition, AUA/KUA cannot onboard any Government Entity independently without intimating UIDAI.

d) AUA/KUA shall ensure secure storage of logs of transactions performed by its respective Government entity onboarded on LITE Code.

e) AUA/KUA to ensure that all its Government entity onboarded with LITE Code complies with the provisions of the Aadhaar Act, 2016 and its associated regulations, directions, processes, standards, guidelines, notifications, specifications and protocols of the Authority.

f) Existing Sub-AUA/Sub-KUA performing transactions i.e. ≤ 1 lakh in a financial year (FY) can apply to onboard on LITE Code as per the procedure mentioned above.

g) No audit shall be applicable to Government entity onboarded using LITE Code, *subject to utilizing infrastructure of their respective AUA/KUA*. However, in case entity onboarded using LITE code decided to keep the Aadhaar authentication data itself, compliance of UIDAI's circular 14 of 2025 dated 4.11.2025 is to be ensured by the respective entity.

h) No license fee will be applicable to Government entity onboarded on LITE Code.

i) In case transactions of any Government entity onboarded on LITE Code exceeds the limit of defined number of transactions within the stipulated financial year (FY), respective entity shall be charged with the license fees of Sub-AUA/Sub-KUA along with the penalty of @1.5% per month and part thereof since date of onboarding on LITE Code.

F no. HQ-13062/3/2020-Auth-II HQ – Part(4)/Comp-20043 dated 12.1.2026

Annexure-III

Format for sharing of details of Unique Transaction Identifiers implemented by AUA/KUA/Sub-AUA/Sub-KUA:

S. No.	Name of the Entity	Name of the Scheme/Service/Use-case	Unique Transaction Identifier Implemented

****

File No. HQ- 13028/1/2021-AUTH-I -HQ-Part (1)

Unique Identification Authority of India

(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road

Gole Market, New Delhi - 110 001

Dated: 03rd March 2026

Circular no 2 of 2026

Subject: Aadhaar face authentication onboarding audit checklist version 2.0 for requesting entities.

Ref no:

a) UIDAI letter no. 13028/1/2021/UIDAI (Auth-I) dated 03.06.2022
b) UIDAI letter no. 13083/6/2021-AUTH-I HQ (E-3605)/6754, dated 11.07.2023
c) UIDAI letter no. 13028/1/2021/AUTH-I-HQ-Part (1) dated 22.01.2025

This circular superseded the UIDAI letter cited at (c) and shall be read in continuation of the UIDAI letter cited at (a) & (b).

2. The face authentication onboarding audit checklist for requesting entities has been revised with immediate effect. Revised audit checklist having version 2.0 is enclosed as Annexure A.

3. This issues with approval of competent authority.

Yours faithfully,

(Pratik Choudhary)
Dy. Director
Tel.: 011-23478608
Email: dd1.auth-hq@uidai.net.in

To:

All requesting entities in Aadhaar authentication ecosystem

Copy to:-

1. All DDG UIDAI Regional offices
2. DDG Technology Centre, Bangalore

INDEX

Annexure A

Aadhaar Face Authentication onboarding Audit checklist version 2.0 for certifying compliance with controls that the entity (AUA/KUA/Sub-AUA/Sub-KUA) are required to have in place [issued in March 2026]

Control no.	Domain	Control description	Compliance status	Auditor's observations	Management comments (to be provided by RE)
A	**Governance**				
1	Restriction on display of Full Aadhaar Number	Application should display masked Aadhaar number only			
2	Log data storage and security	Log retention and use of secure methods such as digital signatures, cryptographic hashes or write once storage to ensure integrity of log data.			
B	**Source Code Review Report**				
3	Jailbreak and root detection	Control to detect and block access from jailbroken or rooted devices.			
4	Resiliency against attacks	Check whether algorithms are optimized for performance (SSL pinning etc) and resilience against potential attacks.			
5	Reverse engineering	Use obfuscation tool(s), to detect and prevent debugging attempts.			
6	Restriction on designing/compiling malicious code	Entity personnel should not intentionally write, generate, compile, copy or attempt to introduce any computer code designed to damage or otherwise hinder performance or access to Aadhaar information.			

