Appendix 4

Compliance checklist for verification of information furnished by applicant for appointment as AUA/KUA

Version 1.0 [issued in March 2024]

Important note: Wherever a control description requires AUA/KUA to ensure or do anything, the same shall be reported as compliant if and only if the auditor finds that the same is being complied with and, further, that appropriate policies, procedures, mechanisms, resources and technical enablements are in place to secure compliance with the same on an ongoing basis.

Control no.	Short title	Control description	Control mapping	Compliance status (Compliant / Non-compliant / Not applicable)	Auditor's observation	Comments of AUA/KUA management
A.	**Information security governance**					
1.	Security organisation and CISO function	AUA/KUA should ensure that it has a designated Chief Information Security Officer (CISO) function that oversees information security governance and compliances. The CISO should have independent reporting to its Board or other governing body or chief executive.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(1)			
2.	Appointment of management and technical single point of contact	AUA/KUA should appoint a Management Single Point of Contact (MPOC) and Technical Single Point of Contact (TPOC) that should oversee the management of the authentication application and Aadhaar related	UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.3			

		activities. MPOC/TPOC should ensure consistent communication with UIDAI on Aadhaar related requirements and compliances. Any change in MPOC/TPOC should be communicated to UIDAI in a timely manner.				
3.	Information security policy and procedure	AUA/KUA should have an information security policy and information security procedures in accordance with industry leading standards, such as ISO27001 (ISMS), NIST Cyber Security Framework, CSA Framework and ISO27701 (PIMS). The entity's information security policy should also address the security aspects of Aadhaar, as provided under the Aadhaar Act, regulations and specifications.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.9			

4.	Aadhaar authentication application design	AUA/KUA should ensure that the authentication application design architecture is documented and validated by UIDAI Technology Centre and covers Aadhaar security requirements.	UIDAI Information Security Policy —UIDAI External Ecosystem — Section 2.3(5)			
5.	Aadhaar authentication application design	AUA/KUA should ensure that the Aadhaar data flow is properly documented for its AUA/KUA applications and those of its Sub-AUAs and Sub-KUAs.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(6)			
6.	Risk assessment	AUA/KUA should implement process and procedure to perform periodic (atleast annual) information security risk assessment of its ICT infrastructure supporting the authentication application. Further, entity should also perform risk assessment of its third party suppliers / vendors having access to the Aadhaar application and the data of Aadhaar number holders.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(13)			

		Security risks should be documented and reviewed periodically by Security Officers / CISO / those incharge of the security governance of the AUA/KUA and its Sub-AUAs and Sub-KUAs.				
7.	Third party information security policy	AUA/KUA should ensure that it has a third party information security policy that lays down the security controls and compliances that its third party vendors, suppliers, ICT service providers and ICT support vendors (*e.g.*, third party / outsource application developers, infrastructure support vendors, data centre hosting agency, cloud service providers etc.) are obligated to adhere to.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(14)			
B.	**Compliance requirement**					
8.	IPR provisionscontained in UIDAI's Aadhaar User AgencyAgreement (latest version)	The AUA/KUA should be in compliance with the intellectual property provisions contained in UIDAI's Aadhaar User Agency	Authentication User Agency Agreement version 6.0 — Section 3			

		Agreement (latest version).				
9.	Annual information security audit by CERT-In-empanelled auditor	AUA/KUA should ensure that its operations and systems are audited by an information systems auditor certified by a recognised body on an annual basis and on need basis to ensure compliance with UIDAI’s standards and specifications. The audit report should be shared with UIDAI. If any non-compliance is found as a result of the audit, AUA/KUAshould — (a) determine the causes of the non-compliance; (b) evaluate the need for actions to avoid recurrence of the same; (c) determine and enforce the implementation of corrective and preventive actions; and	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III — Clause (h) of sub-regulation (1) of regulation 14 • The Aadhaar (Data Security) Regulations, 2016 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.13			

