**Compliance checklist for certifying compliance with controls that the Sub AUA/ Sub KUA is required to have in place**

**Version 1.0 [issued in April 2024]**

**Important note:** Wherever a control description requires Sub AUA/ Sub 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 enablement are in place to secure compliance with the same on an ongoing basis.

| Control no. | Short title | Control description | Compliance status (Compliant / Non-compliant / Not applicable) | Auditor's observation | Comments of Sub AUA / Sub KUA management |
|---|---|---|---|---|---|
| **A.** | **Information security governance** | | | | |
| 1. | Security organisation and CISO function | Sub AUA/ Sub 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. | | | |
| 2. | Appointment of management and technical single point of contact | Sub AUA/ Sub 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 activities.<br>MPOC/TPOC should ensure consistent communication with UIDAI on Aadhaar related requirements and compliances.<br>Any change in MPOC/TPOC should be communicated to UIDAI in a timely manner. | | | |

| | | | | | |
|---|---|---|---|---|---|
| 3. | Information security policy and procedure | Sub AUA/ Sub 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).<br>The entity's information security policy should also address the security aspects of Aadhaar, as provided under the Aadhaar Act, regulations and specifications. | | | |
| 4. | Aadhaar authentication application design | Sub AUA/ Sub KUA should ensure that the authentication application design architecture is documented which covers Aadhaar security requirements. | | | |
| 5. | Aadhaar authentication application design | Sub AUA/ Sub KUA should ensure that the Aadhaar data flow is properly documented for its Sub AUA/ Sub KUA applications. | | | |
| 6. | Risk assessment | Sub AUA/ Sub KUA should implement process and procedure to perform periodic (at least annual) information security risk assessment of its ICT infrastructure supporting the authentication application.<br>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.<br>Security risks should be documented and reviewed periodically by Security Officers / CISO / those in charge of the security governance of the Sub-AUAs and Sub-KUAs. | | | |
| 7. | Third party information security policy | Sub AUA/ Sub 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. | | | |
| **B.** | **Compliance requirement** | | | | |
| 8. | Annual information security audit by CERT-In-empanelled auditor | Sub AUA/ Sub 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.<br>If any non-compliance is found as a result of the audit, Sub AUA/ Sub KUA should—<br>(a) determine the causes of the non-compliance;<br>(b) evaluate the need for actions to avoid recurrence of the same;<br>(c) determine and enforce the implementation of corrective and preventive actions; and<br>(d) review the corrective actions taken.<br>The annual audit should cover all security controls applicable under the Aadhaar (Data Security) Regulations, 2016. | | | |
| **C.** | **Data privacy** | | | | |
| 9. | Data protection policy | Sub AUA/ Sub KUA should establish a data protection policy addressing, *inter alia*, data protection related aspects under—<br>(a) the Aadhaar Act, the regulations made thereunder and the standards and specifications issued by | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | UIDAI from time to time;<br>(b) the Information Technology Act, 2000 (“IT Act”); and<br>(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.<br>Such policy should be published on the website of Sub AUA/ Sub KUA and the URL for the same should be mentioned. | | | |
| 10. | Consent of Aadhaar number holder | The Sub AUA/ Sub 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. | | | |
| 11. | 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, Sub AUA/ Sub 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. | | | |
| 12. | Information to Aadhaar number holder on use of | At the time of authentication, before obtaining consent, Sub AUA/ Sub KUA should inform the Aadhaar number holder or, in case of a child, the consent of the parent or | | | |

| | | | | | |
|---|---|---|---|---|---|
| | information received during authentication | legal guardian of such child, of the uses to which the information received during authentication may be put to by it. | | | |
| 13. | Alternative mechanisms for submission of identity information | At the time of authentication, before obtaining consent, Sub AUA/ Sub 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. | | | |
| 14. | Consent communication in local language | The Sub AUA/ Sub KUA should ensure that the consent information is communicated in local language.<br>The Sub AUA/ Sub 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 notice referred to in sub-sections (1) and (2) of the said section and 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. | | | |
| 15. | Communication of consent related information to persons with visual/hearing disability | The Sub AUA/ Sub KUA should make provisions for communication of consent related information to persons with visual/hearing disability in an appropriate manner. | | | |
| 16. | Consent log retention | Sub AUA/ Sub KUA should maintain the logs for—<br>(a) record of consent of the Aadhaar number holder for authentication; and<br>(b) record of disclosure of information, as mentioned in Control numbers 13, 14, 15, 16, 17 and 18 above, to the Aadhaar number holder at the time | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | of authentication.<br><br>For any given Aadhaar number holder, whose identity information was collected, the Sub AUA/ Sub KUA should be able to demonstrate that consent was taken and disclosure of information was made. | | | |
| 17. | Explicit consent; no umbrella consent | Sub AUA/ Sub 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.<br><br>The Sub AUA/ Sub KUA should also ensure that, 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 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** | | | | |
| 18. | Biometric device management | Sub AUA/ Sub 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. | | | |

