सं .– K-11020/44/2012– यूआईडीएआई (ऑथ-I)
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:27.11.2020

CIRCULAR No. 09 OF 2020

Subject: Best practices for fingerprint authentication- use of BFD and dual finger to increase authentication success rate and improve resident's experience.

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 modes of authentication have been effectively used by various requesting entities (REs) for service delivery to the residents with most of the beneficiaries able to authenticate using these modes of authentication.

3. However, it is observed that in case of fingerprint authentication, some operators of REs insist on use of thumb for the purpose of biometric authentication and in case of failure, multiple attempts are made only with thumb.

4. It is hereby clarified that any of the ten fingers can be used for fingerprint authentication. Sometimes, due to incorrect placement of finger on the device, worn-out fingerprints, quality of capture of fingerprint at the time of enrolment etc., authentication with a finger may not be successful. Therefore, it is advised that if the authentication is not successful with one finger, it may be attempted again with other fingers.

5. Requesting entities may follow the following best practices to increase authentication success rate and enhance resident's experience:

i. Ensure the biometric device is placed on a plain, clean and stable surface.
ii. Ensure that the finger used for authentication is clean and placed properly on the device.
iii. If authentication fails with one finger, other fingers may be tried for authentication.

iv. For applications requiring authentication at regular intervals (e.g. daily, weekly or monthly), resident's Best Finger Detection (BFD) may be performed to identify the best finger for authentication so that resident can authenticate in one attempt.

v. Dual finger authentication (use of 2 different fingers) may be performed.

6. All REs applications must have BFD and dual finger detection provisions in their applications. Further, the reasons for failure of authentication as per UIDAI's error codes should be communicated to the resident through the application.

7. REs should conduct regular operator trainings with focus on best practices to be followed to improve authentication success rates. Operators must be trained on clearly understanding and explaining the reasons of failure from UIDAI's error code/RE Application response and suggesting remedial solutions to the residents. For instance, if UIDAI error code is 330, the application should indicate that the failure is due to locking of biometrics by the resident and that she should unlock her biometrics just before performing authentication (as the biometrics are temporarily unlocked for 10 minutes) or disable biometric lock by visiting UIDAI's website or using mAadhaar mobile application.

8. Operators must be specifically encouraged to use dual finger services; provide BFD services to the residents who fail in the first go and offer alternate mechanisms of authentication as iris authentication. Operators must also be encouraged to report devices that show frequent authentication failures. Operators who show better success rates may be encouraged and those who repeatedly perform poor may be retrained.

9. All REs are advised to analyze and monitor their authentication success rates for all modalities/devices and for operator performance on regular basis. Old, poorly performing and malfunctioning devices that cause more authentication failures should be weeded out from the system.

10. FAQs on 'Improving Auth Success Rates" available on uidai.gov.in may be referred to for details.

This issues with the approval of competent authority.

अमित
27/11/2020

(अमित भार्गव)
उप निदेशक