SMART PAYMENT SOLUTIONS PRIVATE LIMITED

Version 1.0

Aadhaar Information Security Policy

Scope

This is with reference to the Aadhaar Authentication Services of Unique Identification Authority of India (UIDAI) for the stakeholders of Aadhaar Project (hereinafter referred toas “**SPSPL**” or “**AUA**” or “**KUA**”).

This document details the Information Security Policy and standards applicable to SPSPL as an Aadhaar Authentication User Agency (AUA) / KYC User Agency (KUA).

Document distribution

All Employees of SPSPL including its retailers and third parties who access informationthrough SPSPL information system or handle any information Asset of SPSPL related to Aadhaar.

Aadhaar Information Security Policy

Contents

Terms & Definitions

S. No.	Terms	Definition
1	AAS	AADHAAR Authentication Server
2	API	Application Program Interface
3	AUA/ASA	Authentication User Agency/Authentication Service Agency
4	Sub-AUA	Sub Authentication User Agency
5	CA	Certifying Authority
6	CIDR	Central Identities Data Repository
7	CN	Common Name
8	Asset	An asset is anything that has value to the organization. Assets canbe classified into the following 5 categories: 1. Paper assets: (Legal documentation, manuals, policies & procedures, organizational documents etc.) 2. Physical assets: (computer equipment, communications, utility equipment, buildings etc.) 3. Software assets: (database information, applications, software code, development tools, operational software etc.) 4. People assets: UIDAI human resources andstakeholders. 5. Service assets: (Logistics, building management systems, communications, utilities etc.)
9	Information/ Information Asset (IA)	Information that has value to the organization (UIDAI). Including but not limited to Citizen biometric and demographic information, personally identifiable information, employee information,organization information such as CIDR details etc.
10	IT	Information Technology
11	KUA	Know your customer User Agency
12	NDA	Non-Disclosure Agreement
13	NTP	Network Time Protocol
14	OTP	One Time Password
15	PID	Personal Id entity Data
16	SOP	Standard Operating Procedures
17	SPOC	Single Point of Contact

18	SSL	Secure Sockets Layer
19	STQC	Standard Testing and Quality Control
20	VA	Vulnerability Assessment
21	VPN	Virtual Private Network

1. About the Policy

1.1 Policy Statement

Security of UIDAI Information Assets handled by the SPSPL for providing services~~,~~ is of paramount importance. SPSPL shall ensure the confidentiality, integrity, and availability of these at all times by deploying suitable controls commensurate with the asset value and in accordance with applicable rules.

1.2 Policy Scope

This Aadhaar Information Security Policy is applicable wherever UIDAI information is processed and/or stored by SPSPL and its Sub-AUAs. The policy may be amended from time to time as per regulations of UIDAI.

2 Information Security Domains and related Controls

2.2 Human Resources

1. SPSPL shall appoint a SPOC/team for Aadhaar related activities and communication with UIDAI;

2. SPSPL shall conduct a background check or sign an agreement/NDA with all personnel/agency handling Aadhaar related authentication data. UIDAI or agency appointed by UIDAI may validate thisinformation.

3. Induction as well as periodic functional and information security trainings shall be conducted for all SPSPL personnel for Aadhaar related authentication services. The training shall include all relevant security guidelines per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016.
4. All employees accessing UIDAI Information Assets shall be made aware of UIDAI information security policy and controls.

2.3 Asset Management

1. All Assets used by the SPSPL (As defined in 1.1 above) for the purpose of delivering services to residentsusing Aadhaar authentication services shall be identified labelled and classified. Details of the Information Assets shall be recorded.

2. The assets which are scheduled to be disposed shall be disposed as per SPSPL's Information SecurityPolicy;

3. Before sending any equipment out for repair, the equipment shall be sanitized to ensure that it does not contain any UIDAI sensitive data;

4. AUA / KUA and its Sub-AUAs shall not transfer or make an unauthorized copy of any identity information from removable media to any personal device or other unauthorized electronic media / storage devices.