| | | | | | |
|---|---|---|---|---|---|
| 19. | Biometric device management | Devices reporting transactions at a very low frequency over time may be potential targets of frauds. Therefore, Sub AUA/ Sub KUA should maintain oversight in respect of the same and identify and remove such devices from the system. | | | |
| 20. | Biometric device management | Sub AUA/ Sub KUA should monitor the operations of its devices and equipment, on periodic basis, for compliance with the terms and conditions, standards, directions and specifications, issued and communicated by UIDAI from time to time. | | | |
| 21. | Biometric device management | Sub AUA/ Sub KUA should carry out analysis of devices with high failure rates and replace them. | | | |
| 22. | End-point security | Sub AUA/ Sub 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. | | | |
| 23. | Security hardening of assets | Sub AUA/ Sub KUA should ensure all the end-point devices and assets are used only after hardening to reduce/eliminate the attack vector and condense the system attack surface. | | | |
| 24. | Asset inventory maintenance | Sub AUA/ Sub KUA should ensure that all assets (business applications, operating systems, databases, network etc.) used for the purpose of delivering services to Aadhaar number holders using Aadhaar Authentication facilities are identified, labelled and classified.<br>Sub AUA/ Sub KUA should record the details regarding | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | assets used and maintain and update the asset inventory on a continuous basis. Ownership of authentication assets should be clearly documented. | | | |
| 25. | Maintenance of software inventory | Sub AUA/ Sub 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. | | | |
| 26. | Asset disposal procedure | Sub AUA/ Sub 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 disposed of securely. | | | |
| 27. | Asset repair procedure and asset movement logs | Sub AUA/ Sub KUA should, before consigning any asset for repair, sanitise the same to ensure that it does not contain any Aadhaar related data. A register to log the movement of all the assets consigned outside should be maintained. | | | |
| 28. | Asset repair procedure | Sub AUA/ Sub KUA should, in case of in-house repair of assets, document the details of the original equipment manufacturer (OEM) and maintain the logs of the assets being repaired. | | | |
| **E.** | **Human resource security** | | | | |
| 29. | Background verification and signing of confidentiality agreement | Sub AUA/ Sub 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. | | | |

| | | | | | |
|---|---|---|---|---|---|
| 30. | Background verification and signing of confidentiality agreement with third-party contractors | Sub AUA/ Sub KUA should take an undertaking from business correspondents (BCs) and other third-party contractors regarding NDAs and BGVs conducted successfully for their personnel handling Aadhaar related data. | | | |
| 31. | Training and awareness | Sub AUA/ Sub 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. | | | |
| 32. | Operator qualification | Sub AUA/ Sub 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. | | | |
| 33. | Periodic information security and privacy trainings related to Aadhaar authentication operations | Sub AUA/ Sub KUA should impart information security and data privacy trainings to all its personnel as well as those of any BCs and similar entities, in relation to the use of Aadhaar Authentication facilities, during induction of such personnel/entity, on half-yearly basis and as and when changes are made in the authentication ecosystem.<br>Sub AUA/ Sub 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.<br>Sub AUA/ Sub KUA should also maintain a record of such trainings imparted. | | | |
| **F.** | **Incident management** | | | | |
| 34. | Incident management procedure and RCA procedure | Sub AUA/ Sub 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. Sub AUA/ Sub KUA should perform Root Cause Analysis (RCA) for major incidents identified in its ecosystem as well as that of its sub-contractors, if any. | | | |
| 35. | Reporting of incidents to UIDAI and CERT-In | Sub AUA/ Sub KUA should—<br>(a) inform UIDAImisuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or systems within its network, and report any confidentiality security breach of Aadhaar related information to UIDAI within 24 hours;<br>(b) report cyber incidents as mentioned in Annexure I to the directions dated 28.4.2022 of CERT-In, bearing no. 20(3)/2022-CERT-In, within 6 hours of noticing such incidents or the same being brought to their notice; and<br>(c) on and from the date of coming into force of sub-section (6) of section 8 of the DPDP Act, intimation of personal data breach to the Board and each affected Data Principal, within such time as may be prescribed by rules made under the said Act. | | | |