		(d) review the corrective actions taken. The annual audit should cover all security controls applicable under the Aadhaar (Data Security) Regulations, 2016.				
10.	Onboarding of ASA	AUA/KUA should ensure that UIDAI is informed of the ASAs with whom it has entered into agreementto provide necessary infrastructure for ensuring secure network connectivity and related services to it to enable performance of authentication using the Authentication facilities provided by UIDAI.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III —Sub-clause (g) of sub-regulation (1) of regulation 14			
C.	**Data privacy**					
11.	Data protection policy	AUA/KUA should establish a data protection policy addressing, *inter alia*,data protection related aspects under— (a) the Aadhaar Act, the regulations made thereunder and the standards and specifications issued by	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.14(2) • The IT Act • Till the coming into force of the DPDP Act, the SPDI Rules			

		UIDAI from time to time; (b) the Information Technology Act, 2000 ("IT Act"); and (c) till the coming into force of the Digital Personal Data Protection Act, 2023 ("DPDP Act"), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") and, on and from the date of coming into force of the DPDP Act, the said Act and the rules made thereunder. Such policy should be published on the website of AUA/KUA and the URL for the same should be	and, on and from the date of coming into force of clauses (a) and (c) of sub-section (2) of section 44 of the DPDP Act, the said Act and the rules made thereunder[12]			

[12] *See* clauses (a) and (c) of sub-section (2) of section 44 of the DPDP Act, read with clause (ob) of sub-section (2) of section 87 and section 43A of the IT Act

		mentioned.				
12.	Consent of Aadhaar number holder	The AUA/KUA should obtain consent of the Aadhaar number holder or, in case of a child, the consent of the parent or legal guardian of such child, before collecting their identity information for the purposes of authentication. The consent should be obtained preferably in electronic form.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II —Regulation 6			
13.	Information to Aadhaar number holder on the nature of information that will be shared upon performance of authentication	At the time of authentication, before obtaining consent, AUA/KUA should inform the Aadhaar number holder or, in case of a child, the parent or legal guardian of such child,regarding the nature of information that will be shared by UIDAI upon performance of authentication.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II —Clause (a) of sub-regulation (1) of regulation 5			
14.	Information to Aadhaar number holder on use of information	At the time of authentication, before obtaining consent, AUA/KUA should inform the	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter			

	received during authentication	Aadhaar number holder or, in case of a child, the consent of the parent or legal guardian of such child, of the uses to which the information received during authentication may be put to by it.	II —Clause (b) of sub-regulation (1) of regulation 5			
15.	Alternative mechanisms for submission of identity information	At the time of authentication, before obtaining consent, AUA/KUA should inform the Aadhaar number holder or, in case of a child, the parent or legal guardian of such child, of the alternatives to submission of identity information.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II —Clause (c) of sub-regulation (1) of regulation 5			
16.	Consent communication in local language	The AUA/KUA should ensure that the consent information is communicated in local language. The AUA/KUA should also ensure that,on and from the date of coming into force of sub-section (3) of section 5 of the DPDP Act, the Aadhaar number holder has the option to access the contents of the	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Sub-regulation (2) of regulation 5 • On and from the date of coming into force of sub-section (3) of section 5 and sub-section (3) of section 6 of the DPDP Act,			

		notice referred to in sub-sections (1) and (2) of the said sectionand the request for consent referred to in sub-section (3) of section 6in English or any language specified in the Eighth Schedule to the Constitution.	the said Act — Sub-section (3) of section 5 and sub-section (3) of section 6			
17.	Communication of consent related information to persons with visual/hearing disability	The AUA/KUA should make provisions for communication of consent related information to persons with visual/hearing disability in an appropriate manner.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.14			
18.	Explicit consent; no umbrella consent	AUA/KUA should ensure that the consent taken from the Aadhaar number holder should in accordance with the provisions of the Aadhaar Act, 2016 and the regulations made thereunder;no umbrella consent should be taken for sharing e-KYC or Aadhaar number of the Aadhaar number holders with other entities. The AUA/KUA should also ensure that,on and from the date of coming	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.9 • On and from the date of coming into force of sub-section (1) of section 5 and sub-section (1) of section 6 of the DPDP Act, the said Act — Sub-section (1) of section 5 and sub-section (1) of section 6			

		into force of sub-section (1)of section 5 and sub-section (1) of section 6 of the DPDP Act, the consent taken from the Aadhaar number holder is in accordance with the applicable provisions of sections 5 and 6 of the said Act.				
D.	**Asset management**					
19.	Biometric device management	AUA/KUA should capture the biometric information of the Aadhaar number holder using certified and registered biometric devices as per standards specified by UIDAI from time to time.	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Clause(a) of sub-regulation (1) of regulation 7, sub-regulation (1) of regulation 8 and clause (d) of sub-regulation (1) of regulation 14 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.4			

