सं. **एच क्यू-13030/1/2020**-ऑथ-I **एच क्यू**

भारत सरकार

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथंटीकेशन डिवीज़न

यूआईडीएआई मुख्यालय भवन, तीसरी मंजिल,
बंगला साहेब रोड, काली मंदिर के पीछे,
गोल मार्केट,नई दिल्ली-110001

दिनांक: 14.12.2020

Circular No. 11 of 2020

Subject: Improvement in authentication success rate

Aadhaar provides effective and efficient authentication services to residents to authenticate anytime, anywhere. Aadhaar authentication enables implementing agencies including government, banks etc. to verify beneficiaries and ensure targeted delivery of benefits and services. Residents can use the Aadhaar number to authenticate and establish their identity by performing authentication through various modes such as biometric (fingerprint and iris), OTP and demographic authentication.

2. Fingerprint, Iris and OTP mode of authentication are effectively being used by various requesting entities for service delivery to the residents and most of the beneficiaries are able to authenticate using these modes of authentication.

3. With a view to improve the resident's experience, the requesting entities in the authentication ecosystem may work closely with UIDAI to improve their authentication success rate. Towards this end, AUAs/KUAs should perform the following activities on an ongoing basis and submit the report on monthly basis:-

i. Biometric authentication success rate.
ii. Device-Model wise authentication success rate.
iii. Device- wise authentication success rate.
iv. Devices with less than 50% accept rate should be examined and remedial action may be taken to improve the success rate of such devices.
v. Devices with less than 25% success rate should be examined for replacement.
vi. Device operator-wise success rate.
vii. Regular maintenance of replacement of faulty devices.
viii. Regular operator training.
ix. Identify the beneficiaries who are not able to authenticate or require more attempts to authenticate. Perform Best Finger Detection (BFD) for such beneficiaries and/or Dual Finger Authentication. If required, guide the beneficiaries for fresh biometric update.
x. AUA/KUA shall monitor the performance of Sub-AUA for auth success rate.
xi. Deploy more number of IRIS devices which are contactless as well.

4. Further, the AUAs need to ensure that the authentication request is formed as per the UIDAI's specifications and there are no errors in the authentication request format. AUAs shall continuously monitor the error codes (sent by UIDAI) of authentication failures and shall update the authentication application for such errors. Some of the error codes are listed below for AUAs to monitor and correct immediately, if occurring:

i. **Error 563** – Ensure no duplicate authentication request is sent
ii. **Error 527** – Invalid RD Public Key Certificate "mc"
iii. **Error 822** – Invalid value in the "bs" attribute of "Bio" element within "Pid"
iv. **Error 998** (Invalid Aadhaar/VID) – Implement Verhoeff algorithm
v. **Error 800** – Invalid biometric data
vi. **Error 521** – Invalid RD code "dc"

5. AUAs are directed to take appropriate actions as mentioned in paragraphs 3 and 4 and submit the action taken report and improvement report as per **Annexure – I** to the respective UIDAI Regional Office by 5th of every month. The first report of December 2020 should be submitted to the respective UIDAI Regional Office by 5th January 2021.

14.12.2020

(अमित भार्गव)
उप निदेशक

Copy to:

All Regional Offices of UIDAI

Annexure – I

Name of AUA:_____

Report for the month of _____

S. No.	Item Description	Action Taken	Improvement Update
1	Biometric authentication success rate		
2	Device-wise authentication success rate		
3	Device-Model wise auth success rate		
4	Devices with less than 50% success rate should be examined and remedial action taken to improve the success rate of such devices		
5	Devices with less the 25% success rate should be examined for replacement		
6	Device operator-wise success rate		
7	Regular maintenance of replacement of faulty devices		
8	Operator training		
9	Identify the beneficiaries who are not able to authenticate or require more attempts to authenticate. Perform Best Finger Detection (BFD) for such beneficiaries and/or Fusion Finger Authentication.		
10	AUA/KUA shall monitor the performance of Sub-AUA for auth success rate		
11	Deploy more number of IRIS devices which are contactless as well		
12	Error 563 - Ensure no duplicate authentication request is sent		
13	Error 527 – Invalid RD Public Key Certificate "mc"		
14	Error 822 - Invalid value in the "bs" attribute of "Bio" element within "Pid"		
15	Error 998 (Invalid Aadhaar/VID) – Implement Verhoeff algorithm		
16	Error 800 – Invalid biometric data		
17	Error 521 - Invalid RD code "dc"		