| | | | | | |
|---|---|---|---|---|---|
| **G.** | **Access control** | | | | |
| 36. | Multi-factor authentication of operator | Sub AUA/ Sub 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 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. | | | |
| 37. | Operator logs | Sub AUA/ Sub KUA should maintain details of devices and operators employed for the use of Aadhaar Authentication facilities in assisted mode, including proper logs of such operators, along with their name, device ID, date and time, etc. These logs should be verified by Sub AUA/ Sub KUA at regular intervals. | | | |
| 38. | Access provisioning mechanism | Sub AUA/ Sub 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. | | | |
| 39. | Privilege user access management | Sub AUA/ Sub 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. | | | |
| 40. | Privilege accounts | Sub AUA/ Sub 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. | | | |

| | | | | | |
|---|---|---|---|---|---|
| 41. | Periodic access review | Sub AUA/ Sub KUA should ensure that access is provided based on least privilege and that access is reviewed periodically (at least half-yearly). | | | |
| 42. | Access revocation mechanism | Within 24 hours of exit of any personnel, Sub AUA/ Sub KUA should revoke the rights and privileges to access or process Aadhaar related information. Upon such revocation, user IDs should be deleted forthwith if not in use. | | | |
| 43. | Segregation of duties | Sub AUA/ Sub 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 compromise data security.<br>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. | | | |
| 44. | Initial password allocation | Sub AUA/ Sub KUA should ensure that the allocation of initial passwords is done in a secure manner and that such passwords are changed on first log in. | | | |
| 45. | Password management guidelines | Sub AUA/ Sub KUA should ensure that passwords set are complex, with a minimum length of eight characters and—<br>(a) are not based on anything somebody else may easily guess or obtain using person related information, *e.g.*, name, telephone number and date of birth;<br>(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;<br>(d) are required to be changed at regular intervals (passwords for privileged accounts should be changed more frequently than normal passwords);<br>(e) do not allow the use of the last five passwords;<br>(f) do not allow the username and password to be the same for a particular user; and<br>(a) do not use the same password for various UIDAI access needs of a particular user. | | | |
| 46. | User account lockout | Sub AUA/ Sub KUA should ensure that three successive log-in failures result in the user account being locked. End users / operators should not be able to log in until their account is unlocked and the password is reset. | | | |
| 47. | Restriction usage of generic IDs | Sub AUA/ Sub KUA should ensure that common or generic or group user IDs are not used. | | | |
| **H.** | **Change management** | | | | |
| 48. | Change logs management | Sub AUA/ Sub KUA should document all changes to Aadhaar authentication applications, infrastructure, processes and information processing facilities, and maintain change log/register. | | | |
| **I.** | **Physical security** | | | | |
| 49. | Physical security of Sub AUA data centre | Sub AUA / Sub KUA data centre hosting Aadhaar related information should be secured fully and should have access control. | | | |
| 50. | Security of Sub AUA servers | Sub AUA / Sub KUA should ensure that their servers are placed in an isolated, secure cabinet in the data centre. | | | |

