Shreetron India Limited

Revision History

Version	Issue Date	Prepared By	Approved By	Changes
1.0	02.04.2021	Vaneet Soni	A P Panwar	Initial Draft

Scope

This is with reference to the Aadhaar Authentication Services of Unique Identification Authority of India (UIDAI) for the stakeholders of Aadhaar Project, being implemented by AUA Department

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

Document distribution

All Sub AUAs of AUA who access information through AUA information system or handle any information Asset of AUA related to Aadhaar.

Shreetron India Limited

Terms & Definitions

S.No.	Terms	Definition
1	KYC	Know Your Customer
2	AUA	Authentication User Agency
3	ASA	Authentication Service Agency
4	CIDR	Central Identities Data Repository
5	KUA	Know your customer User Agencies
6	NDA	Non-Disclosure Agreement
7	OTP	One Time Password
8	PID	Personal Identity Data
9	STQC	Standard Testing and Quality Control
10	KSA	KYC Service Agency
11	BGV	Back Ground Verification

Shreetron India Limited

1. Introduction

AUA is a Global AUA and has a KUA license issued by Unique Identification Authority of India (UIDAI). It undertake user authentication as per the UIDAI guidelines to enable some of its services / business functions. AUA connects to the CIDR through (Master card) who is an Authentication Service Agency (ASA/KSA).

Since AUA handles sensitive resident information such as the Biometric information, Aadhaar number, e-KYC information etc. of the customers, it becomes imperative to ensure its security and safety to prevent unauthorized access. This Policy is in line with thedirectionsofInformationSecurityPolicyissuedbyUIDAIandisapplicablewhereverUIDAIinformatio nisprocessedand/orstoredbyAUA

2. Objectives of the Policy

The objectives of the policy include:

a) Design suitable controls to ensure the privacy and security of the Biometric information of the customer as well as Aadhaar number and any other data received from the UIDAI in due course of authentication.
b) To provide necessary guidelines to enable compliance with Aadhaar Act 2016 and any other applicable circulars or directions issued by the UIDAI.

3. Applicability

The policy will apply to all departments which access, process or store Aadhaar number and any other data received from the customers or UIDAI in due course of authentication.

4. Aadhaar Data Privacy and Security

AUA will exercise below mentioned controls to ensure the privacy and security of the Aadhaar Data:

4.1 Compliance

- AUA shall comply with all terms and conditions outlined in the AUA/KUA agreement with UIDAI, Aadhaar Act 2016 and various circulars/ directions issued by the UIDAI.

- The operations and systems shall be audited by an information systems auditor certified by recognized body on an annual basis so as to ensure compliance with UIDAI standards and specifications. The audit report shall be shared with UIDAI upon request.

- AUA shall conduct a background check and sign an agreement/NDA with all personnel handling Aadhaar related authentication data.

- Necessary Information security trainings shall be conducted for all personnel for Aadhaar related authentication services during induction.
- Any security incidents affecting the confidentiality, integrity and availability of information received from the UIDAI will be reported to UIDAI at the earliest.
- Display of Full Aadhaar number should be masked and only last four digits of the Aadhaar number shall be displayed.
- AUA will nominate a Management point of contact and a Technical point of contact for Aadhaar related activities and communication with UIDAI.
- UIDAI shall be informed about the ASAs, which AUA has entered into an agreement;
- AUA shall create internal awareness about consequences of breaches of Aadhaar data via various channels such as News letter articles, employee trainings, internal Memos and communications etc.
- AUA shall use only licensed software for Aadhaar related infrastructure environment. Record of all software licenses shall be kept and updated regularly.
- Access to Authentication infrastructure shall not be granted before signing the necessary substantive documentation and completion of BGV for the personnel.