Control no.	Domain	Control description	Compliance status	Auditor's observations	Management comments (to be provided by RE)
7	Hardcoding of security keys	Verify passwords, tokens, security keys and licenses are not hardcoded in application code.			
8	Rate Limiting	Check for Rate Limiting upto 2 transactions/min			
9	Cryptographic protocol configuration	Verify configuration of cryptographic standard algorithms as per NIST FIPS 140-2, such as RSA-2048(asymmetric encryption), AES-256 bits(for symmetric encryption) & SHA 2/3 (for hashing) or any other cryptographic algorithm as mandated by UIDAI			
10	Security header implementation	Check for utilization of security headers as HSTS (HTTP Strict Transport Security) and X-Content-Type-Options.			
11	Input length check	Test for proper input validation check in relevant input fields.			
12	Code and log review	Review code for any signs of improper input validation or exploitation attempts.			
13	Code related attack execution	Test for proper type checking to prevent the execution of arbitrary code and other code-related attacks.			
14	Secure application development	Application must be free from OWASP mobile security vulnerability			

Control no.	Domain	Control description	Compliance status	Auditor's observations	Management comments (to be provided by RE)
C	**VAPT (Vulnerability Assessment and Penetration Testing)**				
15	Multiple Systems Access	Ensure that one concurrent session per user is allowed at a time i.e., parallel login sessions are not allowed.			
16	Authorization check for sensitive data	Check app's API endpoints to ensure proper authorization checks before accessing sensitive data or privileged operations.			
17	User input encoding	Verify that the application is properly encoding user-supplied input to prevent XSS (Cross-site Scripting) and SQL injection.			
18	Session logout mechanism	Ensure that session should not remain valid on server end after log out.			

F
ENFORCEMENT

F.No.16011/257/2019/ED-UIDAI(HQ)/
Ministry of Electronics & Information Technology
Unique Identification Authority of India
*****

Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi-110001
Dated :02nd Aug, 2022

Office Memorandum

Sub: Guidelines for making complaints before Adjudicating Officer – reg.

In pursuance to the notification dated 2nd November, 2021 issued by Central Government vide GSR 772 (E) regarding Unique Identification Authority of India (Adjudication of Penalties) Rules, 2021 (Copy enclosed), an Adjudicating Officer ("A.O") has been appointed, vide order dated 08th March, 2022 (Copy enclosed), for holding inquiry into complaint(s) made by the Authority, with immediate effect and until further orders for the purposes of adjudication and imposing a penalty under Section 33A of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (as amended) (herein after referred to as "the said Act").

2. The guidelines for making a complaint before the A.O shall be as follows: -

a) As per Section 33A of the Act read with Rule 4 of the Unique Identification Authority of India (Adjudication of Penalties) Rules, 2021 (**"Rules"**), the complaint before the A.O can be made by the 'Authority'. Therefore, an officer of the Authority (from ROs/ FWs) may forward the complaint for consideration and approval of the Authority.

b) The complaint can be made against '**entities**' in the Aadhaar eco-system* (as defined under Section 2(aa) of the Act for:

(i) the **failure to** comply with the provisions of the **said Act, the rules or regulations** made thereunder; or

(ii) **failure to** comply with the **directions issued by the Authority** under section 23A of the Act; or

(iii) if the **entity fails to furnish any information, document or return of report** required by the Authority.

c) The complaint should clearly indicate the nature of contravention, relevant provision of the Act or rule or regulation or direction issued by the Authority and the maximum penalty which can be imposed on the person or entity and as far as possible, the timing, place of contravention along with documents in support of such contravention.

[**Aadhaar ecosystem** includes enrolling agencies, Registrars, requesting entities, offline verification- seeking entities and any other entity or group of entities as may be specified by the regulations.]*

INDEX

d) Records of all such cases shall be maintained at Enforcement Division at UIDAI HQ. Necessary coordination shall be done by Enforcement Division in each such case, including seeking approval of the Authority on the complaint and for nomination of an officer to be known as a Presenting Officer, to present the case on behalf of the Authority before the Adjudicating Officer, in each such case. Accordingly, the complaints shall be forwarded by the FW/ROs to Enforcement Division for examination and taking approval of the Authority.

e) The UIDAI (Adjudication of Penalties) Rules, 2021 may be referred as regards manner of making complaint to the adjudicating Officer, for holding inquiry etc.

Enclosures: As above

RSL 2/8/22
(Rupesh Sharma)
Deputy Director

Copy to:

1. All DDG's of Regional Offices and Head quarters
2. OSD to CEO, UIDAI.
3. Guard file.

INDEX

F.No.17022 (11)/11/2022-ENF-HQ
Ministry of Electronics & Information technology
Unique Identification Authority of India
*****

Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi-110001
Dated: 22Nov. 2022

Office Memorandum

Subject: Appointment of Nodal Officer for referring the complaints to the Secretary, Ministry of Electronics & Information technology (MeitY) regarding blocking of access of unauthorized websites.

In pursuance to the notification dated 27th October 2009 issued by the Central Government vide GSR 781(E) regarding the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009, Director, Enforcement Division, UIDAI-HQ has been appointed as a Nodal Officer for receiving the Complaints of unauthorized websites and forwarding the same to the Secretary, Ministry of Electronics & Information technology (MeitY) for blocking of access of such unauthorized websites.

This has the approval of CEO, UIDAI.

22.11.22
(Rupesh Sharma)
Deputy Director

Copy to:

1. All DDG's of Regional Offices and Headquaters
2. OSD to CEO, UIDAI.
3. Guard File.

INDEX