| | | | | | |
|---|---|---|---|---|---|
| 51. | Physical security of Sub AUA data centre | Sub AUA / Sub KUA data centre and servers should be under 24X7 protection of security guards and CCTV surveillance. | | | |
| 52. | Physical security of Sub AUA data centre | Sub AUA / Sub KUAshould ensure that access to the data centre is restricted only to authorised individuals and appropriate logs of entry of individuals should be maintained. | | | |
| 53. | Physical security of Sub AUA data centre | Sub AUA / Sub KUA should ensure that physical access to the data centre and other restricted areas hosting critical Aadhaar related equipment/information is pre-approved and recorded, along with the date, time and purpose of entry. | | | |
| 54. | Physical security of Sub AUA data centre | Sub AUA / Sub KUA should ensure that the movement of all incoming and outgoing assets related to Aadhaar in the Sub AUA / Sub KUA data centre is documented. | | | |
| 55. | Physical security of Sub AUA data centre | Sub AUA / Sub KUA should ensure that visible and clearly readable signs/notices notifying areas designated as restricted areas and provisions restricting entry to the same are posted at all points leading to entry to such areas. | | | |
| 56. | Physical security of Sub AUA data centre | Sub AUA / Sub KUA should provide lockable cabinets or safes in the data centre and information processing facilities for housing servers containing critical Aadhaar related information. Sub AUA / Sub KUA should deploy label, monitor and test regularly the operation of fire exit doors and fire extinguishing systems. | | | |
| 57. | Preventive maintenance activity at data centre | Sub AUA / Sub KUA should ensure that preventive maintenance activities, such as audit of fire extinguishers and CCTV, are carried out on a quarterly basis. | | | |
| 58. | Physical location of | Sub AUA / Sub KUA should ensure that the data centres | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Sub AUA servers | hosting servers on which Aadhaar related information is stored are within India. | | | |
| **J.** | **Data security** | | | | |
| 59. | PID encryption and biometric data security | Sub AUA / Sub KUA should ensure that after collection of requisite demographic and/or biometric information and/or one-time password (OTP) from the Aadhaar number holder, the client application immediately packages and encrypts these input parameters into a PID block, before transmitting the same, and that the same is sent to the server of the AUA/KUA using secure protocols. | | | |
| 60. | PID encryption and biometric data security | Sub AUA / Sub KUA should ensure that the PID block is encrypted with a dynamic session key using AES 256 symmetric algorithm (AES / GCM / No Padding) at the time of capture on the authentication device. The session key should be encrypted with 2048-bit UIDAI public key using asymmetric algorithm (RSA/ECB/PKCS1 Padding). In doing so, Sub AUA / Sub KUA should comply with the latest API specification document issued by UIDAI from time to time. | | | |
| 61. | PID encryption and biometric data security | Sub AUA / Sub KUA should ensure with respect to the operational details referred to against control number 65, that the session key is not stored anywhere except in the memory and that the same is not reused across transactions. Reuse of session key is allowed only when it is used as seed key while using synchronised session key scheme. | | | |
| 62. | Aadhaar number security | Sub AUA / Sub KUA should ensure that the Aadhaar number / Virtual ID (VID) / ANCS token provided by the Aadhaar number holder for authentication request is | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | not retained by the device operator or within the device or at the Sub AUA / Sub KUA server(s). | | | |
| 63. | Restriction in storage of Aadhaar number, biometrics and/or eKYC of Aadhaar number holder | Sub AUA / Sub KUA should ensure that under no circumstances assisted devices and any application associated with Aadhaar authentication stores the Aadhaar number, biometrics and/or e-KYC of the Aadhaar number holder. | | | |
| 64. | Fingerprint biometric data (FMR and FIR) capture in single PID block | For fingerprint-based biometric authentication devices, Sub AUA / Sub KUA should ensure capture of Finger Minutiae Record (FMR) and Finger Image Record (FIR) in single PID block. | | | |
| 65. | Use of ADV | Sub AUA / Sub KUA which is allowed to store Aadhaar number should collect and store Aadhaar number and any connected data only in a separate, secure database/vault/system, termed as Aadhaar Data Vault (ADV).<br>Such Sub AUA / Sub KUA should ensure that each Aadhaar number is referred to by an additional key, called as reference key, and that mapping of the reference key and Aadhaar number is maintained in ADV. | | | |
| 66. | Use of Aadhaar data vault (ADV) on cloud | Sub AUA / Sub 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. | | | |
| 67. | Use of ADV on cloud | Sub AUA / Sub KUA having ADV on cloud should get annual SOC2 Type2 examination performed for cloud hosting service. Management review should be | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | performed for non-compliant / qualified controls reported in the SOC2 Type2 reports. | | | |
| 68. | Use of ADV | Sub AUA / Sub KUA should ensure that Aadhaar numbers along with connected data (such as eKYC XML containing Aadhaar numbers and demographic data), if any, is stored only in a single logical instance of ADV, along with corresponding reference key. Sub AUA / Sub KUA should ensure that appropriate High Availability and Disaster Recovery provisions are made for the vault, with the same level of security. | | | |
| 69. | Use of ADV | Sub AUA / Sub KUA should ensure that only trusted communications are permitted in and out of the vault; this should ideally be done through APIs/microservices dedicated to obtain the mapping and controlling the access to the APIs/microservices at the application level. Sub AUA / Sub KUA should ensure that any authorised users needing to access such mapping necessarily go through the application for viewing/accessing the data, after appropriate user authentication, authorisation and logging. | | | |
| 70. | Use of ADV | Sub AUA / Sub KUA should ensure that strong access controls, authentication measures, monitoring and logging of access and raising of necessary alerts for unusual and/or unauthorised attempts to access ADV are implemented. | | | |
| 71. | End-point security | Sub AUA / Sub 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. | | | |
| 72. | End-point security — antivirus / anti- | Sub AUA / Sub KUA should use licensed malware and antivirus solution (preferably Next-Generation antivirus) | | | |

