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This circular superseded the UIDAI letter cited at (c) and shall be read in continuation of the UIDAI letter cited at (a) & (b).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

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.			