Authentication Service Agency

Audit Compliance Checklist_V3.0

Guidelines for the Auditor/Assessor:

1. Auditor must be CERT In empanelled for conducting IS Audit.

2. All below points need to be checked for the entire ecosystem of Authentication Service Agency (ASA), network connectivity with the requesting agencies, including physical and logical infrastructure of the ASA. The auditor/assessor is expected to mention details of the reason for compliance or non-compliance in the remarks section.

3. The auditor/assessor is expected to provide reasonable evidences as part of the report to support the compliance status provided in the report.

4. The auditor/assessor may add further points in this checklist to include details of the specifications/ requirements defined below. This is specifically for the points where the entire Regulation/ specification / notification / Circular / Policy etc. has been mentioned as a single checkpoint

S.No.	Compliance Control	Yes/No/NA	Auditor Remarks
A1	**Security Policy Framework**		
1	Authentication Service Agency shall establish dual redundant, secured leased lines or MPLS connectivity with CIDR, in accordance with the procedure and security processes as may be specified by the Authority for this purpose.		
2	Encrypted PID blocks and license keys, that came as part of authentication must not be stored anywhere in its system.		
3	The ASA should ensure with respect to above, that Session key must not be stored anywhere except in memory and should not be reused across transactions. Only re-use of session key is allowed when its use as seed key when using synchronized session key scheme.		
4	It is mandatory that network between ASA and AUA be secure. It is strongly recommended to have leased lines or similar secure private lines between ASA and AUA. If a public network is used, a secure channel such as SSL/TLS should be used.		
5	How ASA does ensure strong governance and technical security control/ solution are implemented for restriction, governance and monitoring of internet access for operator as well as staff? Evidence- Network Diagram; Security Architecture Diagram; Information security Policy & Procedure document or policy document providing brief of internet access control are Training and awareness, Developing Acceptable use policy, URL/DNS filtering, Firewall, Network access control's, Proxy Server etc)		
6	Does ASA ensure operator employed for performing		

	authentication functions and for maintaining necessary system and infrastructure, and process'(s) requisite qualification for undertaking such works.		
7	Does ASA have data classification and labeling policy in place? What is the data classification level applied to Aadhaar and correlated data? Please share data labeling and classification policy? Evidence required- Data Labeling / Data classification policy		
8	What are the detection, prevention and recovery controls installed on end user device, server and critical assets by ASA to protect against malware, how are these solution implemented, combined with appropriate user awareness. Evidence- Antivirus solution screenshot highlighting last update date and configuration setting.		
9	Does ASA has planned, established, implemented and maintained an audit program(s), including the frequency, methods, responsibilities, planning requirements and reporting. Does the audit program(s) take into consideration the importance of the processes concerned and the results of previous audits? Evidence- Please provides below- Detail of Internal audit, frequency, team responsible to perform and how identified risks are tracked; Please provide external audit certificate. Please provide detail of audit per regulatory requirement and audit certificate or report.		
10	Does ASA has documented, approved and published data privacy policy, in line with Authority requirement, and IT Act 2011. (Please share the data privacy policy based on which ASA and link to		

	website.) Evidence- Data Privacy policy and link to policy on website.		
11	The ASA server host shall reside in a segregated network segment that is isolated from the rest of the network of the ASA organization. The ASA server host shall be dedicated for the Aadhaar Authentication purposes and shall not be used for any purpose other than those specified in the application for appointment as ASA. Evidence- Network architecture diagram, data flow diagram or supporting artifact		
12	It is mandatory that Authentication Service Agencies shall have their servers used for Aadhaar authentication request formation and routing to CIDR to be located within data centers located in India.		
13	ASA shall maintain logs of (a) identity of the requesting entity; (b) parameters of authentication request submitted; and (c) parameters received as authentication response: Is maintained at least for 2 years or applicable by law. ASA should comply with regulation 20 of Aadhaar act 2016 (Maintenance of logs by Authentication Service Agencies)		
14	Does ASA store Aadhaar number, UID token, Virtual ID (VID), PID information, ANCS Token device id ASA related data and any resident related PII data received as a part of authentication/ e-KYC response in their transaction logs.		
15	Does ASA comply with log retention period defined per The Aadhaar (Authentication and Offline Verification) Regulation, 2021? Is audit trail of authentication transactions		