20.	End-point security	AUA/KUA should ensure that biometric deploying devices are connected with end-point systems that have the latest operating system (OS) specifications (as of March 2024, at least Windows 10 and above and Android OS 10 and above), and that systems based on an OS that is end-of-life or end-of-support are not deployed or used.	Advisory regarding strengthening of Biometric authentication security [AdvisoryF. no. 13043/2/2021-AUTH-1-HQ, dated 31.5.2022]			
21.	Security hardening of assets	AUA/KUA should ensure all the end-point devicesand assets are used only after hardening to reduce/eliminate the attack vector and condense the system attack surface.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			
22.	Maintenance of software inventory	AUA/KUA should ensure that it uses only licensed software for Aadhaar authentication related infrastructure environment. Record of all software licenses should be kept and updated regularly.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.13			

23.	Asset disposal procedure	AUA/KUA should define a procedure for disposal of the information assets being used for authentication operations. Information systems and documents containing Aadhaar related information should be disposedof securely.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.4			
E.	**Human resource security**					
24.	Background verification and signing of confidentiality agreement	AUA/KUA should conduct a background check and sign a confidentiality agreement/ non-disclosure agreement (NDA) with all personnel/agency handling Aadhaar related information. Access to authentication infrastructure should not be granted before signing NDA and completion of background verification(BGV) for personnel.	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			
25.	Background verification and signing of confidentiality agreement with third-party	AUA/KUAshould take an undertaking from business correspondents (BCs) and similar entities, Sub-AUAs/Sub-KUAs	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			

	contractors	and other third party contractors regarding NDAs and BGVs conducted successfully for their personnel handling Aadhaar related data.				
26.	Training and awareness	AUA/KUA should ensure that MPOC, TPOC and their supporting teams that manage and maintain the authentication application and its underlying infrastructure, are aware of Aadhaar security requirements.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.3(7)			
27.	Operator qualification	AUA/KUA should ensure that the operator employed for performing authentication functions and maintaining necessary systems, infrastructure and process, possess requisite qualification for undertaking such work.	The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter III —Clause (f) of sub-regulation (1) of regulation 14			
28.	Periodic information security and privacy trainings related to Aadhaar authentication operations	AUA/KUA should impart information security and data privacy trainings to all its personnel as well as those of any BCs, Sub-AUAs/Sub-KUAs and similar entities, in relation to the use of	UIDAI Information Security Policy —UIDAI External Ecosystem — AUA KUA — Section 2.3			

		Aadhaar Authentication facilities, during induction of such personnel/entity, on half-yearly basis and as and when changes are made in the authentication ecosystem. AUA/KUA should further ensure that specific and specialised training are imparted for various functional roles involved in the authentication ecosystem and that the same cover all relevant security and data privacy guidelines, as per the UIDAI Information Security Policy for Authentication, Aadhaar Act, 2016 and the regulations made thereunder and circulars, notices etc. issued by UIDAI from time to time. AUA/KUA should also maintain a record of such trainings imparted.				
F.	**Incident management**					

29.	Incident management procedure and RCA procedure	AUA/KUA should ensure that incident management framework, including forensic investigation, is implemented in accordance with the requirements under UIDAI's Information Security Policy and circulars. AUA/KUA should perform Root Cause Analysis (RCA) for major incidents identified in its ecosystem as well as that of its sub-contractors, if any.	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA/KUA — Section 2.12 • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.13			
30.	Incident reporting requirement for Sub-AUAs/Sub-KUAs and BCs	AUA/KUAshould ensure that the Sub-AUAs/Sub-KUAs, BCs and other sub-contractors are aware of Aadhaar authentication related incident reporting.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.12			
G.	**Access control**					
31.	Multi-factor authentication of operator	AUA/KUA should ensure in the case of assisted devices and applications where operators need to mandatorily perform application functions, that the operator is authenticated using a multi-factor	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5			

		authentication scheme, such as user id, password, Aadhaar authentication, answer to personal security questions, soft token, hard token, one-time password, voice recognition, biometric data match and PIN.				
32.	Access provisioning mechanism	AUA/KUA should ensure that only authorised individuals are able to access information facilities such as the authentication application, audit logs, authentication servers, application, source code, information security infrastructure, etc., and Aadhaar processing related information.	• UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.5 • The Aadhaar (Data Security) Regulations, 2016 — Clause (h) of regulation 5			
33.	Privilege user access management	AUA/KUA should ensure that systems and procedures are in place for privilege user access management (PAM). Privilege user access should be limited to authorised users only.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 (6)			