| | | | | | |
|---|---|---|---|---|---|
| | malware | to protect against malware. The malware/antivirus installed should be configured to update in real time. | | | |
| 73. | Aadhaar information security — Physical Aadhaar documents | Sub AUA / Sub KUA should mask Aadhaar numbers collected through physical forms or photocopies of Aadhaar letters, by masking the first eight digits of the Aadhaar number, before storing physical copies. | | | |
| 74. | Restriction on display/ publishing of identity information | Sub AUA / Sub KUA, Business Correspondents and other sub-contractors performing Aadhaar authentication should ensure that identity information is not displayed or disclosed to external agencies or unauthorised persons. | | | |
| 75. | Restriction in display/ publishing of identity information | Sub AUA / Sub KUA should not publish any personal identifiable data including Aadhaar in public domain/websites etc. | | | |
| 76. | Restriction in display/ publishing of identity information | Sub AUA / Sub KUA should ensure that display of full Aadhaar number is controlled only for the Aadhaar number holder or for such special roles/users of Sub AUA / Sub KUA as have functional necessity for the same; by default, all other display should be masked such that only the last four digits of the Aadhaar number are displayed. | | | |
| 77. | End-point security | Sub AUA / Sub 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. | | | |
| 78. | Secure software development | Sub AUA / Sub KUA should implement system and processes to ensure secure software development practices.<br>Periodic training of developers should be conducted on | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | secure software development practices. Records of such trainings should be maintained. | | | |
| 79. | Restriction in local storage of Aadhaar data / PII information | Sub AUA / Sub KUA should ensure that there is no local storage of Aadhaar number or VID or the PID block on the system, volatile memory or the database.<br>In case of a mobile application, Sub AUA / Sub KUA should ensure that there is no local storage of Aadhaar number or the PID block in the shared preference folder. | | | |
| 80. | Patch management | Sub AUA / Sub 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.<br>Sub AUA / Sub KUA should ensure that either N or N-1 patches are maintained. | | | |
| 81. | PID encryption and biometric data security | Sub-AUA/Sub-KUA should ensure that biometric data are necessarily encrypted and secured at the time of capture of such information of the Aadhaar number holder, in accordance with such specifications as UIDAI may lay down from time to time | | | |
| 82. | Encryption of stored eKYC data | Sub-AUA/Sub-KUA should ensure that e-KYC data is stored in an encrypted manner in database tables. | | | |
| **K.** | **Network security** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 83. | Network connectivity with AUA | Sub-AUA/Sub-KUA should establish secure network connectivity between Sub-AUA/Sub-KUA and its AUA, and should connect with AUA only through secure leased lines or similar secure private lines. If a public network is used, only a secure channel should be used. | | | |
| 84. | Segregation of Sub AUA servers network | Sub AUA / Sub KUA should ensure that its servers reside in a segregated network segment isolated from the rest of the network of the Sub AUA / Sub KUA organisation. The Sub AUA / Sub KUA servers should be dedicated for online Aadhaar authentication purposes and should not be used for any other activities not related to Aadhaar. | | | |
| 85. | Firewall access of network | Sub AUA / Sub KUA should ensure that authentication application servers and infrastructure are hosted behind a firewall and that firewall rules block incoming access requests to the Sub AUA / Sub KUA server from all sources other than whitelisted IP addresses/zones. | | | |
| 86. | NIPS/IDS implementation | Sub AUA / Sub KUA should ensure that network intrusion and prevention systems (NIPS) and intrusion detection system (IDS) are implemented to safeguard the network from external attacks / DDoS attacks. | | | |
| 87. | Network security | Sub AUA / Sub 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. | | | |
| 88. | Encryption of data on network | Sub AUA / Sub KUA should ensure that transmission of Aadhaar number across open, public networks is always encrypted, using the latest version of Transport Layer Security (TLS) configuration. | | | |