	maintained by the ASA for a period of 2 (two) years and Upon expiry of the period of two years, the audit trail archived for a period of five years, or regulations governing the ASA . Evidence- Logging and monitoring policy.		
16	ASA should only engage with the AUA approved by the Authority and keep the Authority informed of the list of requesting entities that it serves along with all relevant details of its agreements with the AUAs. In case of disengagement with an AUA / KUA, the ASA shall inform UIDAI within a period of 7 days from the date of disengagement.		
17	Does ASA perform basic compliance and completeness checks on the authentication data packet such as checking structural validity of the ASA packet and checking signature of the ASA to ensure no unwanted, malicious requests are sent through.		
18	ASA should ensure that its operations are audited by an information systems auditor certified by a recognized body on an annual basis, and provide a certified audit report, to the Authority, confirming its compliance with the policies, processes, regulations etc.		
A2	**Security and Management of the Aadhaar Authentication Infrastructure**		
19	Does Authentication Service Agency, has identified top management who is responsible for compliance towards UIDAI requirement? Evidence Required- TPOC and MPOC- Name, email and detail Escalation matrix with name, contact, and email detail of top management responsible for compliance toward UIDAI.		
20	Standard Operating Procedure (SOP) shall be		

	developed for all information systems and services related to UIDAI operations. The SOP shall include the necessary activities to be carried out for the operation and maintenance of the system or service and the actions to be taken in the event of a failure.		
21	ASA shall ensure all infrastructure and operations including systems, processes, devices, software and biometric infrastructure, security, and other related aspects, are in compliance with the standards and specifications as may specified by the Authority for this purpose. The ASA shall at the minimum ensure: a) ASA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the server from all sources other than the respective ASA s / ASA s. b) All server/network devices clocks shall be set to an agreed standard using an NTP server or must be managed centrally and procedure shall be made to check for and correct any significant variation. c) Regular patches should be updated at both application and server level. d) An auto lock out mechanism for workstation, servers and/ or network device shall be implemented. e) All the assets (e.g., desktop, laptop, servers, databases etc.) used by ASA shall be used after their hardening has been done as per the ASA hardening baseline document (unless the hardening baseline is defined by UIDAI).		
22	The client applications i.e. software used by ASA for the purpose of authentication, shall conform to the standard APIs and specifications laid down by the Authority from time to time for this purpose.		
23	ASA shall perform Source Code review of the modules and applications used for establishing connectivity with CIDR and undergo audit by a certified auditor and audit plan include organization information security policy inclusive of vulnerability assessment as well as penetration test on ASA		

	network, infrastructure and application. 1. Network and application security policy 2. Vulnerability scans report with frequency 3. Third party penetration test report for ASA application, network and infrastructure		
24	Does all the assets (e.g., desktop, laptop, servers, databases etc.) used by ASA and their sub-contractors for Aadhaar Authentication are used only after their hardening as per the ASA hardening baseline document. Evidence required- ASA Hardening checklist		
25	Are sufficient security measures implemented to detect and prevent data leakage? Please provide detail of data leakage prevention solution or the alternative control implemented. Evidence- Security policy highlighting control DLP policy and its scope. Screenshot from DLP solution or any other supporting artifact. Network intrusion and prevention systems/solution, Patch Management, encryption and identification and authentication mechanism, example DMZ, IPS/ IDS, WAF/Firewall, IAM solution etc. ASA should ensure to comply with Regulation 5, of Aadhaar (Data Security) Regulations, 2016.		
26	Does ASA conduct BGV check on employees, contractor, part timer or its third party having access to Aadhaar data or application or infrastructure used to process same? Are employees required to sign a Non Disclosure agreement or confidentiality agreement prior to granting access to data and infrastructure? Evidence required- 1. BGV Check template or Pre employment check policy document		

