DoIT&C – Aadhaar Data Privacy Policy

10 NOV 2022

Department of Information Technology & Communication,
B2-Basement, IT Building,
Yojna Bhawan Campus, Tilak Marg,
C-Scheme, Jaipur, Rajasthan (302005).

Department of Information Technology & Communication
Government of Rajasthan

Contents

1. Introduction

DoIT&C is a Global AUA/ASA and has a KUA/KSA license issued by Unique Identification Authority of India (UIDAI). It undertakes user authentication as per the UIDAI guidelines to enable some of its services.

Since DoIT&C handles sensitive resident information such as the Aadhaar number, e-KYC information etc. It becomes imperative to ensure its security and safety to prevent unauthorized access. This Policy is in line with the directions of Information Security Policy issued by UIDAI and is applicable wherever UIDAI information is processed and/or stored by DoIT&C.

2. Objectives of the Policy

The objectives of the policy include:

a) Design suitable controls to ensure the privacy and security of the 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/Sub-AUAs 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

DoIT&C will exercise below mentioned controls to ensure the privacy and security of the Aadhaar Data:

a. Compliance

i. e-KYC shall be carried out using OTP and biometric authentication modalities

ii. DoIT&C shall comply with all terms and conditions outlined in the ASA/KSA and AUA/KUA agreement with UIDAI, Aadhaar Act 2016 and various circulars/ directions issued by the UIDAI.

iii. 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.

iv. DoIT&C shall conduct a background check and sign an agreement/NDA with all

personnel handling Aadhar related authentication data.

v. Necessary Information security trainings shall be conducted for all personnel for Aadhaar related authentication services during induction.

vi. Any security incidents affecting the confidentiality, integrity and availability of information received from the UIDAI will be reported to UIDAI at the earliest.

vii. Display of Full Aadhaar number of the customers shall be done only for the Aadhaar number holder or employees with special roles/users having the defined need strictly on a "need toknow" basis. By default, all displays should be masked and only last four digits of the Aadhaar number shall be displayed.

viii. DoIT&C will nominate a management point of contact and a technical point of contact for Aadhaar related activities and communication with UIDAI.

ix. DoIT&C shall create internal awareness about consequences of breaches of Aadhaar data via various channels such as Newsletter articles, employee trainings, internal Memos and communications etc.

x. DoIT&C shall use only licensed software for Aadhaar related infrastructure environment. Record of all software licenses shall be kept and updated regularly.

xi. Access to Authentication infrastructure shall not be granted before signing the necessary substantive documentation and completion of BGV for the personnel.

b. Handling of Personnel Identity Data (PID)

i. DoIT&C will ensure that the Personal Identity data (PID) blockcomprising of the resident's demographic / biometric data is encrypted as per the latestAPI standards/specifications specified by the UIDAI at the end point device used for authentication.

ii. 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.

iii. The authentication request sent by DoIT&C to UIDAI shall be digitally signed at DoIT&C (ASA)

iv. 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.

v. The Aadhaar number and any connected data (e.g., e-KYC XML containing Aadhaar number and data) of the customers received through authentication shall be masked and stored ona secure database.

vi. Aadhaar Data in database shall be kept in highly restricted network zone from any untrusted zone and other internal network zones.

vii. There shall be strong access controls, authentication measures monitoring and logging of access and raising necessary alerts for unusual or unauthorized attempt to access.

viii. While storing the Aadhaar number in the database, the data must be encrypted and stored.Encryption keys must be protected securely using HSM.

c. Operations Security

i. At the time of authentication, the customer 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.

ii. Consent of the Aadhaar number holder shall be obtained for each authentication preferably in electronic form and maintain logs or records of the consent.

iii. DoIT&C shall capture the biometric information of the Aadhaar number holder using certified biometric devices as per the processes and specifications laid down by UIDAI.

iv. No data of the customer shall be stored within the terminal device (i.e., biometric device).

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

vi. Network intrusion and prevention systems shall be in place.

vii. All computer clocks shall be set to an agreed standard using a NTP server or must be managed Centrally.

viii. The ASA/AUA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the ASA/AUA server from all sources other than ASA/KSA and AUA/KUA's PoT (Point of Transaction) terminals.

ix. 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.

x. The logs of KYC authentication transactions and the records of consent obtained during authentication shall be maintained for a period of 5 years, from the cessation of the account-based relationship during which an Aadhaar number holder shall have the right to access such logs.

xi. 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.

xii. DoIT&C shall develop Standard Operating Procedure (SOP) for the operation and maintenance of the Aadhaar related system or service. SOP shall define the actions to be taken in the event of a failure.

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

xiv. All hosts that handle resident's identity information shall be secured using endpoint security solutions. An anti-virus / malware detection software shall be installed on such hosts.

d. Access Control

i. 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.

ii. 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.

iii. There should be periodic review of the Access rights and privileges to information facilities processing UIDAI information.

iv. 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 to UIDAI within 24 hours.

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

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

vii. License keys shall be kept secure and accesscontrolled.

viii. All User passwords (including administrator passwords) for the Aadhaar related systems shall be allocated, stored, created, and transmitted as per a clearly defined password policy of the DoIT&C data center.

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

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

xi. Complex passwords shall be selected.

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

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

e. Asset Management

i. All assets (operating systems, databases, network etc.) used for the Aadhaar authentication services shall be identified, labelled and classified.

ii. There should be a clearly defined procedure for the disposal of the information assets beingused for authentication operations.

iii. Only STQC certified Authentication devices shall be used to capture residents biometric.

iv. Periodic Vulnerability Assessment (VA) exercise shall be conducted forensuring the security of the Aadhaar infrastructure and Necessary network intrusion and prevention systems shall be implemented.

v. Event logs of the critical user-activities, exceptions and security events shall be enabled and stored as per the data retention policy of the DoIT&C datacenter.

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 of the DoIT&C 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 approval of officer in charge.

6. Regulatory References

a) Aadhaar Act 2016
b) Requesting Entity Compliance Checklist_v_2.0
c) Aadhaar regulations 2016
d) UIDAI Information Security Policy for ASA/KSA and AUA/KUA

e) Various circulars issued by UIDAI

7. Glossary

KYC	Know Your Customer
OIC	Officer in charge
AUA	Authentication User Agency
ASA	Authentication Service Agency
CIDR	Central Identities Data Repository
KUA	Know your customer User Agencies
NDA	Non-Disclosure Agreement
OTP	One Time Password
PID	Personal Identity Data
STQC	Standard Testing and Quality Control
KSA	KYC Service Agency
BGV	Back Ground Verification