F. No. 13043/2/2021-AUTH-I-HQ

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: 31.05.2022

To

All AUA/KUAs

Sub: Advisory regarding Strengthening of Biometric Authentication Security

Dear Madam/Sir,

Your entity has been appointed as an AUA/KUA by UIDAI for availing the Aadhaar authentication facility for authentication of the residents. UIDAI extends the facility of biometric (FP, Iris and Face) authentication which provides irrepudiable authentication of the resident as per the data available with its CIDR. This privilege enjoins upon the user entity a set of responsibilities as per Aadhaar Act and its regulations to provide safe and secure authentication process in the interest of residents. In this regard under Regulation 14 (1) of The Aadhaar (Authentication and Offline verification) Regulations-2021, UIDAI hereby issues following directions to AUAs for immediate compliance:

i. **Implementation of FMR-FIR in Single PID block**:

(a) UDAI vide its letter No. 11020/198/2017-UIDAI (Auth-1)/1dated 11.11.202, 03.02.2022, 30.03.2022 and 04.05.2022 has informed to all the ecosystem partners to expedite the FMR-FIR Single PID block implementation as per the guidelines of UIDAI and complete the necessary changes required in regards with AUA/KUA applications and supporting resources and devices by 30.06.2022. Please note that in interest of the overall ecosystem, UIDAI may not be in position to grant any further extension.

(b) All the AUAs currently using the ISO format should migrate to the XML based authentications and adapt FMR-FIR single PID block implementation.

ii. **Assisted Mode authentication:**

(a) Vide Aadhaar Act and Aadhaar (Authentication and Offline Verification) Regulations- 2021, Regulations no. 14 (d), (e) and (f) a requesting entity is required to maintain security of devices being used for biometric authentication.

(b) AUAs/KUAs are therefore requested to maintain details of devices and operators in assisted mode by maintaining proper logs of the operator with name of operator, deviceID, date and time, etc. These logs should be verified by AUAs at regular periods.

(c) Entities must carry out analysis of devices with high failure rate and such devices should be replaced.

(d) Vide Aadhaar Act and Aadhaar (Authentication and Offline Verification) Regulations- 2021, Regulations no. 14 (m), it is responsibility of AUA to ensure that UIDAI guidelines are followed even if Biometric Auth modality in assisted mode is being outsourced to third party or representative hired by AUA.

iii. **Device Level Security:**

(a) Those devices which report very few or zero transactions over a period of time could be potential targets for frauds. Therefore, AUAs are requested to have an oversight over it and such devices, if possible should be taken out of the system.

(b) Devices, though certified by STQC/UIDAI are deployed by AUAs. Therefore AUA needs to ensure that all devices in their system are certified, no tempering is done with them and are compliant with all guidelines.

(c) AUA/KUAs to ensure deploying devices supporting only the latest OS specifications (Windows 10 / Android OS 10 and above).

2. AUA/KUA's are requested to strictly follow the above-mentioned advisories and help towards making the Aadhaar Authentication Ecosystem safe and secure.

3. This issues with the approval of competent authority.

(Sanjeev Yadav)
Director (Auth-1, HQ UIDAI)

Copy for information to:

1. DG, STQC
2. All RO, UIDAI
3. DDG (Tech Centre, UIDAI)