	2. Copy of NDA or Confidentiality agreement signed		
27	Does ASA maintain inventory of assets consisting of informational assets and hardware assets? Are these assets labeled, classified, and monitored/ reviewed periodically? Does the asset register have well defined owners and custodians and reflect correct classification scheme for each and every asset? Are the asset registers updated and reviewed periodically?		
28	Does ASA have data and asset disposal policy in place? Can you please confirm no obsolete asset is used example Windows 2008, End of Life device		
29	Does the user ID credentials and access rights of personnel handling Aadhaar related authentication, data revoked/ deactivated within 24 hours of exit of the personnel.		
30	Does ASA maintain movement log register for equipment send out for repair, and ensures equipment are sanitized it does not contain any Aadhaar related data. . Does ASA take the necessary steps to ensure the sanitization of the remanence data?		
31	ASA shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets containing any Aadhaar related data.		
32	Does end user device have encryption software installed to secure data? Please share name of the software.		
33	ASA servers should be placed in a secure cabinet in the ASA Data Centre. The facility should be manned by security guards during and after office hours.		
34	The Test and Production facilities / environments must be physically and logically separated.		

	Evidence- secure software development policy (SSDLC)		
35	ASA should ensure the license keys are kept secure and access controlled.		
A3	**Cryptography and Key Management**		
36	The key(s) used for digitally signing of authentication request shall be stored in HSM only. The HSM used shall be FIPS 140-2 compliant.		
37	The authentication request shall be digitally signed by the requesting ASA and/or by the Authentication Service Agency (using FIPS 140-2 compliant HSM), as per the mutual agreement between them and forwarded to CIDR.		
38	In case of decryption of e-KYC response data received from UIDAI for e-KYC request, the ASA can decrypt the data at its end only subject to UIDAI approval.		
A4	**Compliance Requirements**		
39	ASA shall comply with all the provisions as defined in the UIDAI Information Security Policy for External Ecosystem ASA.		
40	The ASA shall comply with all applicable laws in respect of storage and maintenance of authentication transaction logs, including the Information Technology Act, 2000.		
41	ASA shall, at all times, comply with any contractual terms and all rules, regulations, policies, manuals, procedures, specifications, standards, and directions issued by the Authority.		
42	ASA should be in compliance with the Intellectual Property provisions as defined in the agreement with UIDAI.		
43	ASA should comply with the Aadhaar Act, 2016 and any subsequent amendment(s).		

44	ASA should comply with Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
45	ASA should comply with Aadhaar (Data Security) Regulations, 2016.		
46	ASA should comply with Aadhaar (Sharing of Information) Regulations, 2016.		
47	The ASA should comply with all the requirements of UIDAI circular K-11022/204/2017-UIDAI (Auth-I) dated 22 June 2017. (Implementation of HSM in Aadhaar authentication services).		
48	ASA should comply with Regulation number 19 (Roles, responsibilities and code of conduct of Authentication Service Agencies), Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
49	ASA should comply with Regulation number 20 (Maintenance of logs by Authentication Service Agencies), Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
50	ASA should comply with Regulation number 21 (Audit of requesting entities and Authentication Service Agencies), Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
51	ASA should comply with Regulation number 22 (Data Security), Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
52	ASA should comply with all relevant laws, rules and regulations in respect to storage and maintenance of logs, including, but not limited to, Aadhaar Act, 2016 and its Regulations and the Information Technology Act, 2000.		
53	ASA should comply with all the circulars, notices, mandates issued by UIDAI from time to time.		