5. AUA and its Sub-AUAs shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets.

6. Authentication devices used to capture residents' biometric shall be STQC certified as specified by UIDAI.

2.4 Access Control

1. Only authorized individuals shall be provided access to information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing UIDAI information;

2. SPSPL employees with access to UIDAI information assets shall:

   a) Have least privilege access for information access andprocessing;

   b) The operator must be logged out after the session is finished.

   c) Implement an equipment locking mechanism for workstation, servers and/ or network device

3. The application should have auto log out feature i.e. after a certain time of inactivity (15 mins or as specified in the UIDAI Authentication Regulations document), the application should logout.

4. Access rights and privileges to information processing facilities for UIDAI information shall be revoked within 24 hours separation of respective personnel or as mentioned in the exit management policy ofthe organization Post deactivation, user IDs shall be deleted if not in use as per Exit formalities

5. Access rights and privileges to information facilities processing UIDAI information shall be reviewed on a quarterly basis and the report shall be stored for auditpurposes;

6. Common user IDs / group user IDs shall not be used. Exceptions/ risk acceptance shall be approvedand documented where there is no alternative;

7. Procedures shall be put in place for secure storage and management of administrative passwords forcritical information systems. If done manually, then a fireproof safe or similar password vault must beused to maintain the access log register.

8. The users should not be provided with local admin access rights on their system. In the case of administrative access being provided, the users shall be prohibited from modifying the local security settings. Modifying the same shall result in disciplinary action.

9. Three successive login failures or as per the access control policy/password policy of the organizationshould result in a user's account being locked; they should not be able to login until their account is unlocked and the password reset in case of server logins. The user should contact the System Engineers/Administrators for getting the account unlocked. For applications, there should be an automatic lock out period of 30 mins in case of three consecutive login failures or as per the access control policy/password policy of the organization.

10. The local security settings on all the systems shall be aligned and synced with the Active Directory orsimilar solutions for local policy enforcement.

11. If the application is operator assisted, the operator shall first confirm his identity by authenticating himself before authenticating the residents.

12. The access rules of firewalls shall be maintained only by users responsible for firewall administration.

2.5 Password Policy

1. The allocation of initial passwords shall be done in a secure manner and these passwords shall be changed at first login;

2. All User passwords (including administrator passwords) shall remain confidential and shall not be shared, posted, or otherwise divulged in any manner;

3. Keeping a paper record of passwords shall be avoided, unless this can be stored securely;

4. If the passwords are being stored in the database or any other form, they should be stored in encryptedform.

5. Passwords shall be changed whenever there is any indication of possible system or password compromise;

6. Complex passwords shall be selected.

7. Passwords shall not be hardcoded in codes, login scripts, any executable program or files;

8. Password should not be stored or transmitted in applications in clear text or in any reversible form.

9. Passwords shall not be included in any automated log-on process, e.g. stored in a macro or functionkey;

2.6 Cryptography

1. The Personal Identity data (PID) block comprising of the resident’s demographic~~/~~ /biometric data shallbe encrypted as per the latest API documents specified by the UIDAI at the end point device used for authentication.

2. The PID shall be encrypted during transit and flow within the AUA ecosystem and while sharing this information with ASAs; Logs of the authentication transactions shall be maintained but PID

information shall not be retained.

3. The encrypted PID block should not be stored unless in case of buffered authentication for not morethan 24 hours after which it should be deleted from the localsystems;

4. The authentication request shall be digitally signed by SPSPL.

5. While establishing a secure channel to the AADHAAR Authentication Server (AAS), the SPSPL shall verify the following:

   a) The digital certificate presented by the AAS has been issued~~/~~/signed by a trusted Certifying Authority (CA);

   b) The digital certificate presented by the AAS has neither been revoked norexpired;

   c) The Common Name (CN) on the certificate presented by the AAS matches with its fully qualified domain name (presently, auth.uidai.gov.in);

6. Key management activities shall be performed by SPSPL to protect the keys throughout their lifecycle.The activities shall address the following aspects of key management, including;

   a) key generation;

   b) key distribution;

   c) Secure key storage;

   d) key custodians and requirements for dual Control;

   e) prevention of unauthorized substitution of keys;

   f) Replacement of known or suspected compromised keys;

   g) Key revocation and logging and auditing of key management related activities.