4.2 Handling of Personnel Identity Data (PID)

- AUA will ensure that the Personal Identity data (PID) block comprising of the resident's demographic/biometric data is encrypted as per the latest API standards /specifications specified by the UIDAI at the end point device used for authentication.
- The encrypted PID block including OTP shall not be stored unless in case of buffered authentication and in such case it shall be deleted from the local systems post authentication.
- The authentication request sent by AUA to UIDAI shall be digitally signed either at AUA or at ASA.
- The identity information of the Aadhaar number holders collected during authentication and any other information generated during the authentication process shall be kept confidential, secure and protected against un-authorized access ,use and disclosure.
- The Aadhaar number of the citizens received through authentication shall be masked and stored on a secure database.
- Aadhaar Data in database shall be kept in highly restricted network zone from any untrusted zone and other internal network zones.
- There shall be strong access controls, authentication measures monitoring and logging ofaccessandraisingnecessaryalertsforunusualorunauthorisedattempttoaccess.
- While storing the Aadhaar number in the database, the data must be encrypted and stored. Encryption keys must be protected securely using HSM.

4.3 Operations Security

- At the time of authentication, the citizen shall be informed on: (a) the nature of information that will be shared by the UIDAI upon authentication; (b) the uses to which the information received during authentication may be put; and (c) alternatives for submission of identity information.

- Consent of the Aadhaar number holder shall be obtained for each authentication preferably in electronic form and maintain logs or records of the consent.
- AUA shall capture the biometric information of the Aadhaar number holder using certified biometric devices as per the processes and specifications laid down by UIDAI.
- No data of the customer shall be stored within the terminal device (i.e., biometric device).
- Logs shall not ,in any event, retain the PID, biometric and OTP information
- Network intrusion and prevention systems shall be in place
- All computer clocks shall be set to an agreed standard using a NTP server or must be managed Centrally
- The AUA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the AUA server from all sources other than AUA/KUA's PoT (Point of Transaction)terminals;
- Before sending any equipment out for repair which contains the UIDAI sensitive data, the equipment shall be sanitized to ensure that it does not contain any sensitive data/information.
- The authentication logs shall not be shared with any person other than the concerned Aadhaar number holder upon his request or for grievance redressal and resolution of disputes or with the UIDAI for audit purposes or in compliance with any legal/regulatory compliances.
- Periodic VA exercise should be conducted for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.
- All hosts that handle resident's identity information shall be secured using end point security solutions. An anti-virus / malware detection software shall be installed on such hosts.

4.4 Access Control

- 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 Aadhaar related information. An Access Control List shall be maintained.
- Access rights of employees accessing/processing information received from UIDAI shall be revoked within 24 hours of termination of service or as mentioned in the HR policy of the organization.
- There should be periodic review of the Access rights and privileges to information facilities processing UIDAI information.
- The servers shall be dedicated for the online Aadhaar Authentication purpose and necessary controls should be in place for physical security and surveillance of the servers. Any confidentiality breach/security breach of Aadhaar related information shall be reported toUIDAIwithin24 hours.
- 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.
- The access rules of firewalls shall be maintained only by users responsible for fire wall administration.
- License keys shall be kept secure and access controlled.
- All User passwords (including administrator passwords) shall remain confidential and shall not be shared, posted, or otherwise divulged in any manner

- If the passwords are being stored in the database or any other form, they should be stored in encrypted form
- Complex passwords shall be selected.
- Passwords shall not be hard coded in codes, login scripts ,any executable program or files;
- Password should not be stored or transmitted in applications in clear text or in any reversible form

4.5 Asset Management

- All assets (business applications, operating systems, databases, network etc.) used for the Aadhaar authentication services shall be identified, labeled and classified.
- There should be a clearly defined procedure for the disposal of the information assets being used for authentication operations.
- Only STQC certified Authentication devices shall be used to capture residents biometric.
- Periodic Vulnerability Assessment (VA) exercise shall be conducted for ensuring the security of the Aadhaar infrastructure and Necessary network intrusion and prevention systems shall be implemented.

5. Policy Review and Updates

The Policy shall be reviewed as and when required or at least once in a year, to address the requirements and to comply with guidelines issued by the UIDAI or any applicable regulator or judiciary from time to time. However, any of the regulatory changes, during the year, will be implemented immediately with the approvals.

6. Regulatory References

1. Aadhaar Act 2016
2. Requesting Entity Compliance Checklist_v_2.0
3. Aadhaar regulations 2016
4. UIDAI Information Security Policy for AUA/KUA
5. Various circulars issued by UIDAI

End of Document