54	Please provide detail on grievance handling mechanism set (by ASA), and detail on channel's they can be approached via. Please share supporting evidence or link		
55	The requesting ASA should comply with provisions of ASA Agreement with UIDAI at all times		
56	The ASA should comply with Regulation number 23, Chapter-III, Aadhaar (Authentication) Regulations, 2016.		
57	ASA shall ensure that its operations and systems are audited by an information systems auditor certified by a recognized body on an annual basis and on a need basis to ensure compliance with UIDAI standards and specifications. The audit report shall be shared with UIDAI upon request; If any non-compliance is found as a result of the audit, management shall: 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 action; d) Review the corrective action taken The ASA should ensure to comply with Regulation Aadhaar (Data Security) Regulations, 2016. Evidence- Risk management policy document		
58	ASA should ensure message security and integrity between there server's, and AUA server. If ASA can digitally sign the request XML if it is a domain-specific aggregator and forms the request XML on behalf of the AUA.		
59	ASA should ensure private key used for digitally signing the authentication request and the license keys are kept secure and access controlled. The private key should meet below parameter specified by the authority and documented in SPI		

	Specification document (latest):- a) Digital signature certificate used/ procured should be of class II or class III certificate		
60	ASA should connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronization of all their ICT systems clocks. असा having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC. Reference- CERT-In Directive No. 20(3)/2022-CERT-In dated April 28, 2022. Evidence- Clock Sync evidence from CMD;		
61	Does Authentication Service Agency, has set of policies for information security defined, approved by management, published and communicated to employees on and relevant external parties on periodic basis? Evidence- Latest Information security policy/procedure document		
62	Do all employees of the Authentication Service Agency and, are relevant, contractors receive information security awareness education and training and regular updates in ASA policies and procedures, as relevant to job function. Are new hire required to undergo mandatory information security and awareness training? Does, the training provided include all relevant security and privacy guidelines laid by the Authority. Evidence- 1. Information security awareness training record; 2. Information security awareness training content		

	or PPT.		
63	Does ASA have user access right provisioning and deprovisioning process in place? How does ASA manage and monitor individuals access information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing Aadhaar related information. What is the frequency of periodic user access right review? Evidence- Access control procedure and policy document.		
64	Are access rights and privileges to information processing facilities for Aadhaar related information revoked within 24 hours of exit of respective personnel? Post deactivation, user IDs deleted if not in use? Evidence- Email or IAM solution screenshot as supporting evidence		
65	The ASA servers should be placed in a secure cabinet in the ASA Data Centre. Evidence- Physical and environmental security policy		
66	ASA Data Center hosting Aadhaar related information shall be fully secured and access controlled. ASA Data Center shall be manned by security guards during and after office hours CCTV surveillance shall cover the ASA servers. Access to the ASA Data Center shall be limited to authorize personnel only and appropriate logs for entry of personnel should be maintained.		

	Physical access to ASA Data Center and other restricted areas hosting critical Aadhaar related equipment/information shall be pre-approved and recorded along with the date, time and purpose of entry. The movement of all incoming and outgoing assets related to Aadhaar in the ASA Data Center shall be documented. Signs or notices legibly setting forth the designation of restricted areas and provisions of entry shall be posted at all entrances and at other points along the restricted areas		
67	Lockable cabinets or safes shall be provided in the ASA Data Center and information processing facilities having critical Aadhaar related information. Fire doors and fire extinguishing systems shall be deployed, labeled, monitored, and tested regularly Evidence- Physical and environmental security policy		
68	Preventive maintenance activities like audit of fire extinguishers, CCTV shall be conducted quarterly. Evidence- Physical and environmental security policy		
69	ASA personnel shall 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. Evidence- Secure software development policy document;		
70	The ASA server shall reside in a segregated network segment that is isolated from the rest of the network of the ASA organization. The ASA server shall be dedicated for the online Aadhaar Authentication		