34.	Privilege accounts	AUA/KUA should ensure through the PAM tool that privileged accounts, such as NT Authority, Administrator and root accounts, are accessible only to a limited set of users, and thataccess to privileged account is not allowed to normal users.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			
35.	Periodic access review	AUA/KUA should ensure that access is provided based on least privilege and that access is reviewed periodically (at leasthalf-yearly).	• UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.5 (2) • The Aadhaar (Data Security) Regulations, 2016 — Clause (h) of regulation 5			
36.	Segregation of duties	AUA/KUA should ensure that personnel involved in operational, development or testing functions should not be given additional responsibilities in system administration processes, audit log maintenance, security review of system or processes that may	UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.9(4) and(5)			

		compromise data security. Where segregation of duties is not possible or practicable, the process should include compensating controls, such as monitoring of activities, maintenance and review of audit trails and management supervision.				
37.	Initial password allocation	AUA/KUA should ensure that the allocation of initial passwords is done in a secure manner and that such passwords are changed on first login.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.6 (1)			
38.	Password management guidelines	AUA/KUA should ensure that passwords set are complex, with a minimum length of eight characters and— (a) are not based on anything somebody else may easily guess or obtain using person related information, *e.g.*,	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.6 (5)			

		name, telephone number and date of birth; (b) is free of consecutive identical characters or all-numeric or all-alphabetical groups; (c) contain at least one numeric, one uppercase letter, one lowercase letter and one special character; (d) are required to be changed at regular intervals (passwords for privileged accounts should be changed more frequently than normal passwords); (e) do not allow the use of the last five passwords; (f) do not allow the				

		username and password to be the same for a particular user; and (g) do not use the same password for various UIDAI access needs of a particular user.				
39.	User account lockout	AUA/KUA should ensure that three successive log-in failures result in the user account being locked. End users / operators should not be able to login until their account is unlocked and the password is reset.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 (9)			
40.	Restriction usage of generic IDs	AUA/KUA should ensure that common or generic or group user IDs are not used.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.5 (5)			
H.	**Change management**					
41.	Change logs management	AUA/KUA should document all changes to Aadhaar authentication applications, infrastructure, processes and information processing	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.15 (1)			

		facilities, and maintain change log/register.	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.15 (2)			
I.	**Data security**					
42.	Use of Aadhaar data vault (ADV) on cloud	AUA/KUA should ensure that if ADV is hosted on cloud, the ADV cloud service complies with UIDAI's Guidelines for ADV on Cloud. The ADV should be hosted only by Government Community Cloud (GCC) service providers, recognised as such by the Ministry of Electronics and Information Technology.	UIDAI Guidelines for ADV on Cloud			
43.	End-point security	AUA/KUA should ensure that USB access on the servers and endpoints is, in the default, restricted for all, and the same is allowed only on approval basis.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			
44.	End-point security — antivirus / anti-malware	AUA/KUA should use licensed malware and antivirus solution (preferablyNext-Generation antivirus) to	UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.9(10)			

		protect against malware. The malware/antivirus installed should be configured to update in real time.				
45.	Use of security communication protocols	AUA/KUA and ASA should ensure message security and integrity between their servers and those of third party entities, such as Sub-AUAs and Sub-KUAs. AUA/KUA should procure digital certificate from a Certifying Authority as defined in the IT Act.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.11(6)			
46.	End-point security	AUA/KUA should ensure that end-point devices used for developing, process and handling Aadhaar data and application timeout after a session is idle for more than 30 to 15 minutes, based on the criticality of the application.	• UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(29) • UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.9(30)			