| | | | | | |
|---|---|---|---|---|---|
| **L.** | **Operations security** | | | | |
| 89. | Segregation of testing and production environments | Sub AUA / Sub KUA should ensure that the testing and production facilities/environments are physically and/or logically separated.<br>Sub AUA / Sub KUA should ensure that authentication application testing utilises test data / non-production data and that Aadhaar number holder's identity data are not used for testing the application. | | | |
| 90. | Restrictions on designing/ compiling malicious code | Sub AUA / Sub 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. | | | |
| 91. | Implementation of Virtual ID | Sub AUA / Sub KUA must provide in their authentication application the option for an Aadhaar number holder to use a Virtual ID (VID) for authentication, in place of their Aadhaar number. | | | |
| 92. | Restriction on the use of Aadhaar as domain-specific identifier | Sub AUA / Sub KUA should ensure that Aadhaar number and VID are never used as domain-specific identifiers and that domain-specific identifiers are revoked and/or reissued. For example, instead of using Aadhaar number as bank customer ID or license number or student ID etc., a local, domain-specific identifier mapped in the back-end database should be used. | | | |
| 93. | Unique device code of each device | Sub AUA / Sub KUA should ensure that each authentication device has a unique device code and that a unique transaction number is automatically generated by the authentication device and incremented for each transaction processed. | | | |

| | | | | | |
|---|---|---|---|---|---|
| 94. | Back-up / alternative identity authentication mechanism | Sub AUA / Sub KUA should implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication delivery of services to Aadhaar number holders. | | | |
| 95. | Notification to Aadhaar number holders | Sub AUA / Sub KUA should notify the Aadhaar number holder of the success or failure of each authentication request, through email and/or SMS. Such notification should shall include the name of the requesting entity, the date and time of authentication, the authentication response code (in case of online authentication), the last four digits of the Aadhaar number and the purpose of authentication, as the case may be.<br>In case of authentication failure, the AUA/KUA should, in clear and precise language, inform the Aadhaar number holder of the reasons of authentication failure, such as “Aadhaar cancelled”, “Aadhaar deactivated”, “Aadhaar locked”, “Aadhaar omitted”, “Aadhaar suspended” and “Biometrics locked”. | | | |
| 96. | Establishment of grievance handling mechanism | Sub AUA / Sub KUA should have an effective grievance handling mechanism and provide the same through multiple channels. | | | |
| 97. | Aadhaar authentication for banks | Where applicable, Sub AUA / Sub KUA should comply with notification no. 13012/79/2017/Legal-UIDAI (No. 6 of 2017), dated 19.12.2017, regarding the process for placing and overriding bank accounts on Aadhaar Payments Bridge (APB) — National Payments Corporation of India (NPCI) Mapper. In particular, the Sub AUA / Sub KUA should comply with the following: | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | (a) Override request pertaining to an Aadhaar number holder should be accompanied by the name of his/her current bank on the APB mapper and confirmation from the requesting bank that it has obtained the requisite consent of the Aadhaar holder for switching to the requesting bank on the mapper.<br>(b) Send request for mapping of a new account or overriding an existing bank account to NPCI only after taking explicit, informed consent of the customer.<br>(c) Inform each accountholder through SMS and email, within 24 hours, that a request has been sent to NPCI to put his/her bank account on the mapper or, as the case may be, to change his bank account on the NPCI mapper (while providing the name of current bank on the mapper and the last four digits of the account number of the new bank, along with the bank name) and, in case he/she does not want to put his/her new bank account on the mapper, provide the customer an option to reverse such mapping.<br>(d) If an accountholder does not have an email or mobile number and communication cannot be sent, his/her physical signature on a paper consent form should be obtained prior to sending the request to the NPCI mapper.<br>(e) The records of consents obtained in (b) and the communications made in items (a), (b) and (c) and scanned copy of the consent form in (d) | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | should be retained for seven years by the bank, in accordance with the Aadhaar (Authentication and Offline Verification) Regulations, 2021.<br>(f) Make available the aforesaid records at the time of audit, in accordance with the Aadhaar (Authentication and Offline Verification) Regulations, 2021. | | | |
| **M.** | **Application security** | | | | |
| 98. | Compliance to API specifications and application security | Sub AUA / Sub 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. | | | |
| 99. | API whitelisting and API gateway implementation | Sub AUA / Sub KUA should ensure that it has API whitelist implemented to limit the data exchange using only authorised APIs and with whitelisted IP addresses.<br><br>Sub AUA / Sub KUA should also ensure that API gateway is deployed for centralised security enforcement, monitoring and management.<br><br>Sub AUA / Sub KUA should ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDoS) attacks.<br><br>Sub AUA / Sub KUA should ensure that Cross-Origin Resource Sharing (CORS) parameters are configured to restrict unauthorised domains from accessing APIs from the client side. | | | |
| 100. | Source code review | Sub AUA / Sub KUA should perform source code | | | |