2.7 Operations Security

1. SPSPL shall complete the AADHAAR AUA on-boarding process before the commencement of formal operations;

2. 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;

3. Persons involved in operational/development/testing functions shall not be given additional responsibilities in system administration processes, audit log maintenance, security review of systemor process and which may compromise data securityrequirements;

4. Where segregation of duties is not possible or practical, the process shall include compensating controls – such as monitoring of activities, maintenance and review of audit trails and management supervision;

5. The Test and Production facilities~~/~~ /environments must be physically and/or logically separated.

6. The Operating System as well as the network services used for communication shall be updated withthe latest security patches.

7. A formal Patch Management Procedure shall be established for applying patches to the information systems. Patches should be updated at both application and serverlevel;

8. Periodic VA exercise should be conducted for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.

9. SPSPL employees 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 PID information;

10. All hosts that connect to the AADHAAR Authentication Service information shall be secured using endpoint security solutions. At the minimum, anti-virus~~/~~ /malware detection software shall be installedon such hosts;

11. SPSPL shall ensure that the event logs are to be recorded and stored to assist in future investigationsand access control monitoring;

12. Regular monitoring of the audit logs shall take place for any possible unauthorized use of information systems and results shall be recorded. Access to audit trails and event logs shall be provided to authorized personnel only;

13. The authentication audit logs should contain, but not limited to, the following transactional details:

    a) Aadhaar Number against which authentication is sought;

    b) Specified parameters of authentication request submitted;

    c) Specified parameters received as authentication response;

    d) The record of disclosure of information to the Aadhaar number holder at the time of authentication

    e) Record of the consent of Aadhaar number holder for theresident

    f) Details of the authentication transaction such as API Name, AUA / KUA Code, Sub-AUA, TransactionId, Timestamp, Response Code, Response Timestamp, and any other non-identity information.

14. Network intrusion and prevention systems should be in place;

15. Logs shall not, in any event, retain the PID, biometric and OTP information;

16. The logs of authentication transactions shall be maintained by SPSPL for a period of 2 years, duringwhich an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified;

17. Upon expiry of the period of 2 years, the logs shall be archived for a period of 5 years or the numberof years as required by the laws or regulations of Govt. of Punjab, whichever is later, and upon expiryof the said period, the logs shall be deleted except those records required to be retained by court or for any pending

disputes;

18. All computer clocks shall be set to an agreed standard using a NTP server or must be managed centrally and procedure shall be made to check for and correct any significant variation;

19. The AUA server host shall reside in a segregated network segment that is isolated from the rest of thenetwork of the SPSPL; The AUA server host shall be dedicated for the Online AADHAAR Authenticationpurposes and shall not be used for any other activities;

2.8 Communications security

1. In case of a composite terminal device that comprises of a biometric reader without embedded software to affect the encryption of the personal identity data, communication between the biometricreader and the device performing the encryption shall be secured against all security threats / attacks

2. Terminal devices shall provide different logins for operators. These users shall be authenticated usingsome additional authentication scheme such as passwords, AADHAAR authentication, etc.;

3. Each terminal shall have a unique terminal ID. This number must be transmitted with each transactionalong with UIDAI assigned institution code for the AUA as specified by the latest UIDAI API documents

4. A Unique Transaction Number (unique for that terminal) shall be generated automatically by the terminal which should be incremented for each transactionprocessed;

5. The network between AUA ASA shall be secured. AUA shall connect with ASAs through leased linesor similar secure private lines. If a public network is used, a secure channel such as SSL or VPN shallbe used.

6. The AUA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the AUA server from all sources;

7. Special consideration shall be given to Wireless networks due to poorly defined network perimeter. Appropriate authentication, encryption and user level network access control technologies shall be implemented to secure access to the network;

8. Use of web-based e-mail shall be restricted to official use and in accordance with the acceptable usage guidelines or as per organization policy;

9. UIDAI should be informed about the ASAs, the AUA has entered into an agreement;

2.9 Information Security Incident Management

1. SPSPL shall be responsible for reporting any security weaknesses, any incidents, possible misuse, orviolation of any of the stipulated guidelines to UIDAI immediately.

-------------------------------End of Document---------------------