

F. No. K-11020/219/2018-UIDAI (Auth-I)
Government of India
Ministry of Electronics and Information Technology
Unique Identification Authority of India

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

Dated: 15th January 2018

CIRCULAR No. 2 OF 2018

Sub: Implementation of Face Authentication

Aadhaar Authentication provides a digital, online identity platform to verify the identity of Aadhaar number holders instantly anytime, anywhere. Aadhaar Authentication is the process by which the Aadhaar number along with the demographic information or biometric information (fingerprint or iris) of an Aadhaar number holder is submitted to the Central Identities Data Repository (CIDR) for its verification and such repository verifies the correctness, or the lack thereof, on the basis of the information available with it. Aadhaar authentication is being used as the primary identity verification mechanism by many systems such as Banks, Telecom companies, PDS, Income Tax, Employees attendance etc. which are mandated through various laws and also by a number of private entities. As on date, more than 1510 crore authentications have been performed by various Authentication User Agencies (AUAs) out of which more than 1045 crore are biometric transactions.

2. For biometric based authentication, the Aadhaar number and biometric information submitted by an Aadhaar number holder are matched with the biometric information of the said Aadhaar number holder stored in the CIDR. This may be fingerprints-based or iris-based authentication or other biometric modalities based on biometric information stored in the CIDR. Presently UIDAI provides two modes of biometric authentication i.e. Fingerprint authentication and Iris authentication.

3. While most of the residents are able to authenticate using fingerprint or iris authentication, some residents face difficulty in successfully using biometric authentication using one of the modalities. While residents can use either fingerprint or iris authentication when both capture devices are available, many AUAs have not yet deployed both types of devices for their use.

Y. J. J.
15/1/2018

4. At the time of Aadhaar enrolment, photo of the face of resident is also captured. To provide inclusive authentication, face photo can also be leveraged to verify the identity of a Aadhaar number holder. While Aadhaar Authentication API had the technical provision for sending photo of the face, this option is currently not enabled within CIDR. Some of the advantages of including this are:

- a. Face Authentication will provide additional choice to create inclusive authentication for residents having difficulty with their fingerprints/iris authentication.
- b. Since face photo is already available in UIDAI database there is no need to capture any new reference data at UIDAI CIDR.
- c. Camera is now pervasively available on laptops and mobiles making the face capture easily feasible for AUAs without needing any additional hardware.
- d. Face authentication with liveness detection can be used as an additional factor to increase security.

5. Therefore, UIDAI has decided to enable Face Authentication. The salient features of Face Authentication are:

- a. Face Authentication provides additional option for AUAs to ensure that inclusive authentication is offered to all residents.
- b. Face Authentication shall be allowed ONLY in fusion mode along with one more authentication factor. This means Face Authentication must be combined with either fingerprint or iris or OTP to be able to successfully authenticate an Aadhaar number holder.
- c. UIDAI provides the fingerprint and iris biometric authentication to select AUAs, similarly Face Authentication shall also be allowed on need basis.

6. UIDAI will work with biometric device providers to integrate face modality into the certified registered devices and also may provide standalone Registered Device (RD) service as required by the ecosystem. UIDAI will provide Software Development Kits (SDKs) / Registered Device (RD) services in various operating systems which will have the ability to capture face image, check liveness, and create digitally signed and encrypted authentication input (PID block) as required.

7. The AUAs shall be required to implement the following:


- a. To ensure inclusive authentication, when single modality is not working for specific residents, applications need to enable face capture via RD service to capture face photo in addition to fingerprint/iris/OTP.
- b. Make necessary changes such as doing validation, auditing, etc. on the AUA server side to process the encrypted authentication input.

8. The Registered Device (RD) Service Providers shall be required to integrate the UIDAI provided face capture SDK into their service and allow application to use that option whenever required by the AUA application.

Y
J
15/11/2018

9. UIDAI will share technical documents, software development kits (SDKs), guidelines, and conduct workshops & training sessions for AUAs and Registered Device (RD) Service Providers to support changes for enabling Face Authentication. UIDAI will release necessary details for implementation by 1st March 2018. Face Authentication as an additional modality to be used in fusion mode along with fingerprint/iris/OTP will be available in production for AUAs to use by 1st July 2018.

10. All AUAs and Registered Device (RD) Service Providers, under Regulations 8 and 14(n) of Aadhaar (Authentication) Regulations, 2016, are required to comply with the directions issued and process laid down under this Circular for the purposes of using the authentication facilities provided by the Authority. Any non-compliance of these directions shall invite action under sections 42 and 43 of the Aadhaar Act, 2016.


15/1/2018
(Yashwant Kumar)
Assistant Director General (Auth)

To,

All AUAs, RD Service Providers

Copy to:

All DDGs, UIDAI