47.	Secure software development	AUA/KUA should implement system and processes to ensure secure software development practices. Periodic training of developers should be conducted on secure software development practices. Records of such trainings should be maintained.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.9(5)			
48.	Patch management	AUA/KUA should ensure that the patch management process is implemented for applying patches to information systems. Patches should be updated at both the application and the server and network levels. AUA/KUA should ensure that either N or N-1 patches are maintained.	UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.9(8)			
J.	**Network security**					
49.	Network security	AUA/KUA should ensure that Internet access on systems are restricted to necessary or work-related websites and that access to web portals known for pirated software, gambling etc. are restricted.	UIDAI Information Security Policy — UIDAI External Ecosystem — AUA KUA — Section 2.4			

K.	**Operations security**					
50.	Restrictions on designing/ compiling malicious code	AUA/KUA personnel should not intentionally write, generate, compile, copy or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any Aadhaar information.	UIDAI Information Security Policy— UIDAI External Ecosystem — AUA KUA — Section 2.9			
51.	Implementation of Virtual ID	AUA/KUA must provide in their authentication application the option for an Aadhaar number holderto use a Virtual ID (VID) for authentication, in place of their Aadhaar number.	UIDAI circular no. K-11020/217/2018-UIDAI (Auth-I), dated 1.5.2018 (Implementation of VID, UID Token and Limited KYC)			
52.	Establishment of grievance handling mechanism	AUA/KUA should have an effective grievance handling mechanism and provide the same through multiple channels.	Authentication User Agency Agreement version 6.0 — Paragraph 14.3			
L.	**Application security**					
53.	Compliance to API specifications and application security	AUA/KUA should ensure that the client applications and software used for authentication should conform to the latest API standards and specifications laid down by UIDAI from time to time, and that itsSub-	• The Aadhaar (Authentication and Offline Verification) Regulations, 2021 — Chapter II — Sub-regulation (2) of regulation 8 and Chapter III — Clause			

		AUAs and Sub-KUAs use client applications or software development kit (SDK) developed or digitally signed by the AUA/KUA.	(a) of sub-regulation (3) of regulation 15 • UIDAI Aadhaar Authentication Application Security Standard, version 1.0, 2020 • UIDAI Aadhaar Authentication API Specification Version 2.5, Revision 1, January 2022			
54.	API whitelisting and API gateway implementation	AUA/KUA should ensure that it has API whitelist implemented to limit the data exchange using only authorised APIs and with whitelisted IP addresses. AUA/KUA should also ensure that API gateway is deployed for centralised security enforcement, monitoring and management. AUA/KUA should ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(4)			

		API and Distributed Denial of Service (DDoS) attacks. AUA/KUA should ensure that Cross-Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the clientside.				
55.	Vulnerability assessment	AUA/KUA should plan organisation information security policy, inclusive of vulnerability assessment and penetration testing on its network, infrastructure and applications.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(6)			
56.	Configuration reviews and system walkthrough	AUA/KUA should ensure that authentication applications are integrated with IDAM, PIM/PAM and SIEM.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.11(8)			
57.	Application code review	AUA/KUA should ensure that the passwords, tokens, security keys and licenses are not hardcoded in the application code.	UIDAI Information Security Policy — UIDAI External Ecosystem — Section 2.10(5)			
M.	**Logging and monitoring**					
58.	Clock synchronisation through use of Network	AUA/KUA should connect to the Network Time Protocol (NTP) server of the	• UIDAI Information Security Policy— UIDAI			

	Time Protocol (NTP)	National Informatics Centre (NIC) or National Physical Laboratory (NPL), or with NTP servers traceable to the said NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC; however, it should be ensured that such time source does not deviate from NPL and NIC.	External Ecosystem — AUA KUA — Section 2.9 (22) • CERT-In Directive No. 20(3)/2022-CERT-In dated 28.4.2022			
N.	**Providing Aadhaar Authentication facilities to Sub-AUAs and Sub-KUAs**					
59.	Authentication application security	AUA/KUA should ensure that the authentication application to be used or being used for Aadhaar authentication by its Sub-AUAs and Sub-KUAs is developed and be digitally signed by AUA/KUA.	UIDAI Circular K11022/460/2016-UIDAI (Auth-II), dated 28.2.2017 — Clause 1(i)			
60.	Authentication application security	AUA/KUA should ensure that the authentication application used by its Sub-AUAs and Sub-KUAs does not store biometric data under any	UIDAI Circular K11022/460/2016-UIDAI (Auth-II), dated 28.2.2017 — Clause 1(ii)			

		circumstance, and that the biometrics / PID block is encrypted at the front-end device / client level.				

***