| | | | | | |
|---|---|---|---|---|---|
| | by CERT-In-empanelled auditor | review of the modules and applications used for authentication and e-KYC as part of IS Audit and should undergo such audit by a CERT-In-empanelled auditor. | | | |
| 101. | SAST/DAST application audit | Sub AUA / Sub KUA should ensure that authentication application security assessment {including static application security testing (SAST) and dynamic application security testing (DAST)} is performed at least annually or at the time of major changes to the authentication application, and that all vulnerabilities are addressed for remediation and no vulnerable third party components are used by the authentication application. | | | |
| 102. | Vulnerability assessment | Sub AUA / Sub KUA should plan organisation information security policy, inclusive of vulnerability assessment and penetration testing on its network, infrastructure and applications. | | | |
| 103. | Configuration reviews and system walkthrough | Sub AUA / Sub KUA should ensure that authentication applications are integrated with IDAM, PIM/PAM and SIEM. | | | |
| 104. | Application code review | Sub AUA / Sub KUA should ensure that the passwords, tokens, security keys and licenses are not hardcoded in the application code. | | | |
| **N.** | **Logging and monitoring** | | | | |
| 105. | Authentication log maintenance | Sub AUA / Sub KUA should maintain logs of the authentication transactions processed by it, which should contain the following transaction details:<br>(a) specified parameters of authentication request submitted;<br>(b) specified parameters received as authentication response;<br>(c) the record of disclosure of information to the | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Aadhaar number holder at the time of authentication; and<br>(d) record of consent of the Aadhaar number holder for authentication, but shall not, in any event, retain the PID information, Aadhaar number / VID. | | | |
| 106. | Authentication log retention | Sub AUA / Sub KUA should ensure that the logs of authentication transactions are stored online for audit purposes for two years and, thereafter, archived for another five years. | | | |
| 107. | Security incident recording | Sub AUA / Sub KUA should ensure that the event/security logs recording critical user-activities, exceptions and security events are enabled and stored to assist any future investigation and enable access control monitoring. | | | |
| 108. | Security incident monitoring | Sub AUA / Sub KUA should ensure that regular monitoring of event/security logs takes place to detect unauthorised use of information systems and that results of the same are recorded. Further, access to audit trails and event logs should be provided to authorised personnel only. | | | |
| 109. | Clock synchronisation through use of Network Time Protocol (NTP) | Sub AUA / Sub KUA should connect to the Network Time Protocol (NTP) server of the 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. | | | |

| | | | | | |
|---|---|---|---|---|---|
| **O.** | **Fraud and forensics** | | | | |
| 110. | Fraud analytics module | Sub AUA / Sub KUA should deploy, as part of its systems, a fraud analytics module that is capable of analysing authentication related transactions to identify fraud. | | | |
| 111. | Authentication application security | Sub-AUA/Sub-KUA should ensure that the client application(s) does/do not, under any circumstance, replay the authentication request. | | | |

***