	service purposes and shall not be used for any other activities not related to Aadhaar Evidence- Network architecture diagram; Network and application security policy		
71	ASA and other sub-contractors providing Aadhaar authentication service to AUA shall ensure AUA information is not displayed or disclosed to external agencies or unauthorized persons. Also, Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate or any other document/service shall not be published or displayed at any platform.		
72	ASA must have its Aadhaar related servers hosted in data centers within India.		
73	ASA should inform UIDAI without delay within 72 hours after having knowledge of misuse of any information related to the Aadhaar related information or system, compromise of Aadhaar related information. Evidence- Incident response policy and plan document; Incident notification timeline; Contact personnel and channel of information to UIDAI.		
74	ASA should document all changes to Aadhaar authentication applications, Infrastructure, processes and Information Processing facilities, and maintain Change log/ register. Evidence- Change management policy		
75	ASA shall not publish any personal identifiable data including Aadhaar in public domain/websites		

	etc.		
76	ASA shall define a procedure for disposal of the information assets being used for authentication operations. Information systems/documents containing Aadhaar related information shall be disposed of securely Evidence- Data retention policy; Data destruction policy		
77	ASA should ensure incident management framework is implemented in accordance to Information security policy requirement/circular with inclusion of forensic investigation. ASA shall perform Root Cause Analysis (RCA) for major incidents identified in it's as well as sub-contractors' (if any) ecosystem. It is recommended that ASA shall deploy as part of its systems, a Fraud Analytics module that is capable of analyzing authentication related transactions to identify fraud. Evidence- Incident response policy and plan document. Escalation matrix;		
78	ASA should implement exception-handling mechanisms and back-up mechanisms to ensure seamless provision of authentication delivery of services to the residents Evidence- Back- up policy;		
79	How does ASA ensure operational continuity and high availability of service? Please share business continuity and disaster recovery plan. 1. BCP and DR policy document 2. BCP Dr test detail 3. Crisis management detail		

80	End user device used for developing, process and handling Aadhaar data and application should timeout after session is idle for more than 30 minute to 15 minute based on criticality of application.		
81	ASA should ensure to integrate secure software development during application and software development lifecycle, to ensure security requirement is embedded throughout the development phase. Developer should be periodically provided training to ensure they are aware of SSDLC process. (Security testing (Dynamic and Static, architectural testing, code review. penetration test, User acceptance testing etc)		
82	ASA should utilize test data or non-production data for testing of application or software during testing phase.		
83	ASA should implement process and procedure to perform periodic information security risk assessment on its third party having access to Aadhaar application and resident data. Evidence- Third party risk assessment policy, Name of fourth party and Fourth party name.		
84	How is segregation of duty achieved to conflict of duties and responsibilities to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets?		
85	What is the password construction policy used for creating of password? Does user require to change its password after first login? What is frequency of password? Does the password policy meet's following requirement, if No please share brief comment- 1. Minimum password length of 8 characters		

	2. Contain at least one numeric, one uppercase letter, one lowercase letter and one special character 3. Password expiry after an interval; 4. Password age not less than 5; (Compliance as per Information security ASA policy shared by UIDAI) Evidence- Password construction policy		
86	Does ASA have implemented Single sign on to access UIDAI applications? What is the authentication mechanism utilized? (Example MFA etc) Evidence- Screenshot of SSO portal; Access and authentication policy or supporting artifact which provide over view on authentication process and mechanism		
87	Are password hardcoded in codes, login scripts, any executable program or files OR included in any automated log-on process, e.g. stored in a macro or function key?		

Note: In case of any interpretation issues between this checklist and Aadhaar Act or Regulations, the requesting entity should rely on the Aadhaar Act, its Regulations and other specifications issued by UIDAI.

Declaration by Audit Organization

I hereby declare that the above requirements have been audited and meet the UIDAI standards & Specifications.

Auditor Name:

Auditor Signature:

Date:

Seal/Digital Sign/Company Seal: